Spot Security

Competitive Analysis

OVERVIEW

Analysis of fifteen competitors in the Cloud Security market including overview of products, differentiators, features, and screenshots of existing product UIs for each competitor.

***Note**: This is a very long document with a lot of images of UIs. Please use the document outline to the left to quickly navigate to individual competitors and sections.*

IDENTIFIED COMPETITORS

From Kevin

Identified from Top Cloud Security Companies and Tools Blog

1. CloudPassage
2. FireEye
3. LaceWork
4. McAfee Cloud Security
5. Palo Alto Networks
6. Qualys
7. Symantec
8. Tenable
9. Trend Micro
10. VMware Cloud

From Azzedine

1. CloudSploit
2. CheckPoint CloudGuard
3. Vantage

Others

1. Lumigo
2. SafeBreach

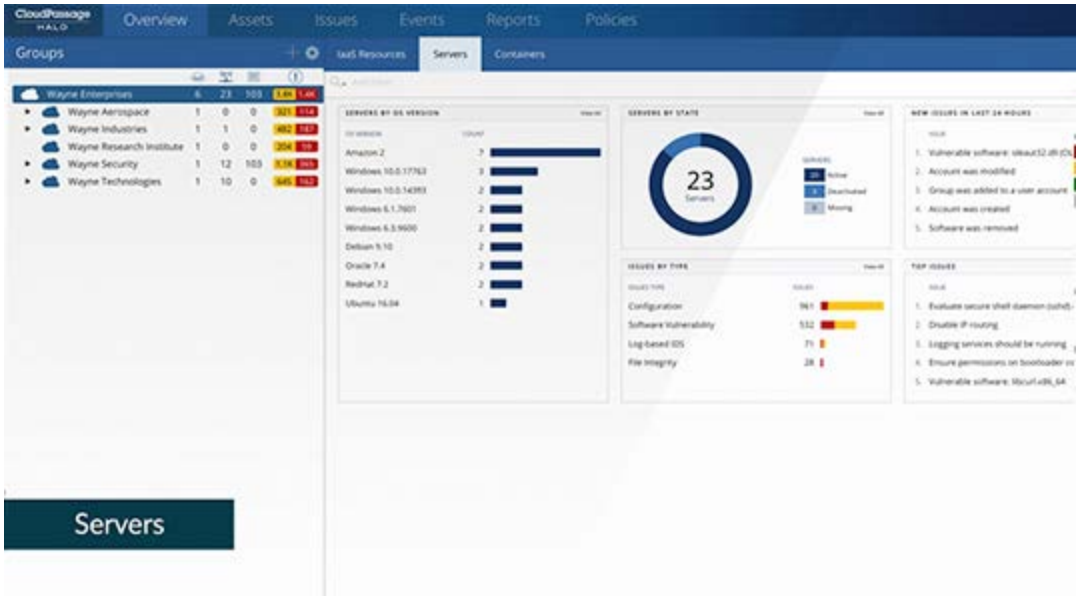
COMPETITOR BREAKDOWN

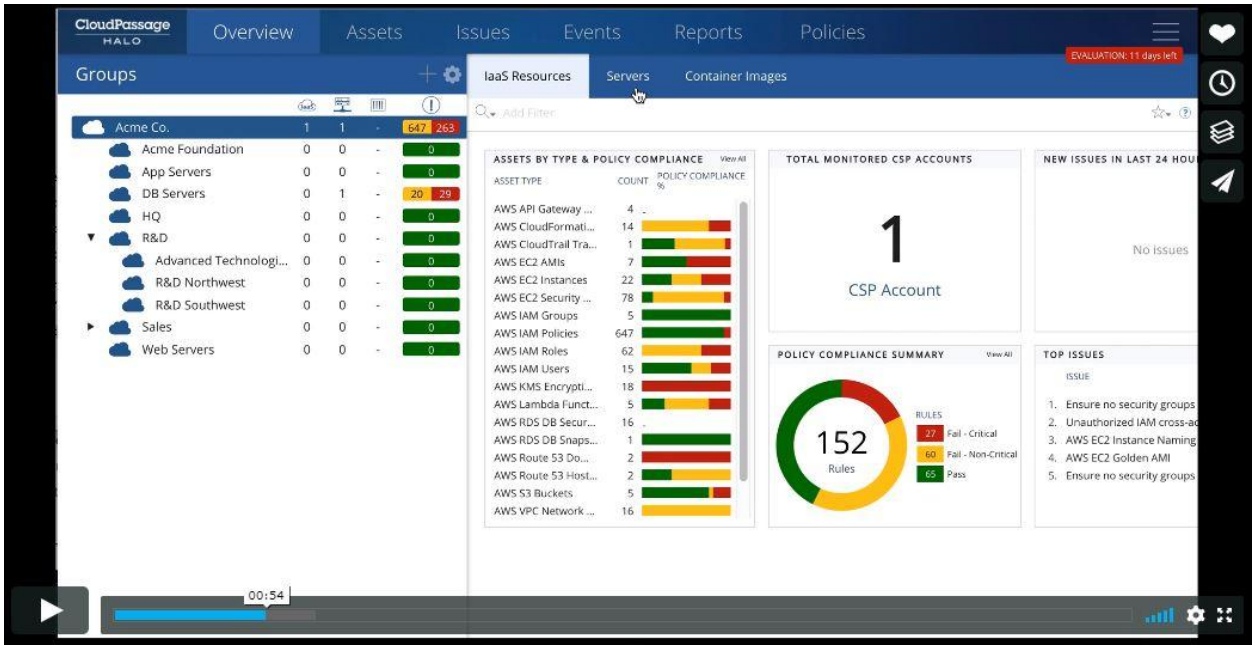
CloudPassage

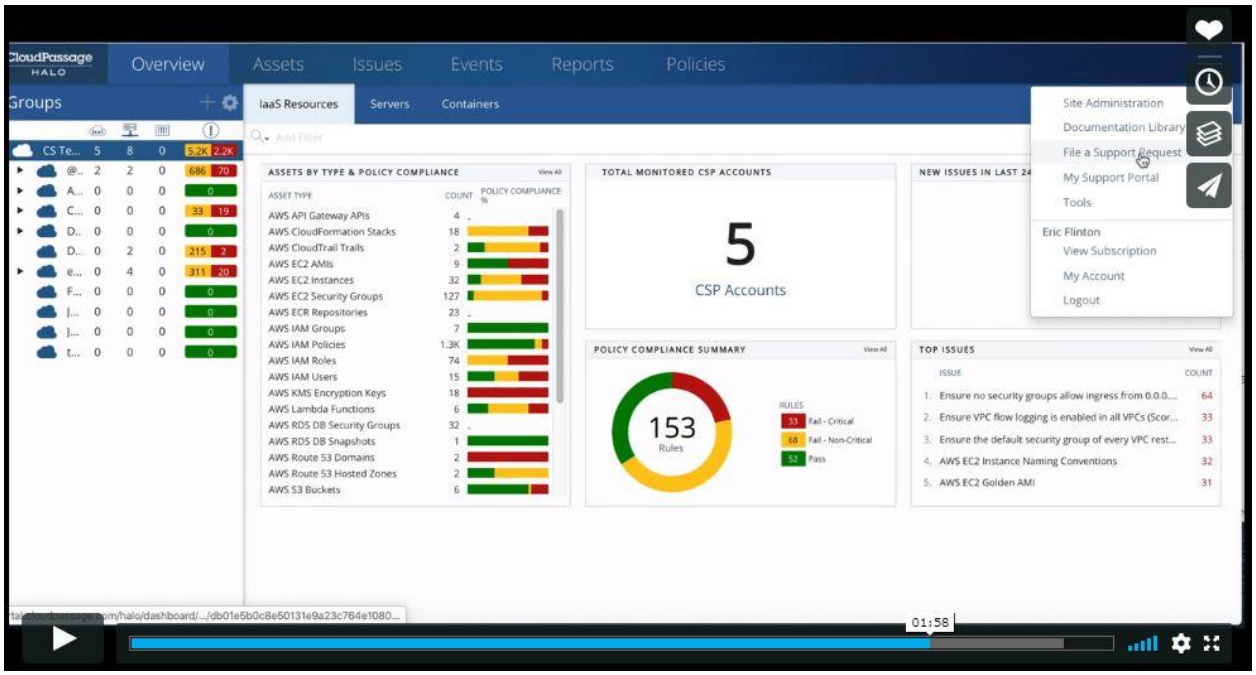
CloudPassage's Halo platform is a cloud workload protection platform that is suitable for organizations of any size.

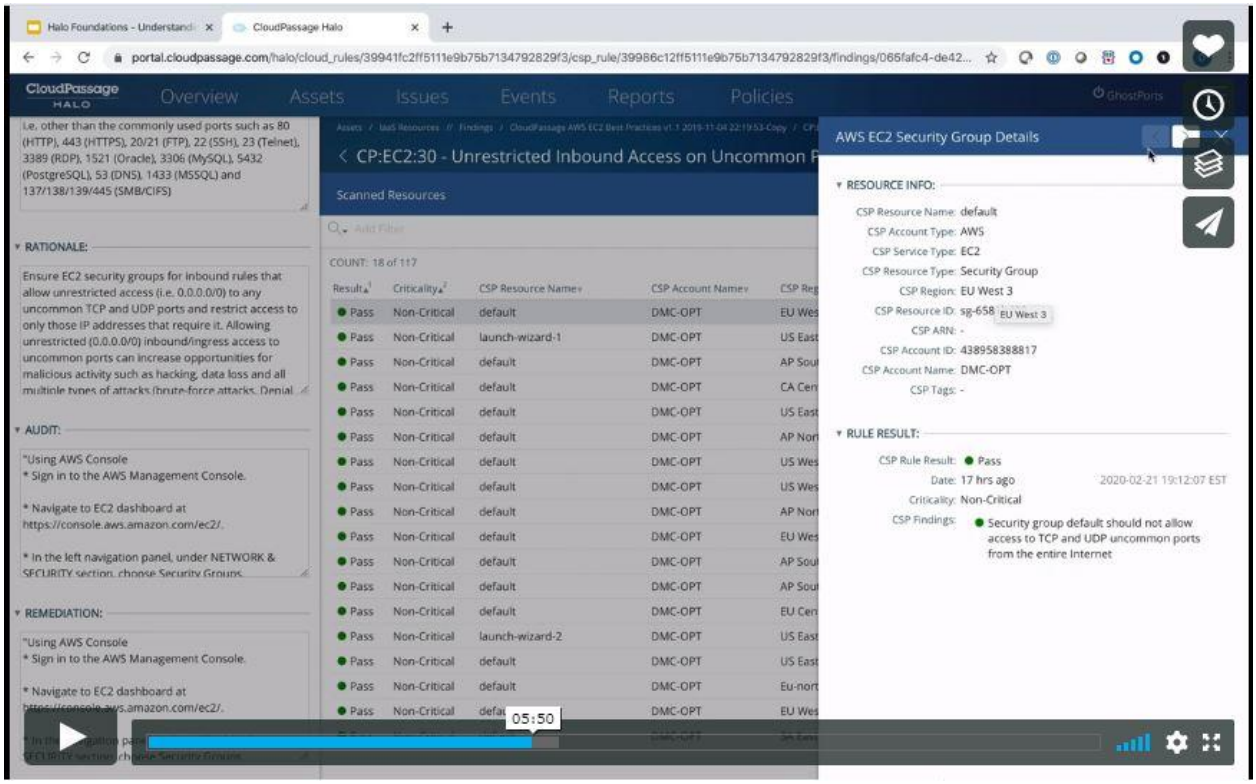
- **Key Values and Differentiators**:
    - Single platform with three SKUs licensed by usage level
    - Offers automated security visibility and compliance monitoring for workloads that run in any on-premises, public cloud, or hybrid cloud environment
    - Automated approach to identify when and if a given workload or configuration strays outside of the defined policies
- **Features include:**
    - Export / Reports
    - RBAC
    - Agent based
    - Resource grouping to apply policies by group
    - Alert
    - SIEM (Security information and event management) like integration with Splunk

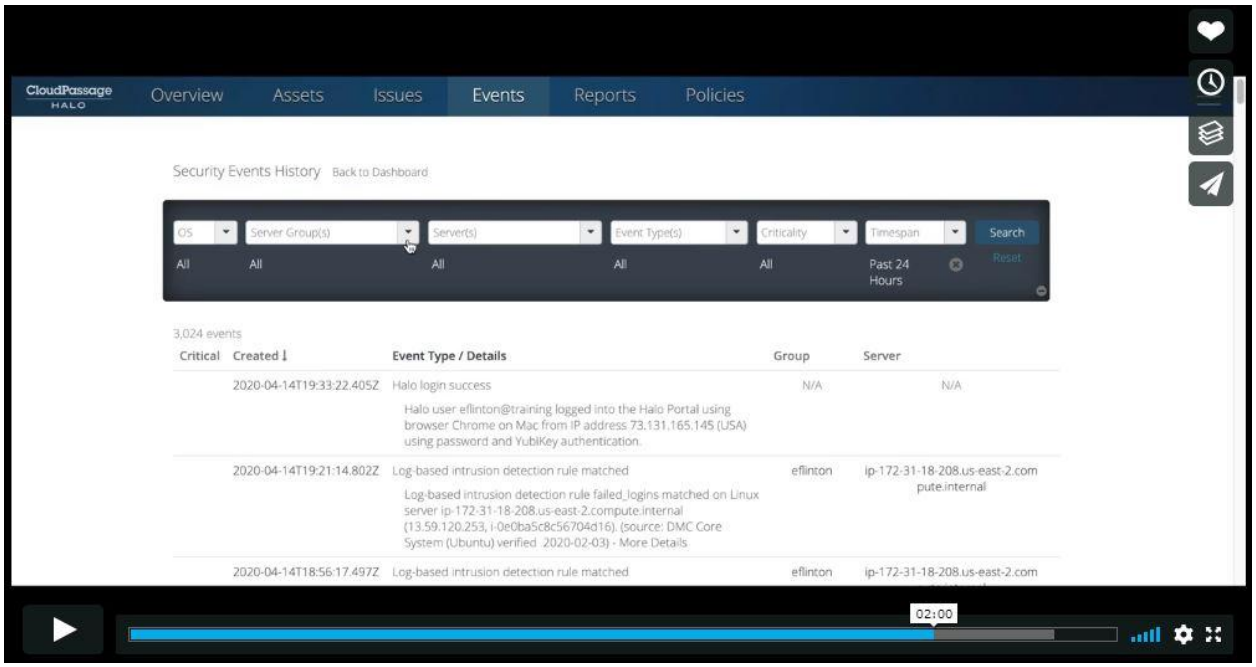
Screenshots of UI:
This doc has a lot of video screengrabs of the UI

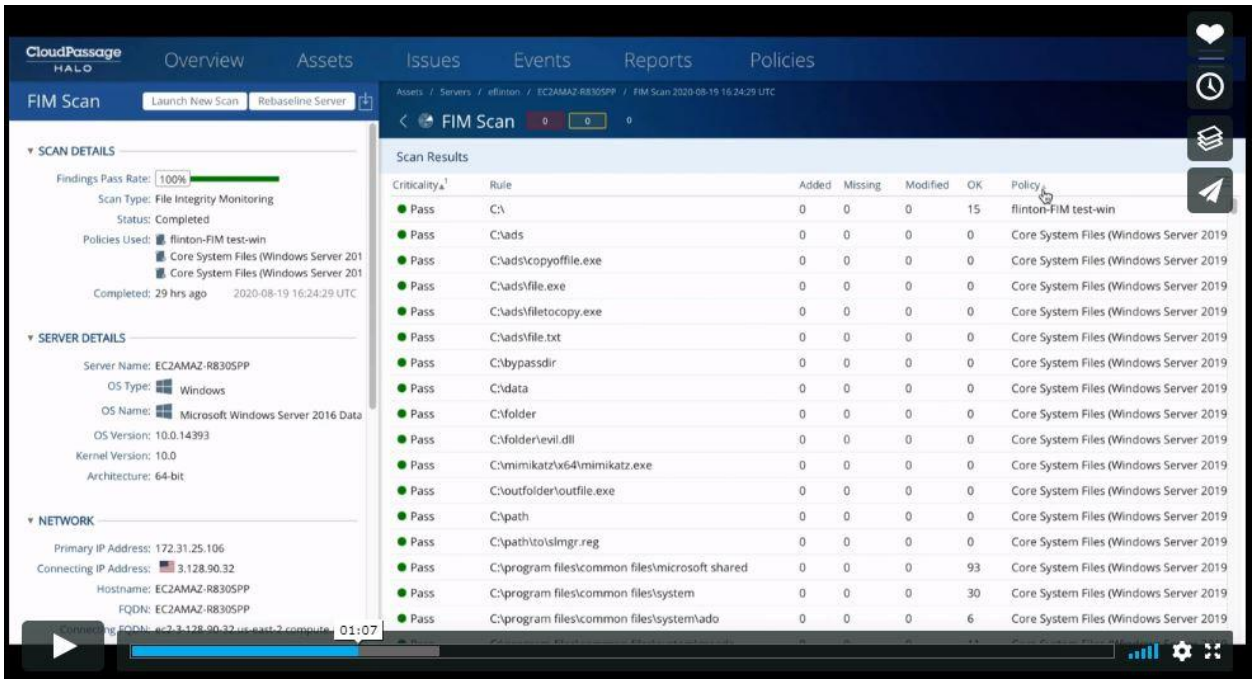


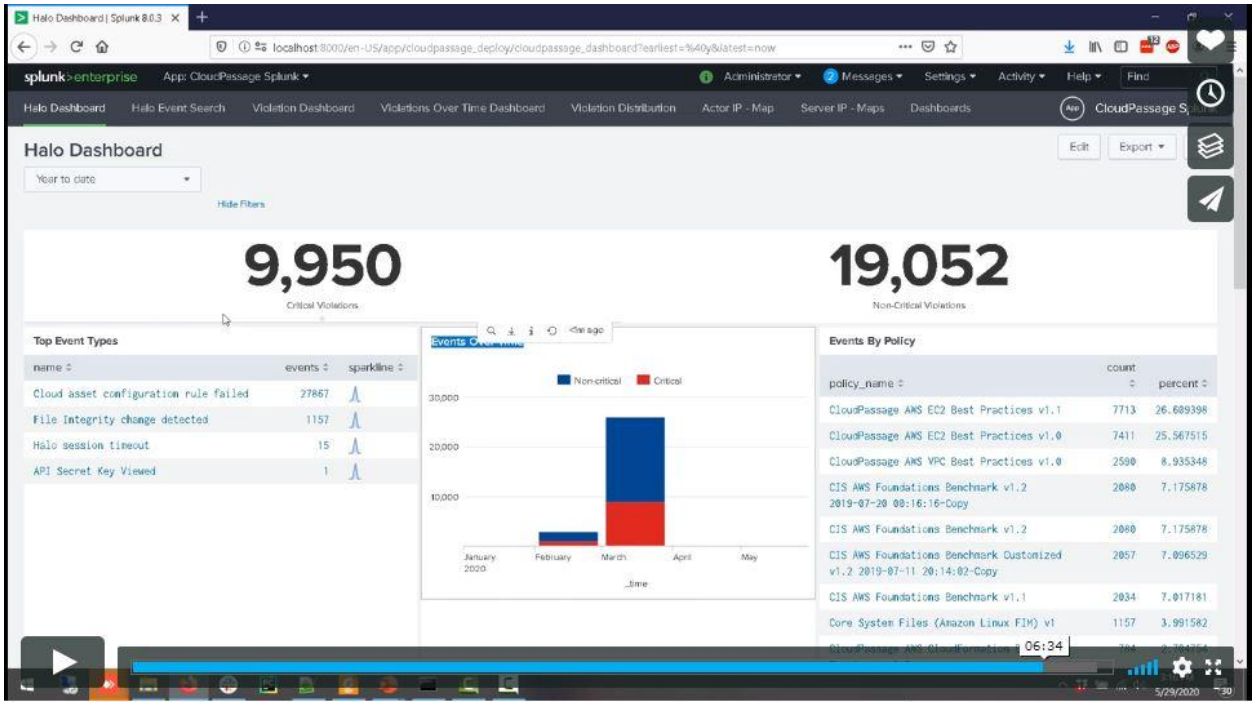

CloudPassage HALO
Overview
Assets
Issues
Events
Reports
Policies
Groups
IaaS Resources
Servers
Container Images
EVALUATION: 11 days left
Acme Co.
Acme Foundation
App Servers
DB Servers
HQ
R&D
Advanced Technologi...
R&D Northwest
R&D Southwest
Sales
Web Servers
ASSETS BY TYPE & POLICY COMPLIANCE
TOTAL MONITORED CSP ACCOUNTS
1
CSP Account
NEW ISSUES IN LAST 24 HOU
No issues
POLICY COMPLIANCE SUMMARY
152
Rules
27 Fail - Critical
60 Fail - Non-Critical
65 Pass
TOP ISSUES
1. Ensure no security groups
2. Unauthorized IAM cross-ac
3. AWS EC2 Instance Naming
4. AWS EC2 Golden AMI
5. Ensure no security groups
00:54

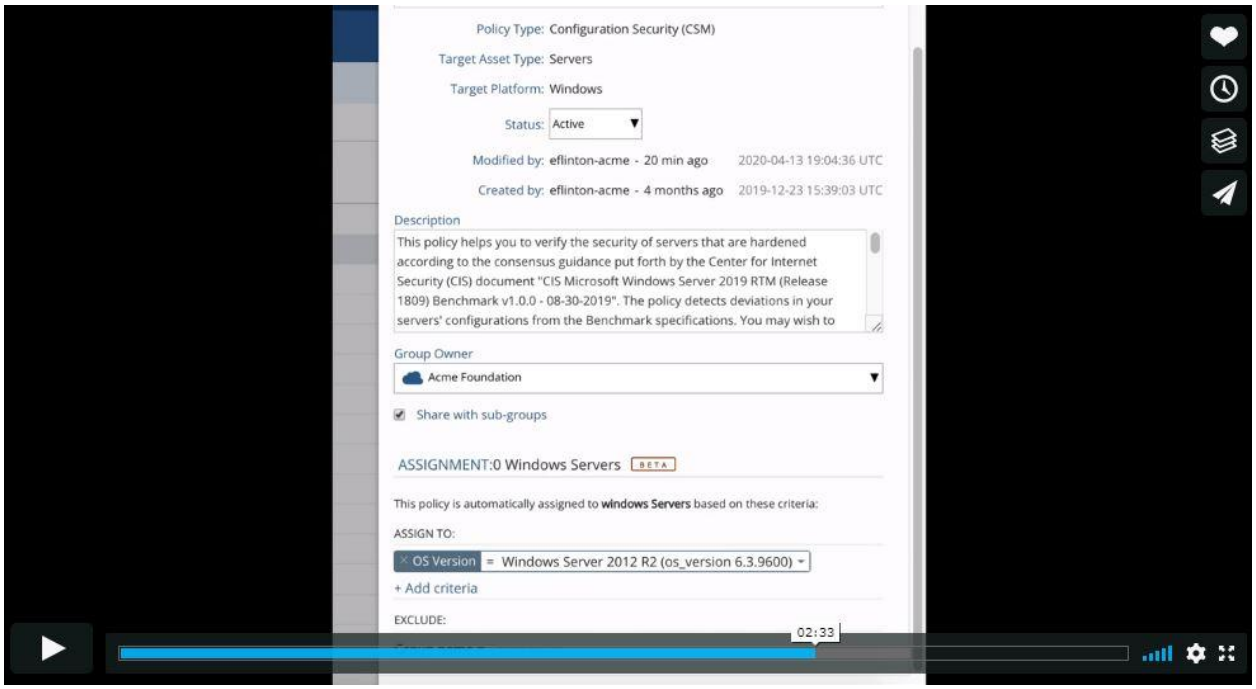

CloudPassage HALO
Overview
Assets
Issues
Events
Reports
Policies
Groups
IaaS Resources
Servers
Containers
Site Administration
Documentation Library
File a Support Request
My Support Portal
Tools
Eric Flinton
View Subscription
My Account
Logout
ASSETS BY TYPE & POLICY COMPLIANCE
TOTAL MONITORED CSP ACCOUNTS
5
CSP Accounts
POLICY COMPLIANCE SUMMARY
153
Rules
33 Fail - Critical
68 Fail - Non-Critical
52 Pass
TOP ISSUES
1. Ensure no security groups allow ingress from 0.0.0.... 64
2. Ensure VPC flow logging is enabled in all VPCs (Scor... 33
3. Ensure the default security group of every VPC rest... 33
4. AWS EC2 Instance Naming Conventions 32
5. AWS EC2 Golden AMI 31
01:58

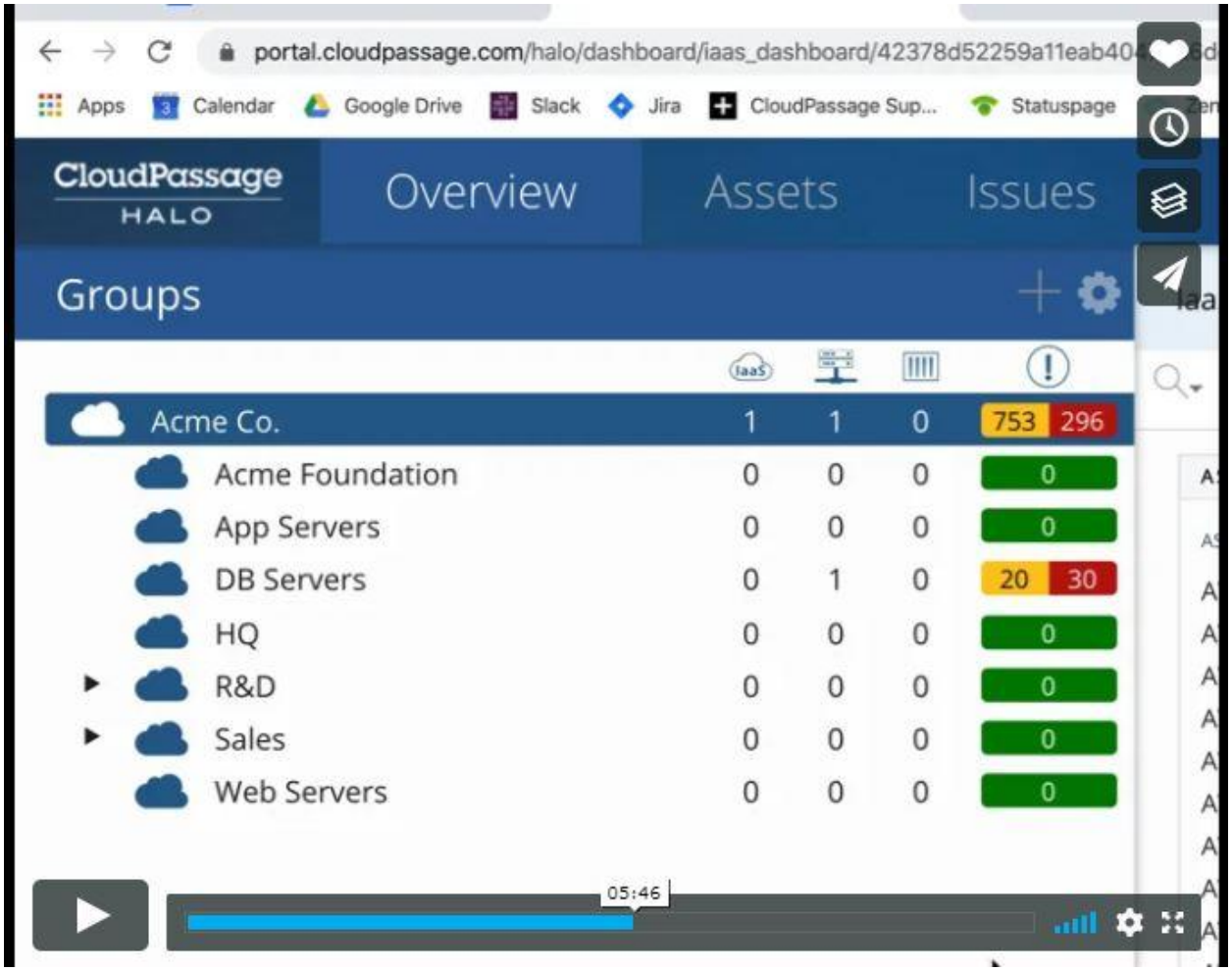

CloudPassage HALO
Overview
Assets
Issues
Events
Reports
Policies
CP:EC2:30 - Unrestricted Inbound Access on Uncommon P
Scanned Resources
AWS EC2 Security Group Details
RESOURCE INFO:
CSP Resource Name: default
CSP Account Type: AWS
CSP Service Type: EC2
CSP Resource Type: Security Group
CSP Region: EU West 3
CSP Account ID: 438958388817
CSP Account Name: DMC-OPT
CSP Tags: -
RULE RESULT:
CSP Rule Result: Pass
Date: 17 hrs ago
2020-02-21 19:12:07 EST
Criticality: Non-Critical
CSP Findings: Security group default should not allow access to TCP and UDP uncommon ports from the entire Internet
RATIONALE:
AUDIT:
REMEDIATION:
05:50


CloudPassage HALO
Overview
Assets
Issues
Events
Reports
Policies
Security Events History
Back to Dashboard
OS
Server Group(s)
Server(s)
Event Type(s)
Criticality
Timespan
Search
Reset
All
All
All
All
All
Past 24 Hours
3,024 events
Critical
Created
Event Type / Details
Group
Server
2020-04-14T19:33:22.405Z
Halo login success
N/A
N/A
Halo user eflinton@training logged into the Halo Portal using browser Chrome on Mac from IP address 73.131.165.145 (USA) using password and YubiKey authentication.
2020-04-14T19:21:14.802Z
Log-based intrusion detection rule matched
eflinton
ip-172-31-18-208.us-east-2.compute.internal
Log-based intrusion detection rule failed_logins matched on Linux server ip-172-31-18-208.us-east-2.compute.internal (13.59.120.253, i-0e0ba5c8c56704d16). (source: DMC Core System (Ubuntu) verified 2020-02-03) - More Details
2020-04-14T18:56:17.497Z
Log-based intrusion detection rule matched
eflinton
ip-172-31-18-208.us-east-2.com
02:00


CloudPassage HALO
Overview
Assets
Issues
Events
Reports
Policies
FIM Scan
Launch New Scan
Rebaseline Server
SCAN DETAILS
Findings Pass Rate: 100%
Scan Type: File Integrity Monitoring
Status: Completed
Policies Used: flinton-FIM test-win
Core System Files (Windows Server 201
Core System Files (Windows Server 201
Completed: 29 hrs ago 2020-08-19 16:24:29 UTC
SERVER DETAILS
Server Name: EC2AMAZ-R830SPP
OS Type: Windows
OS Name: Microsoft Windows Server 2016 Data
OS Version: 10.0.14393
Kernel Version: 10.0
Architecture: 64-bit
NETWORK
Primary IP Address: 172.31.25.106
Connecting IP Address: 3.128.90.32
Hostname: EC2AMAZ-R830SPP
FQDN: EC2AMAZ-R830SPP
Assets / Servers / eflinton / EC2AMAZ-R830SPP / FIM Scan 2020-08-19 16:24:29 UTC
FIM Scan
Scan Results
Criticality
Rule
Added
Missing
Modified
OK
Policy
Pass C:\ 0 0 0 15 flinton-FIM test-win
Pass C:\ads 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\ads\copyoffile.exe 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\ads\file.exe 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\ads\filetocopy.exe 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\ads\file.txt 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\bypassdir 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\data 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\folder 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\folder\evil.dll 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\mimikatz\x64\mimikatz.exe 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\outfolder\outfile.exe 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\path 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\path\to\slmgr.reg 0 0 0 0 Core System Files (Windows Server 2019
Pass C:\program files\common files\microsoft shared 0 0 0 93 Core System Files (Windows Server 2019
Pass C:\program files\common files\system 0 0 0 30 Core System Files (Windows Server 2019
Pass C:\program files\common files\system\ado 0 0 0 6 Core System Files (Windows Server 2019
01:07


Halo Dashboard | Splunk 8.0.3
splunk>enterprise
App: CloudPassage Splunk
Administrator
Messages
Settings
Activity
Help
Find
Halo Dashboard
Halo Event Search
Violation Dashboard
Violations Over Time Dashboard
Violation Distribution
Actor IP - Map
Server IP - Maps
Dashboards
CloudPassage S
Halo Dashboard
Edit
Export
Year to date
Hide Filters
9,950
Critical Violations
19,052
Non-Critical Violations
Top Event Types
name
events
sparkline
Cloud asset configuration rule failed 27867
File Integrity change detected 1157
Halo session timeout 15
API Secret Key Viewed 1
Non-critical
Critical
30,000
20,000
10,000
January 2020
February
March
April
May
_time
Events By Policy
policy_name
count
percent
CloudPassage AWS EC2 Best Practices v1.1 7713 26.689398
CloudPassage AWS EC2 Best Practices v1.0 7411 25.567515
CloudPassage AWS VPC Best Practices v1.0 2590 8.935348
CIS AWS Foundations Benchmark v1.2 2019-07-20 00:16:16-Copy 2080 7.175878
CIS AWS Foundations Benchmark v1.2 2080 7.175878
CIS AWS Foundations Benchmark Customized v1.2 2019-07-11 20:14:02-Copy 2057 7.096529
CIS AWS Foundations Benchmark v1.1 2034 7.017181
Core System Files (Amazon Linux FIM) v1 1157 3.991582
06:34
5/29/2020


Policy Type: Configuration Security (CSM)
Target Asset Type: Servers
Target Platform: Windows
Status: Active
Modified by: eflinton-acme - 20 min ago 2020-04-13 19:04:36 UTC
Created by: eflinton-acme - 4 months ago 2019-12-23 15:39:03 UTC
Description
This policy helps you to verify the security of servers that are hardened according to the consensus guidance put forth by the Center for Internet Security (CIS) document "CIS Microsoft Windows Server 2019 RTM (Release 1809) Benchmark v1.0.0 - 08-30-2019". The policy detects deviations in your servers' configurations from the Benchmark specifications. You may wish to
Group Owner
Acme Foundation
Share with sub-groups
ASSIGNMENT:0 Windows Servers BETA
This policy is automatically assigned to windows Servers based on these criteria:
ASSIGN TO:
OS Version = Windows Server 2012 R2 (os_version 6.3.9600)
+ Add criteria
EXCLUDE:
02:33


portal.cloudpassage.com/halo/dashboard/iaas_dashboard/42378d52259a11eab40
Apps
Calendar
Google Drive
Slack
Jira
CloudPassage Sup...
Statuspage
CloudPassage HALO
Overview
Assets
Issues
Groups
IaaS
Acme Co. 1 1 0 753 296
Acme Foundation 0 0 0 0
App Servers 0 0 0 0
DB Servers 0 1 0 20 30
HQ 0 0 0 0
R&D 0 0 0 0
Sales 0 0 0 0
Web Servers 0 0 0 0
05:46

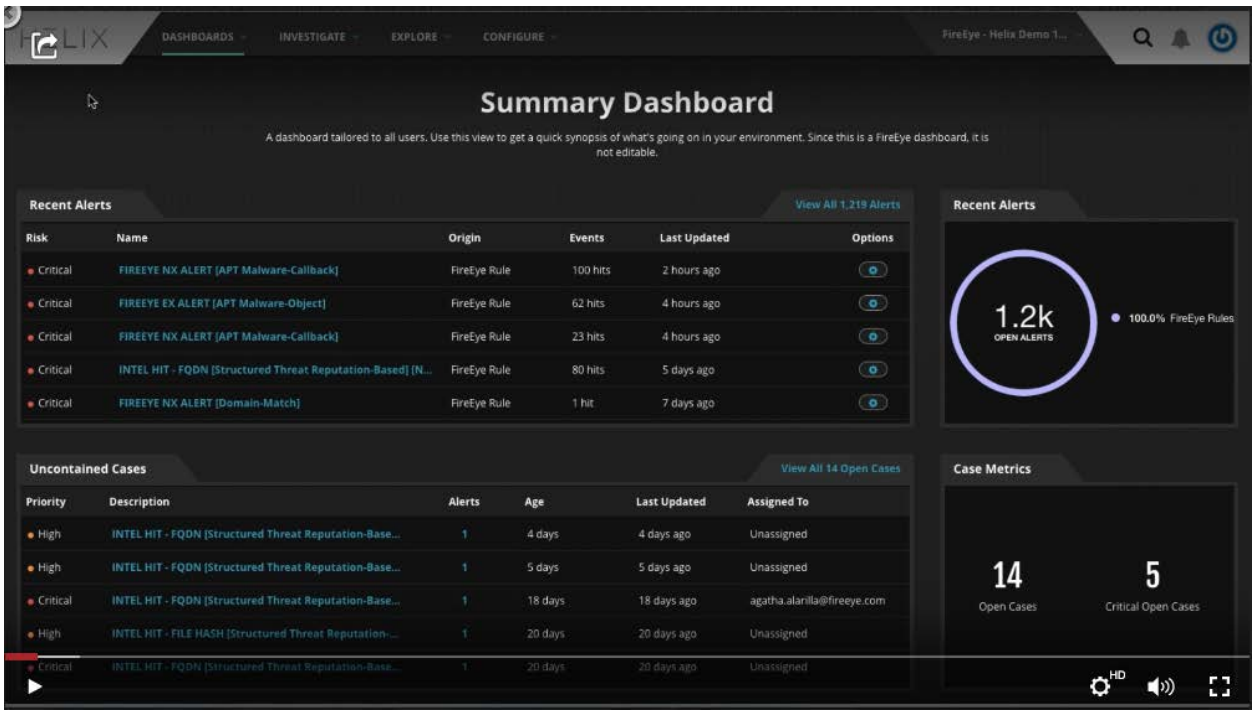
FireEye

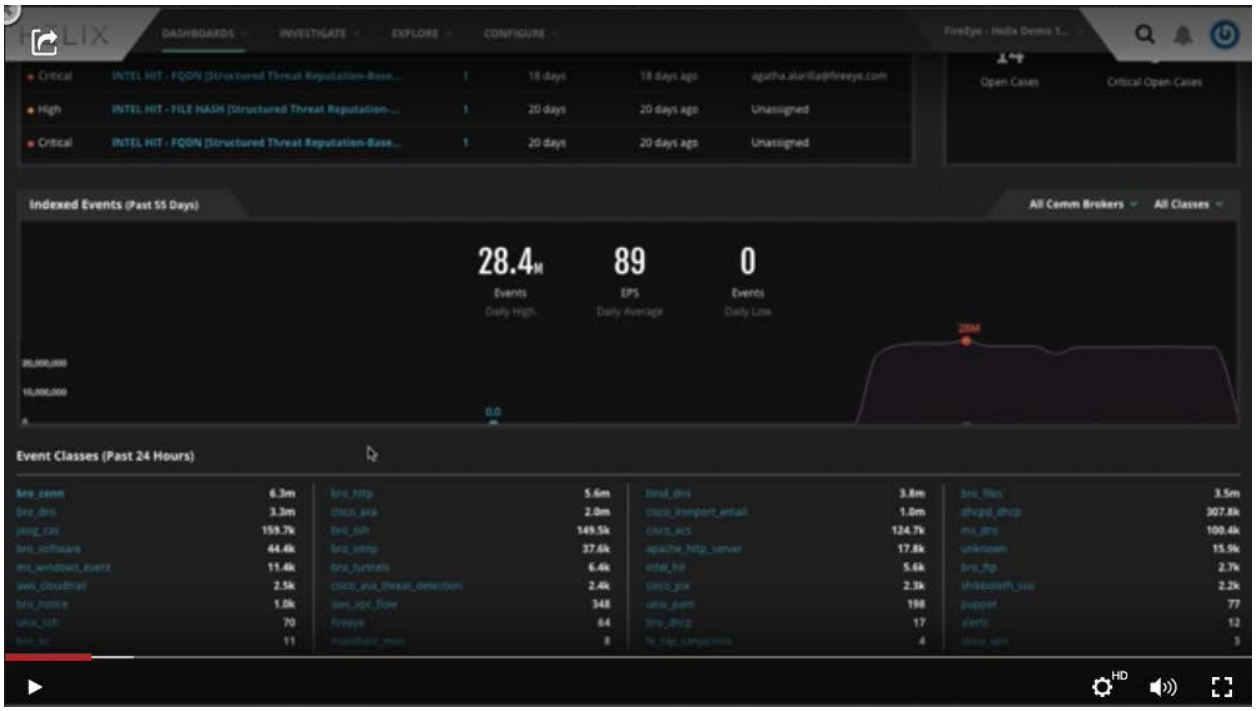
FireEye is a suite of enterprise security products to defend organizations across the biggest threat vectors. It is well known for its incident response and investigation capabilities but has been expanding into cloud security in recent years. FireEye's services provide cloud server workload protection against threats.

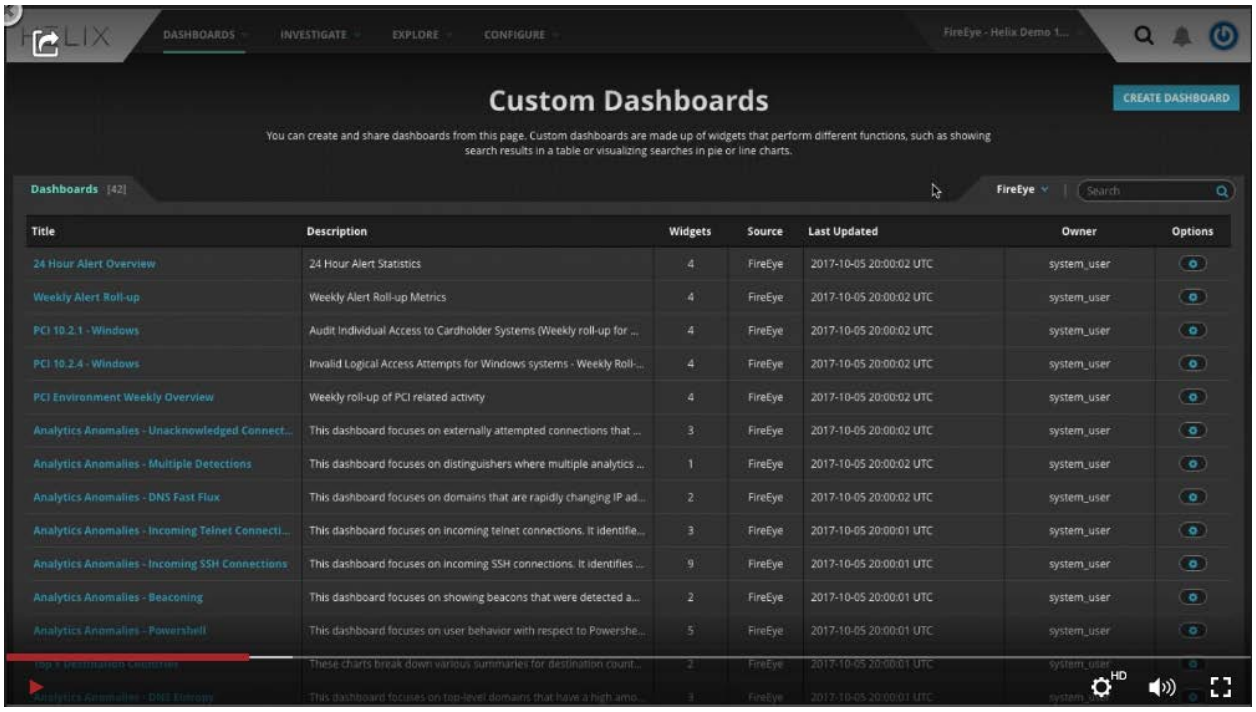
Product demo

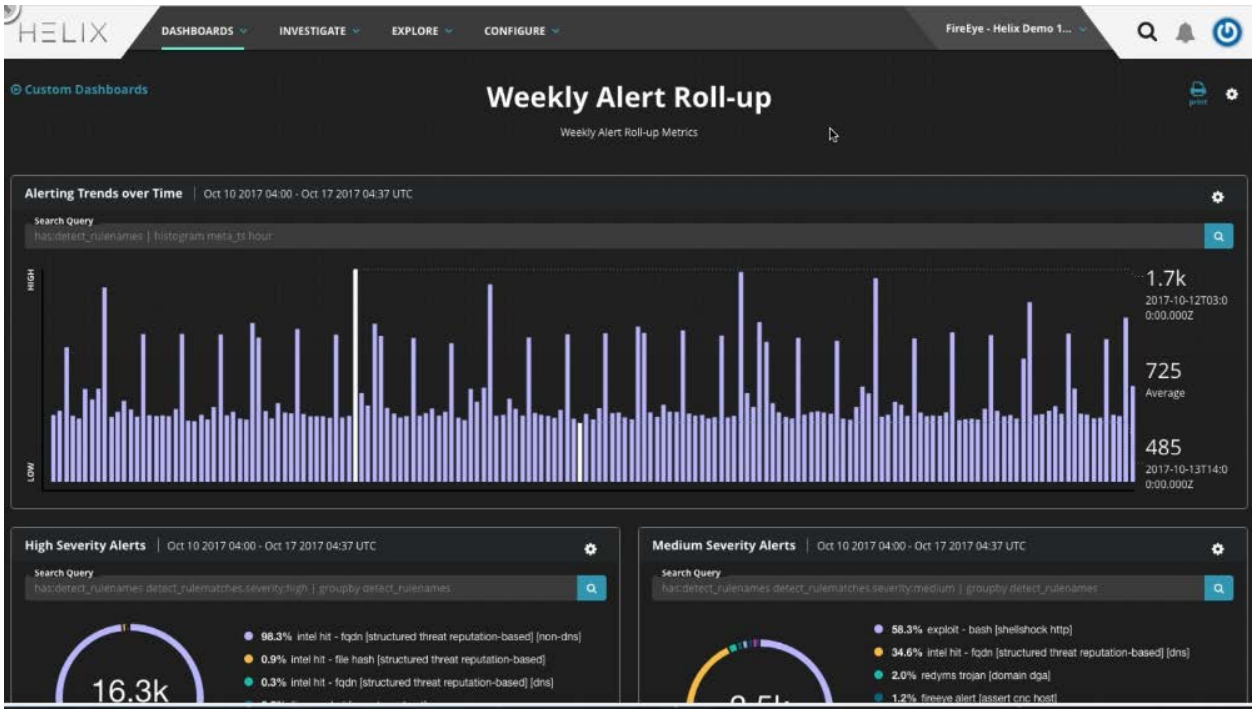
- **Key Values and Differentiators**:
    - FireEye Cloud Security Solution includes cloud versions of FireEye Network Security, Detection On Demand security scanning, and the FireEye Helix security operations platform
    - Virtual network security capability is a keep differentiator, enabling organizations to get full visibility into traffic with deep granularity
    - Threat analytics with Helix data analytics platform
    - Detection on Demand capability ensures users to apply security controls to any AWS cloud service
- **Features include:**
    - Security Information and Event Management (SIEM)
    - Security Analytics
    - Threat Intelligence
    - Workflow and Case Management
        - Assigning cases and linking them manually, not automatically and using Queues to manage alerts/events
    - Security Orchestration, Automation, and Response (SOAR)
    - User and Entity Behavior Analytics
    - Compliance reporting
    - Lightweight deployment

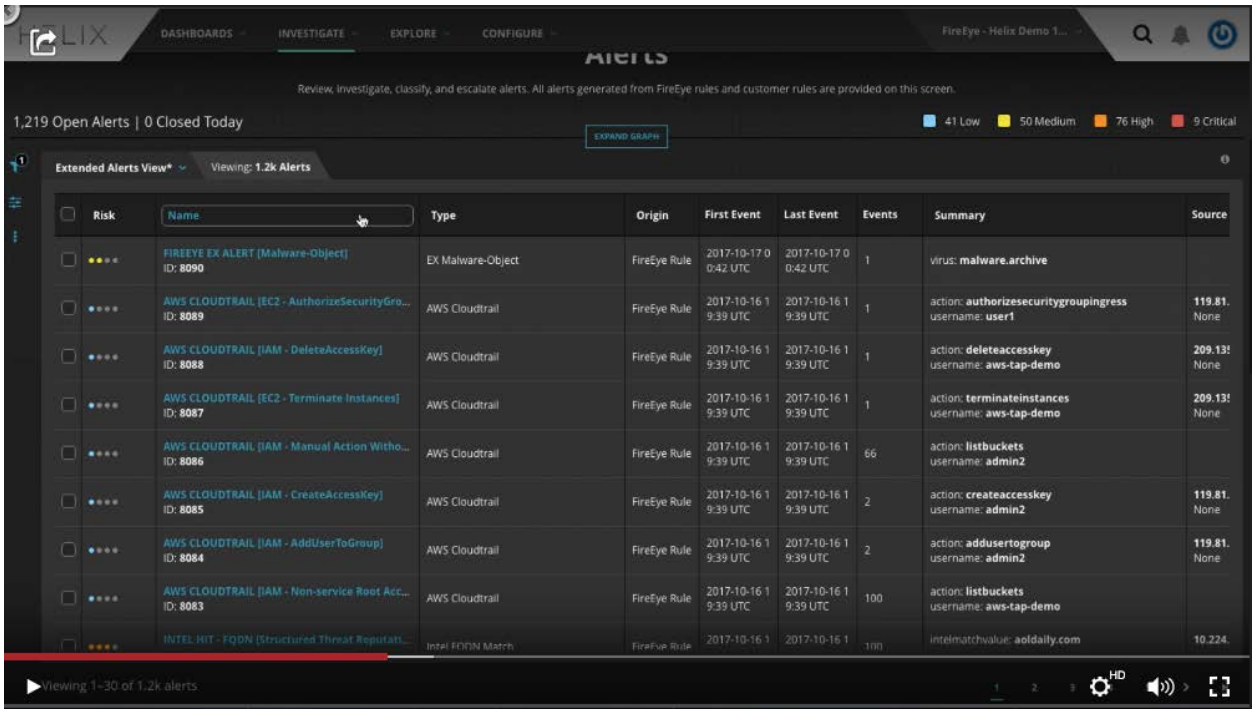
Screenshots of UI:

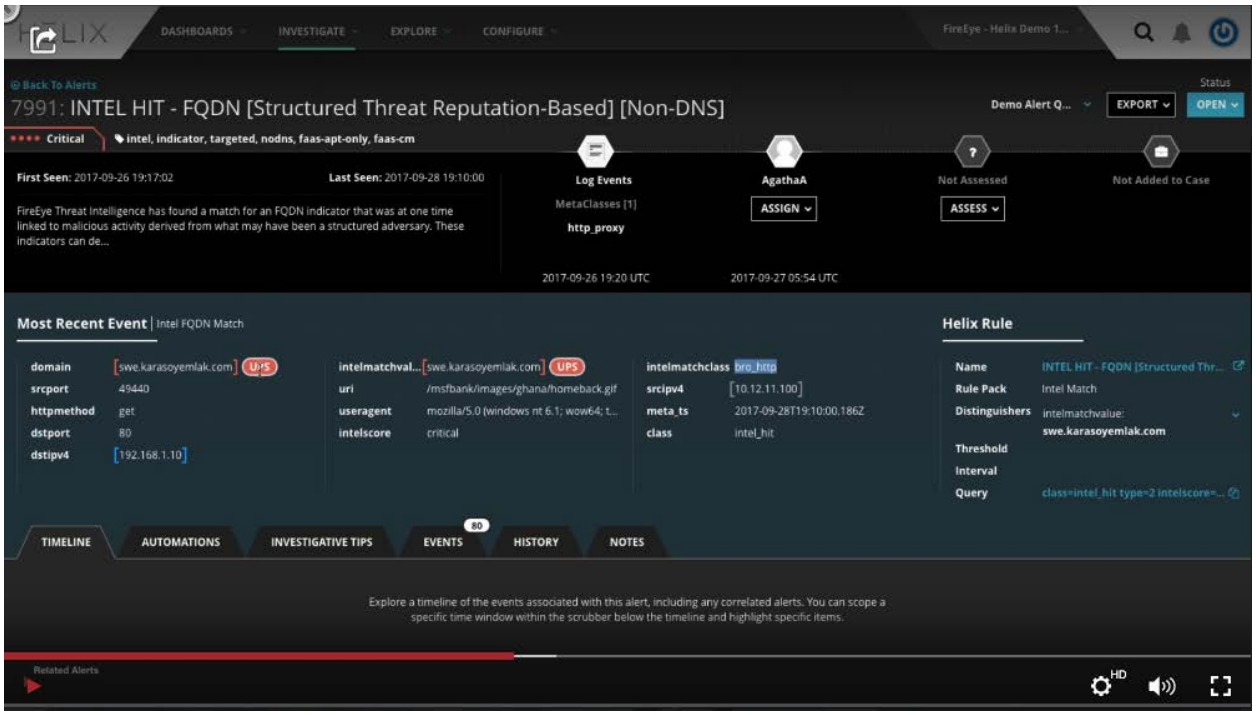

DASHBOARDS
INVESTIGATE
EXPLORE
CONFIGURE
Summary Dashboard
A dashboard tailored to all users. Use this view to get a quick synopsis of what's going on in your environment. Since this is a FireEye dashboard, it is not editable.
Recent Alerts
View All 1,219 Alerts
Risk
Name
Origin
Events
Last Updated
Options
Critical
FIREEYE NX ALERT [APT Malware-Callback]
FireEye Rule
100 hits
2 hours ago
Critical
FIREEYE EX ALERT [APT Malware-Object]
FireEye Rule
62 hits
4 hours ago
Critical
FIREEYE NX ALERT [APT Malware-Callback]
FireEye Rule
23 hits
4 hours ago
Critical
INTEL HIT - FQDN [Structured Threat Reputation-Based] [N...
FireEye Rule
80 hits
5 days ago
Critical
FIREEYE NX ALERT [Domain-Match]
FireEye Rule
1 hit
7 days ago
Recent Alerts
1.2k
OPEN ALERTS
100.0% FireEye Rules
Uncontained Cases
View All 14 Open Cases
Priority
Description
Alerts
Age
Last Updated
Assigned To
High
INTEL HIT - FQDN [Structured Threat Reputation-Base...
1
4 days
4 days ago
Unassigned
High
INTEL HIT - FQDN [Structured Threat Reputation-Base...
1
5 days
5 days ago
Unassigned
Critical
INTEL HIT - FQDN [Structured Threat Reputation-Base...
1
18 days
18 days ago
agatha.alarilla@fireeye.com
High
INTEL HIT - FILE HASH [Structured Threat Reputation-...
1
20 days
20 days ago
Unassigned
Case Metrics
14
Open Cases
5
Critical Open Cases
HD


DASHBOARDS
INVESTIGATE
EXPLORE
CONFIGURE
Critical
INTEL HIT - FQDN [Structured Threat Reputation-Base...
1
18 days
18 days ago
agatha.alarilla@fireeye.com
High
INTEL HIT - FILE HASH [Structured Threat Reputation-...
1
20 days
20 days ago
Unassigned
Critical
INTEL HIT - FQDN [Structured Threat Reputation-Base...
1
20 days
20 days ago
Unassigned
Open Cases
Critical Open Cases
Indexed Events (Past 55 Days)
All Comm Brokers
All Classes
28.4M
Events
Daily High
89
EPS
Daily Average
0
Events
Daily Low
28M
0.0
Event Classes (Past 24 Hours)
bro_conn
6.3m
bro_dns
3.3m
pagg_cpu
159.7k
bro_software
44.4k
ms_windows_event
11.4k
aws_cloudtrail
2.5k
bro_notice
1.0k
unix_stat
70
bro_ssl
11
bro_http
5.6m
cisco_asa
2.0m
bro_ssh
149.5k
bro_smtp
37.6k
bro_tunnels
6.4k
cisco_asa_threat_detection
2.4k
aws_vpc_flow
348
fireeye
64
maxmind_misc
8
bind_dns
3.8m
cisco_ironport_email
1.0m
cisco_acs
124.7k
apache_http_server
17.8k
intel_hit
5.6k
cisco_pix
2.3k
unix_pam
198
bro_dhcp
17
fe_logs_sequences
4
bro_files
3.5m
dhcpd_dhcp
307.8k
ms_dns
100.4k
unknown
15.9k
bro_ftp
2.7k
shibboleth_sso
2.2k
puppet
77
alerts
12
cisco_vpn
3
HD


HELIX
DASHBOARDS
INVESTIGATE
EXPLORE
CONFIGURE
FireEye - Helix Demo 1...
Custom Dashboards
CREATE DASHBOARD
You can create and share dashboards from this page. Custom dashboards are made up of widgets that perform different functions, such as showing search results in a table or visualizing searches in pie or line charts.
Dashboards [42]
FireEye
Search
Title
Description
Widgets
Source
Last Updated
Owner
Options
24 Hour Alert Overview
24 Hour Alert Statistics
4
FireEye
2017-10-05 20:00:02 UTC
system_user
Weekly Alert Roll-up
Weekly Alert Roll-up Metrics
4
FireEye
2017-10-05 20:00:02 UTC
system_user
PCI 10.2.1 - Windows
Audit Individual Access to Cardholder Systems (Weekly roll-up for ...
4
FireEye
2017-10-05 20:00:02 UTC
system_user
PCI 10.2.4 - Windows
Invalid Logical Access Attempts for Windows systems - Weekly Roll-...
4
FireEye
2017-10-05 20:00:02 UTC
system_user
PCI Environment Weekly Overview
Weekly roll-up of PCI related activity
4
FireEye
2017-10-05 20:00:02 UTC
system_user
Analytics Anomalies - Unacknowledged Connect...
This dashboard focuses on externally attempted connections that ...
3
FireEye
2017-10-05 20:00:02 UTC
system_user
Analytics Anomalies - Multiple Detections
This dashboard focuses on distinguishers where multiple analytics ...
1
FireEye
2017-10-05 20:00:02 UTC
system_user
Analytics Anomalies - DNS Fast Flux
This dashboard focuses on domains that are rapidly changing IP ad...
2
FireEye
2017-10-05 20:00:02 UTC
system_user
Analytics Anomalies - Incoming Telnet Connecti...
This dashboard focuses on incoming telnet connections. It identifie...
3
FireEye
2017-10-05 20:00:01 UTC
system_user
Analytics Anomalies - Incoming SSH Connections
This dashboard focuses on incoming SSH connections. It identifies ...
9
FireEye
2017-10-05 20:00:01 UTC
system_user
Analytics Anomalies - Beaconing
This dashboard focuses on showing beacons that were detected a...
2
FireEye
2017-10-05 20:00:01 UTC
system_user
Analytics Anomalies - Powershell
This dashboard focuses on user behavior with respect to Powershe...
5
FireEye
2017-10-05 20:00:01 UTC
system_user
HD


HELIX
DASHBOARDS
INVESTIGATE
EXPLORE
CONFIGURE
FireEye - Helix Demo 1...
Custom Dashboards
Weekly Alert Roll-up
Weekly Alert Roll-up Metrics
Alerting Trends over Time
Oct 10 2017 04:00 - Oct 17 2017 04:37 UTC
Search Query
has:detect_rulenames | histogram meta_ts hour
HIGH
LOW
1.7k
2017-10-12T03:00:00.000Z
725
Average
485
2017-10-13T14:00:00.000Z
High Severity Alerts
Oct 10 2017 04:00 - Oct 17 2017 04:37 UTC
Search Query
has:detect_rulenames detect_rulematches.severity:high | groupby detect_rulenames
16.3k
98.3% intel hit - fqdn [structured threat reputation-based] [non-dns]
0.9% intel hit - file hash [structured threat reputation-based]
0.3% intel hit - fqdn [structured threat reputation-based] [dns]
Medium Severity Alerts
Oct 10 2017 04:00 - Oct 17 2017 04:37 UTC
Search Query
has:detect_rulenames detect_rulematches.severity:medium | groupby detect_rulenames
58.3% exploit - bash [shellshock http]
34.6% intel hit - fqdn [structured threat reputation-based] [dns]
2.0% redyms trojan [domain dga]
1.2% fireeye alert [assert cnc host]





LaceWork

Lackwork is a cloud workload security and compliance solution that is well suited for organizations looking for a visual approach to cloud security. Comprehensive, continuous

end-to-end security for workloads, containers, users, Kubernetes, and cloud accounts running in multi-cloud environments.

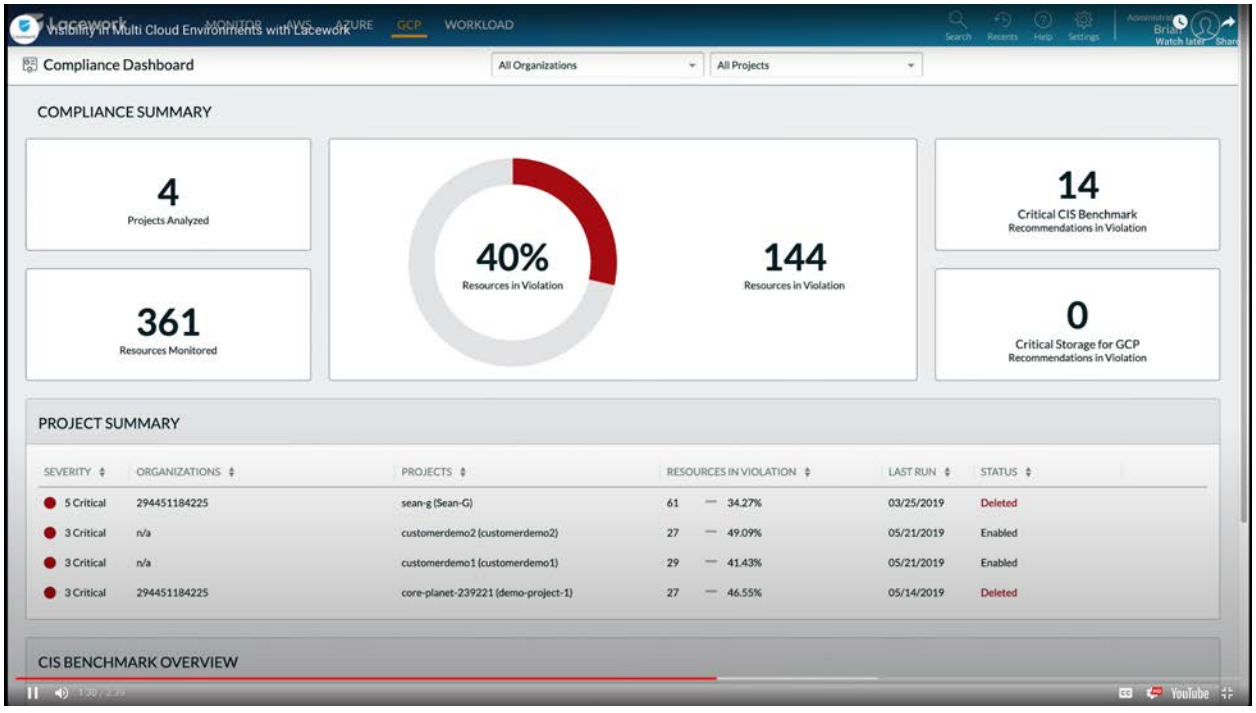
Product demos:

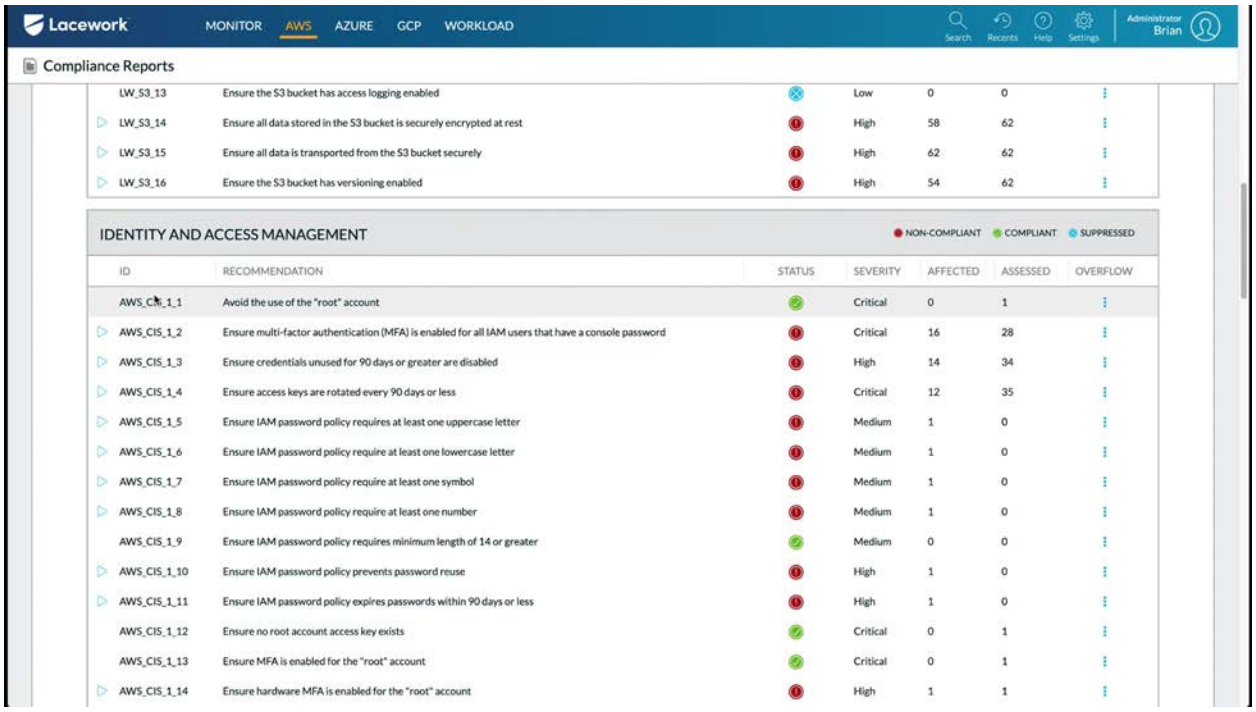
- Visibility in Multi Cloud Environments
- Compliance & Auditing
- Anomaly Detection & Investigation (based on previous behavior)
- Container Security
- Kubernetes Orchestration Security

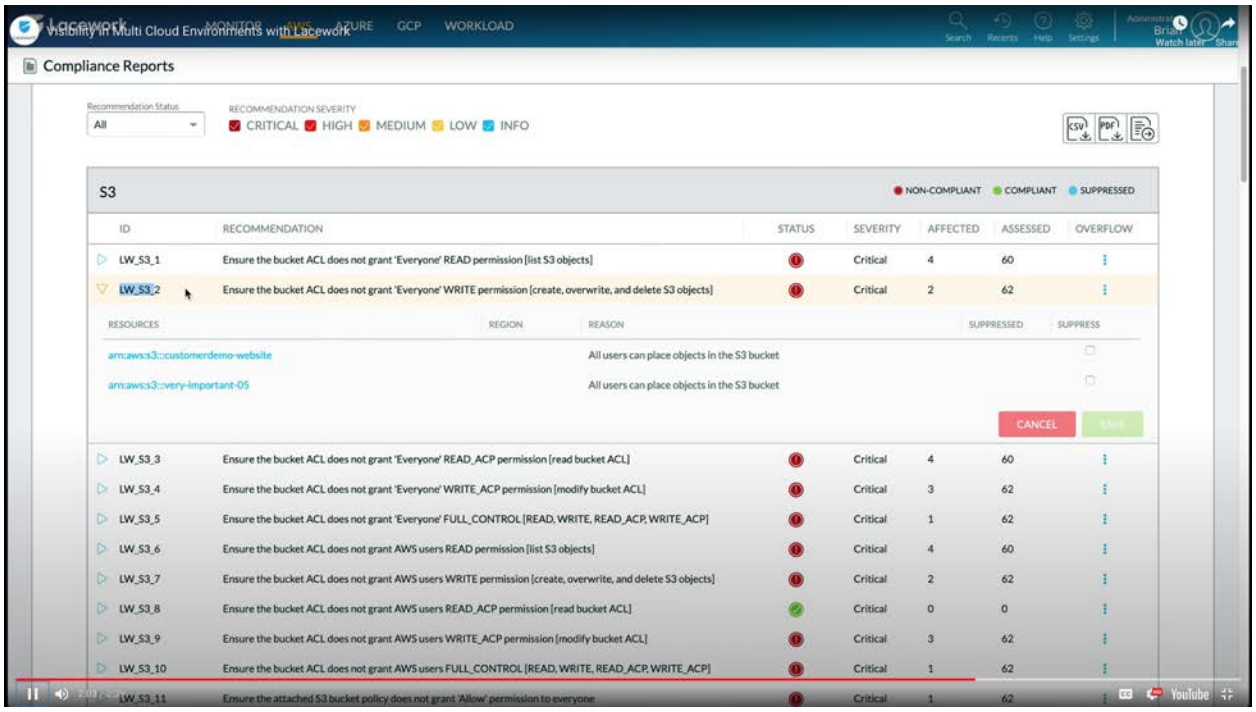
- **Key Values and Differentiators**:
    - The Polygraph feature, provides a visual representation of relationships across account roles, workloads and APIs in an attempt to deliver better context
    - Provides monitoring of cloud workloads for compliance and security concerns
    - Automated workload intrusion detection capability that is powered by machine learning to help reduce risks
    - Configuration best practices support and guidance
- **Features include:**
    - Configuration & audit control
    - Workload and container security
    - Advanced threat detection
    - Vulnerability monitoring
    - DevSecOps optimizations
    - Visualize interactions and communication between cloud entities
    - Quickly review incidents at any level of detail
    - Accurate alerts
        - Summarized alerts provide visibility and context
        - Aggregation, risk score, links and additional info with each alert

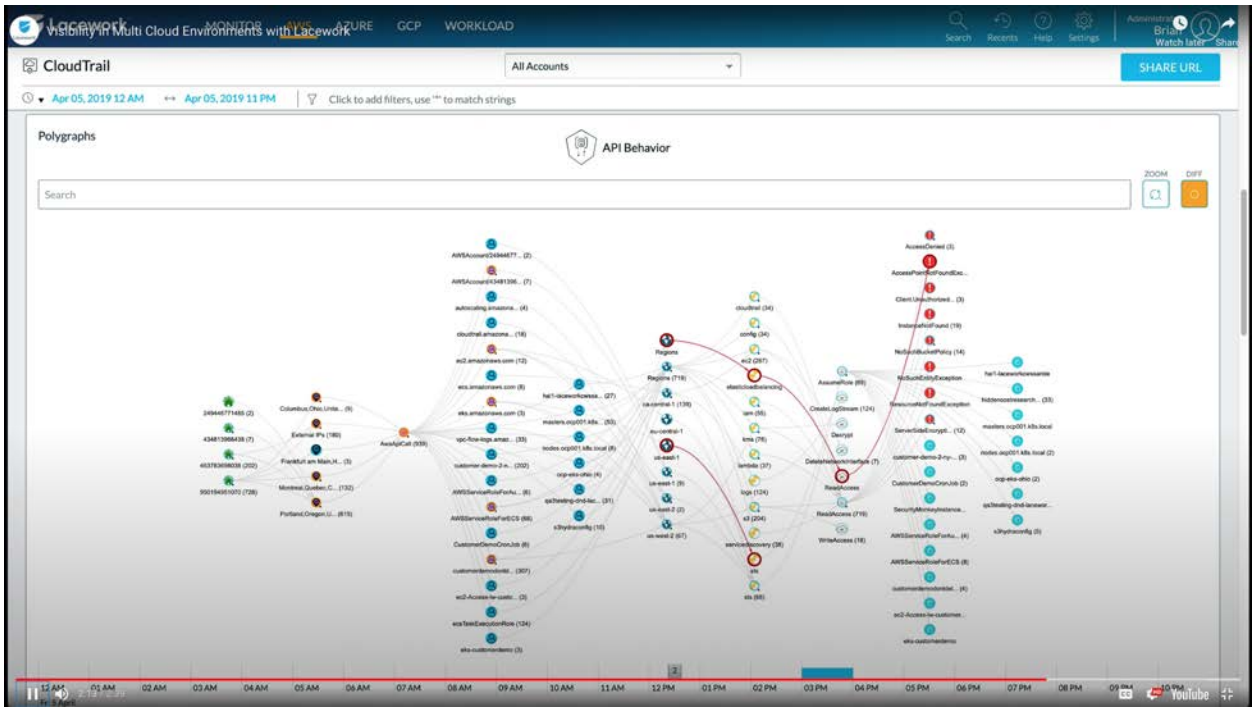
Screenshots of UI:

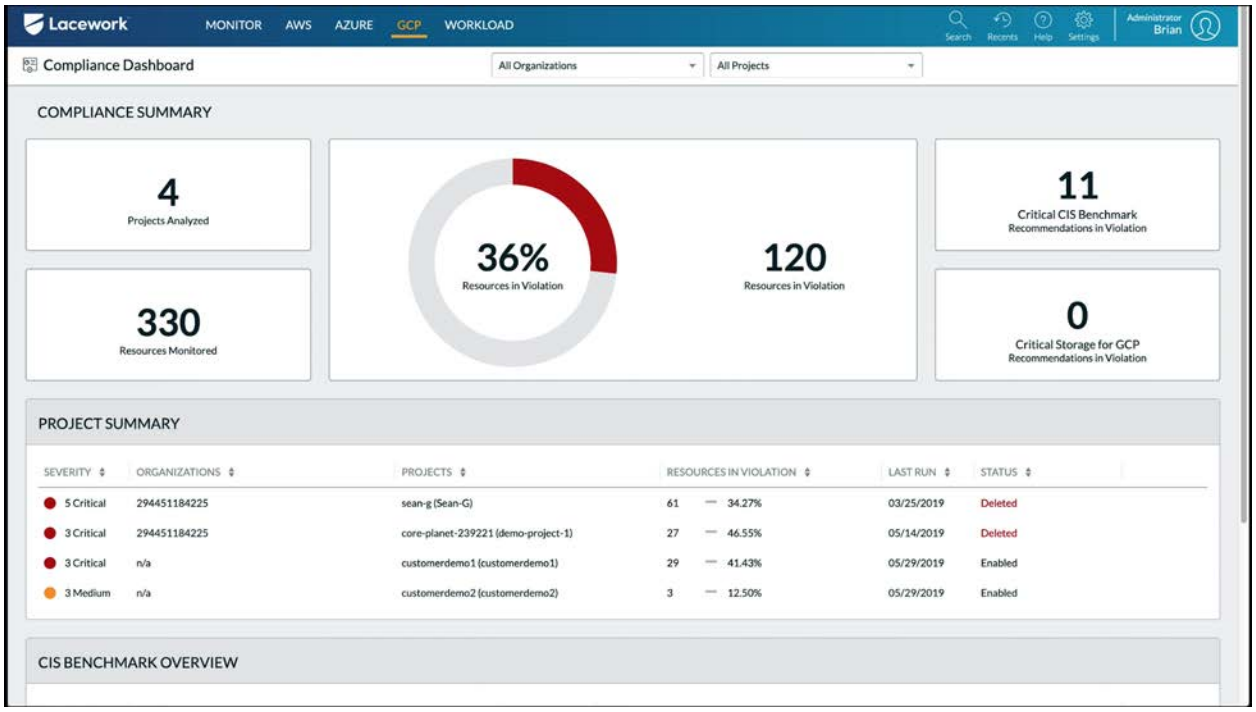

Visibility in Multi Cloud Environments with Lacework
Applications
SHARE URL
Polygraphs
Application Communication
Application Launch
Insider Behavior
Search

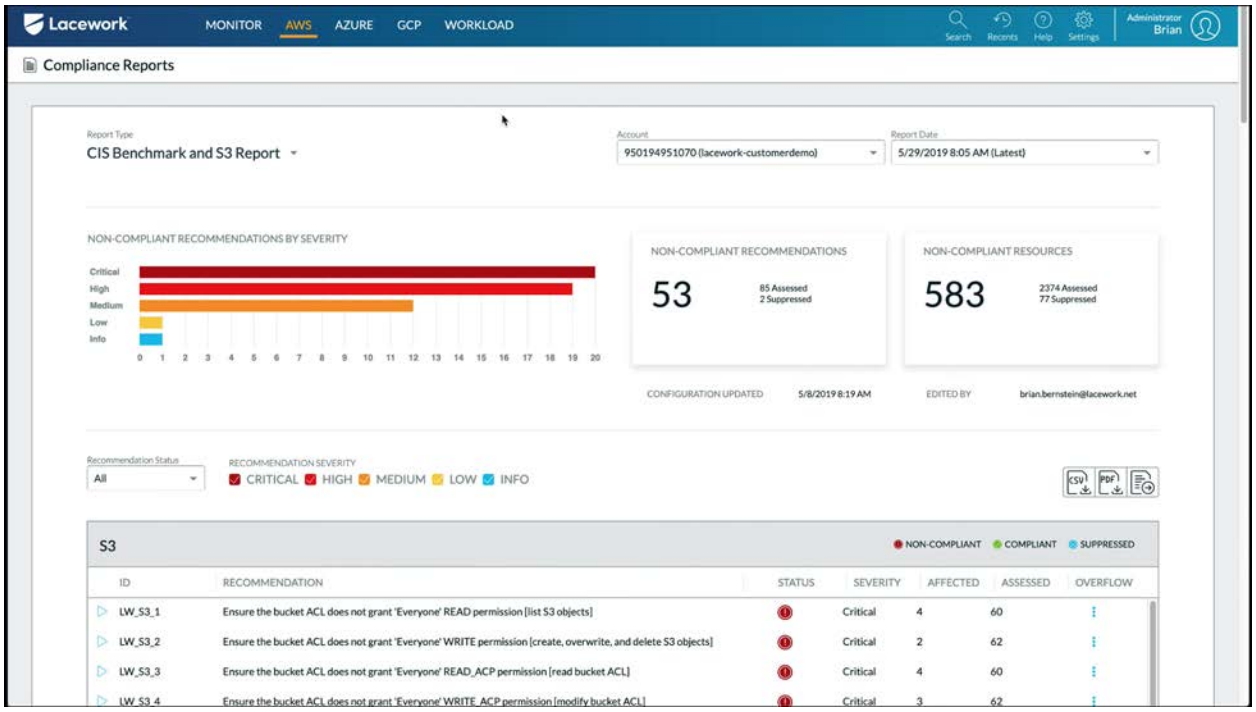

Visibility in Multi Cloud Environments with Lacework
Compliance Dashboard
All Organizations
All Projects
COMPLIANCE SUMMARY
4
Projects Analyzed
40%
Resources in Violation
144
Resources in Violation
14
Critical CIS Benchmark Recommendations in Violation
361
Resources Monitored
0
Critical Storage for GCP Recommendations in Violation
PROJECT SUMMARY
SEVERITY
ORGANIZATIONS
PROJECTS
RESOURCES IN VIOLATION
LAST RUN
STATUS
5 Critical 294451184225 sean-g (Sean-G) 61 — 34.27% 03/25/2019 Deleted
3 Critical n/a customerdemo2 (customerdemo2) 27 — 49.09% 05/21/2019 Enabled
3 Critical n/a customerdemo1 (customerdemo1) 29 — 41.43% 05/21/2019 Enabled
3 Critical 294451184225 core-planet-239221 (demo-project-1) 27 — 46.55% 05/14/2019 Deleted
CIS BENCHMARK OVERVIEW

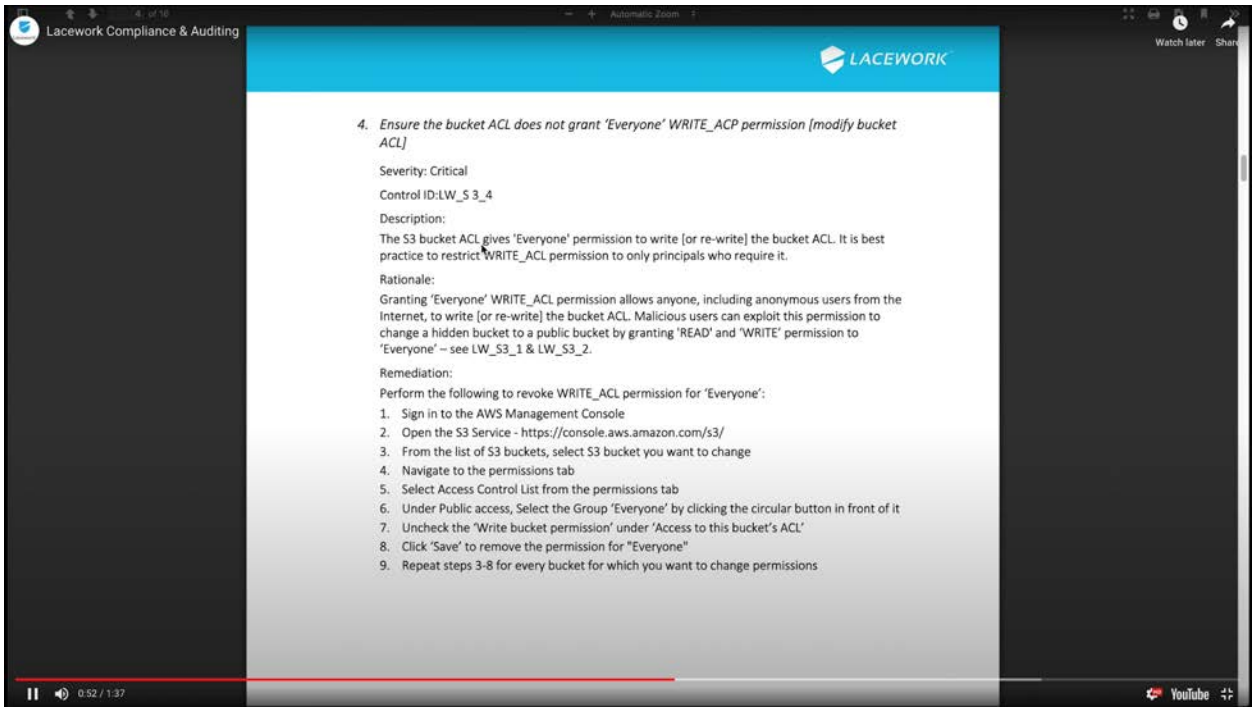

Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Administrator
Brian
Compliance Reports
LW_S3_13 Ensure the S3 bucket has access logging enabled Low 0 0
LW_S3_14 Ensure all data stored in the S3 bucket is securely encrypted at rest High 58 62
LW_S3_15 Ensure all data is transported from the S3 bucket securely High 62 62
LW_S3_16 Ensure the S3 bucket has versioning enabled High 54 62
IDENTITY AND ACCESS MANAGEMENT
NON-COMPLIANT
COMPLIANT
SUPPRESSED
ID
RECOMMENDATION
STATUS
SEVERITY
AFFECTED
ASSESSED
OVERFLOW
AWS_CIS_1_1 Avoid the use of the "root" account Critical 0 1
AWS_CIS_1_2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password Critical 16 28
AWS_CIS_1_3 Ensure credentials unused for 90 days or greater are disabled High 14 34
AWS_CIS_1_4 Ensure access keys are rotated every 90 days or less Critical 12 35
AWS_CIS_1_5 Ensure IAM password policy requires at least one uppercase letter Medium 1 0
AWS_CIS_1_6 Ensure IAM password policy require at least one lowercase letter Medium 1 0
AWS_CIS_1_7 Ensure IAM password policy require at least one symbol Medium 1 0
AWS_CIS_1_8 Ensure IAM password policy require at least one number Medium 1 0
AWS_CIS_1_9 Ensure IAM password policy requires minimum length of 14 or greater Medium 0 0
AWS_CIS_1_10 Ensure IAM password policy prevents password reuse High 1 0
AWS_CIS_1_11 Ensure IAM password policy expires passwords within 90 days or less High 1 0
AWS_CIS_1_12 Ensure no root account access key exists Critical 0 1
AWS_CIS_1_13 Ensure MFA is enabled for the "root" account Critical 0 1
AWS_CIS_1_14 Ensure hardware MFA is enabled for the "root" account High 1 1

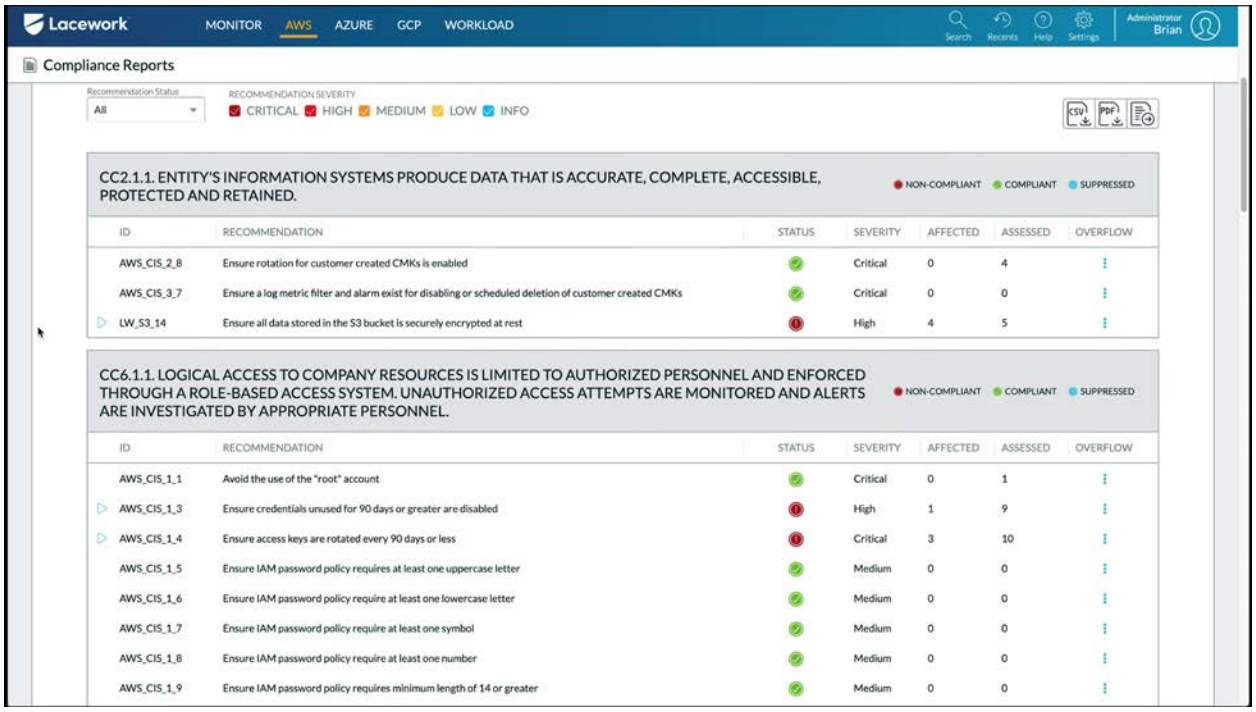

Visibility in Multi Cloud Environments with Lacework
Watch later
Share
Compliance Reports
Recommendation Status
All
RECOMMENDATION SEVERITY
CRITICAL HIGH MEDIUM LOW INFO
S3
NON-COMPLIANT
COMPLIANT
SUPPRESSED
ID
RECOMMENDATION
STATUS
SEVERITY
AFFECTED
ASSESSED
OVERFLOW
LW_S3_1 Ensure the bucket ACL does not grant 'Everyone' READ permission [list S3 objects] Critical 4 60
LW_S3_2 Ensure the bucket ACL does not grant 'Everyone' WRITE permission [create, overwrite, and delete S3 objects] Critical 2 62
RESOURCES
REGION
REASON
SUPPRESSED
SUPPRESS
arn:aws:s3:::customerdemo-website All users can place objects in the S3 bucket
arn:aws:s3:::very-important-05 All users can place objects in the S3 bucket
CANCEL
LW_S3_3 Ensure the bucket ACL does not grant 'Everyone' READ_ACP permission [read bucket ACL] Critical 4 60
LW_S3_4 Ensure the bucket ACL does not grant 'Everyone' WRITE_ACP permission [modify bucket ACL] Critical 3 62
LW_S3_5 Ensure the bucket ACL does not grant 'Everyone' FULL_CONTROL [READ, WRITE, READ_ACP, WRITE_ACP] Critical 1 62
LW_S3_6 Ensure the bucket ACL does not grant AWS users READ permission [list S3 objects] Critical 4 60
LW_S3_7 Ensure the bucket ACL does not grant AWS users WRITE permission [create, overwrite, and delete S3 objects] Critical 2 62
LW_S3_8 Ensure the bucket ACL does not grant AWS users READ_ACP permission [read bucket ACL] Critical 0 0
LW_S3_9 Ensure the bucket ACL does not grant AWS users WRITE_ACP permission [modify bucket ACL] Critical 3 62
LW_S3_10 Ensure the bucket ACL does not grant AWS users FULL_CONTROL [READ, WRITE, READ_ACP, WRITE_ACP] Critical 1 62
LW_S3_11 Ensure the attached S3 bucket policy does not grant 'Allow' permission to everyone Critical 1 62
YouTube

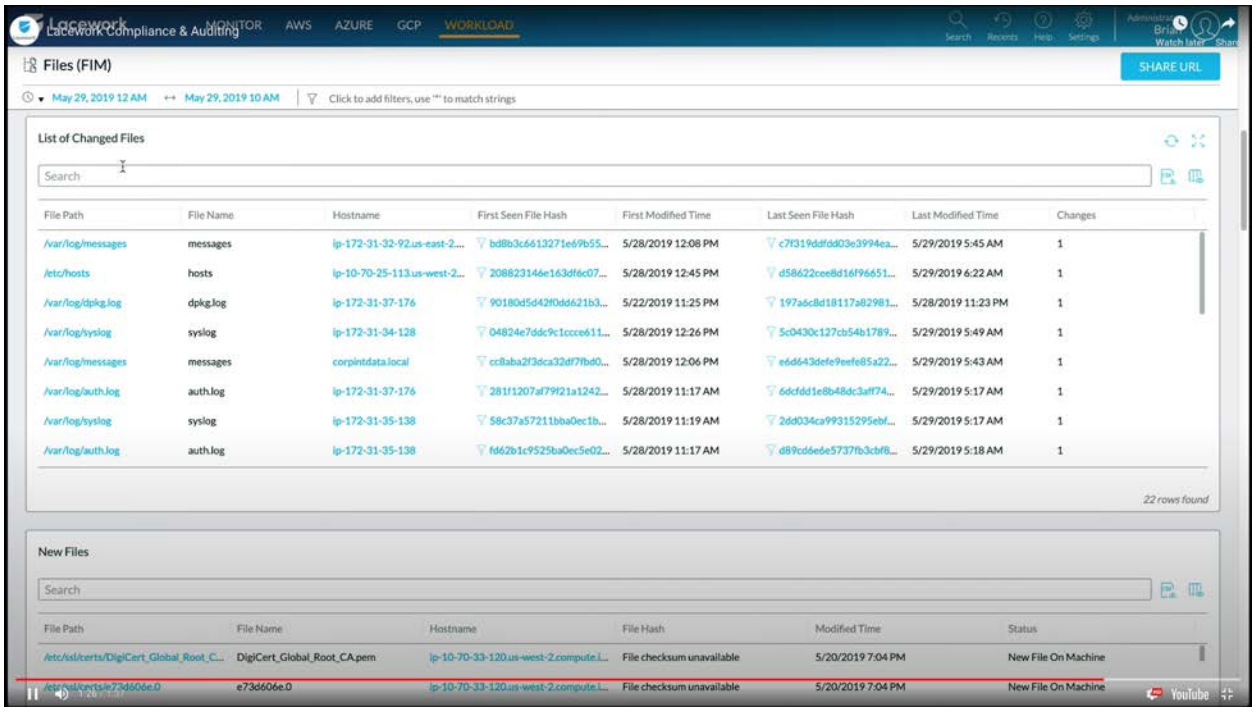

Visibility in Multi Cloud Environments with Lacework
CloudTrail
All Accounts
SHARE URL
Apr 05, 2019 12 AM
Apr 05, 2019 11 PM
Click to add filters, use '*' to match strings
Polygraphs
API Behavior
Search

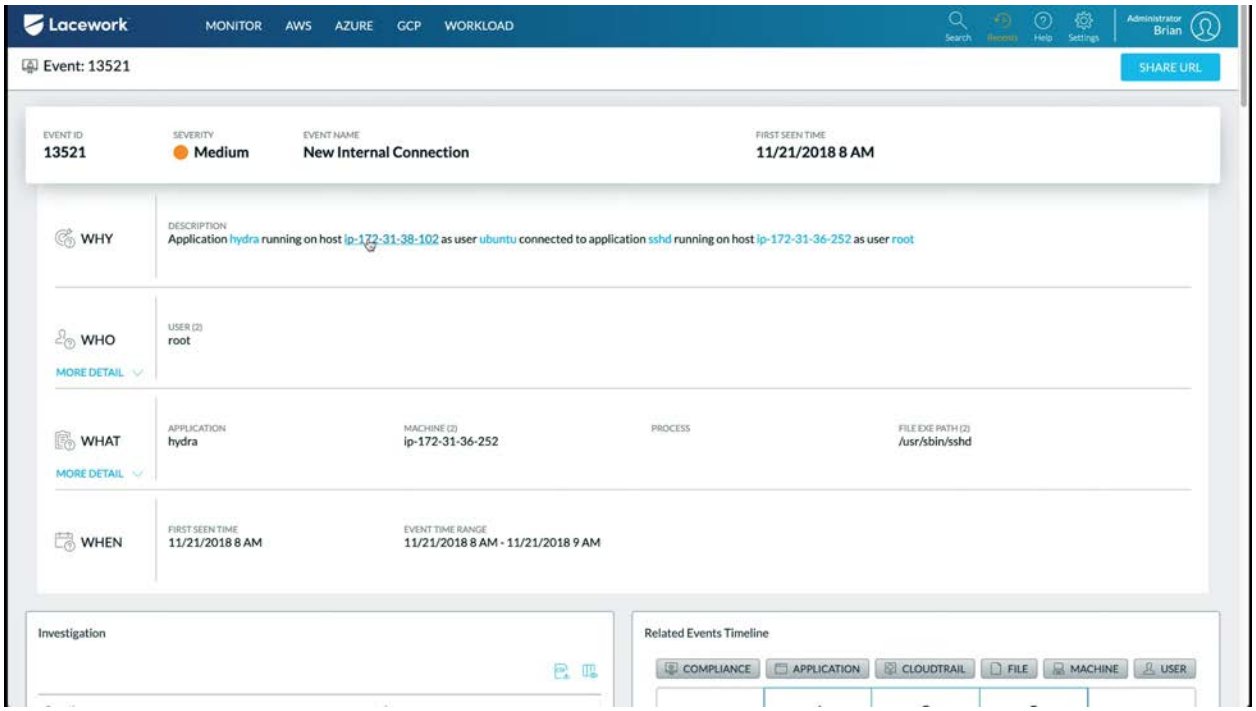

Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Administrator
Brian
Compliance Dashboard
All Organizations
All Projects
COMPLIANCE SUMMARY
4
Projects Analyzed
330
Resources Monitored
36%
Resources in Violation
120
Resources in Violation
11
Critical CIS Benchmark
Recommendations in Violation
0
Critical Storage for GCP
Recommendations in Violation
PROJECT SUMMARY
SEVERITY
ORGANIZATIONS
PROJECTS
RESOURCES IN VIOLATION
LAST RUN
STATUS
5 Critical 294451184225 sean-g (Sean-G) 61 — 34.27% 03/25/2019 Deleted
3 Critical 294451184225 core-planet-239221 (demo-project-1) 27 — 46.55% 05/14/2019 Deleted
3 Critical n/a customerdemo1 (customerdemo1) 29 — 41.43% 05/29/2019 Enabled
3 Medium n/a customerdemo2 (customerdemo2) 3 — 12.50% 05/29/2019 Enabled
CIS BENCHMARK OVERVIEW

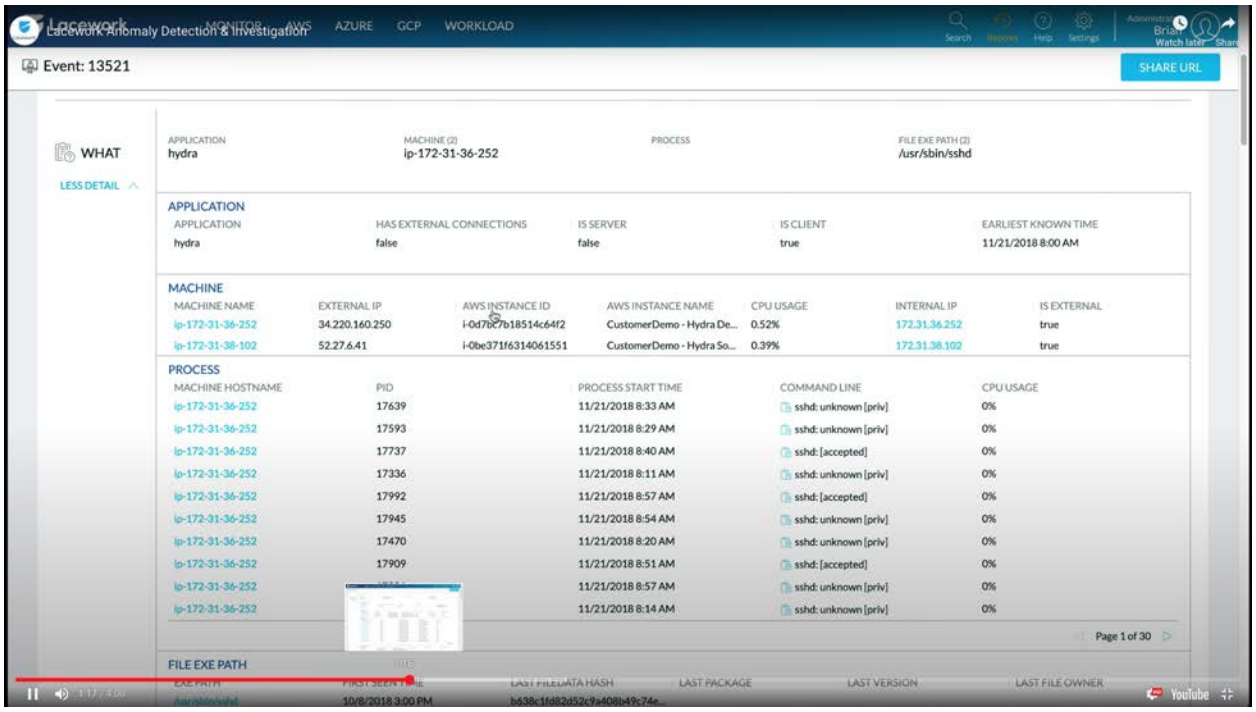

Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Administrator
Brian
Compliance Reports
Report Type
CIS Benchmark and S3 Report
Account
950194951070 (lacework-customerdemo)
Report Date
5/29/2019 8:05 AM (Latest)
NON-COMPLIANT RECOMMENDATIONS BY SEVERITY
Critical
High
Medium
Low
Info
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
NON-COMPLIANT RECOMMENDATIONS
53
85 Assessed
2 Suppressed
NON-COMPLIANT RESOURCES
583
2374 Assessed
77 Suppressed
CONFIGURATION UPDATED
5/8/2019 8:19 AM
EDITED BY
brian.bernstein@lacework.net
Recommendation Status
All
RECOMMENDATION SEVERITY
CRITICAL HIGH MEDIUM LOW INFO
CSV
PDF
S3
NON-COMPLIANT
COMPLIANT
SUPPRESSED
ID
RECOMMENDATION
STATUS
SEVERITY
AFFECTED
ASSESSED
OVERFLOW
LW_S3_1
Ensure the bucket ACL does not grant 'Everyone' READ permission [list S3 objects]
Critical
4
60
LW_S3_2
Ensure the bucket ACL does not grant 'Everyone' WRITE permission [create, overwrite, and delete S3 objects]
Critical
2
62
LW_S3_3
Ensure the bucket ACL does not grant 'Everyone' READ_ACP permission [read bucket ACL]
Critical
4
60
LW_S3_4
Ensure the bucket ACL does not grant 'Everyone' WRITE_ACP permission [modify bucket ACL]
Critical
3
62

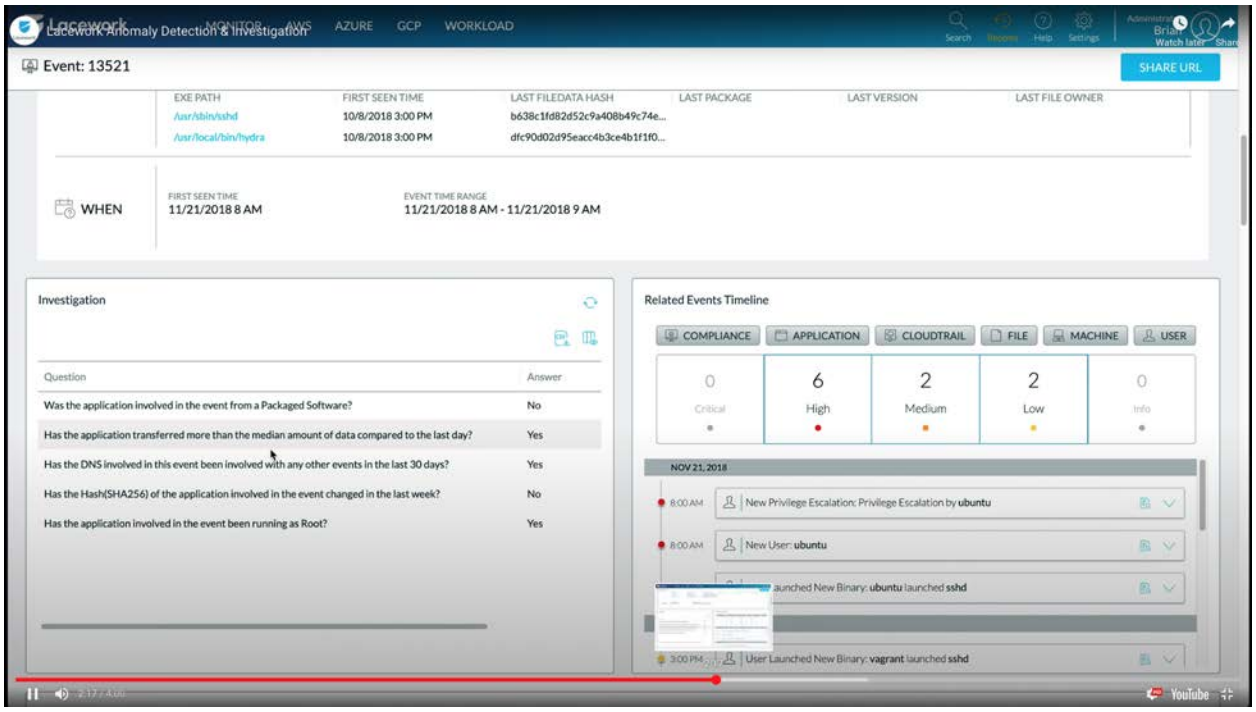

Lacework Compliance & Auditing
Watch later
LACEWORK
4. Ensure the bucket ACL does not grant 'Everyone' WRITE_ACP permission [modify bucket ACL]
Severity: Critical
Control ID:LW_S 3_4
Description:
The S3 bucket ACL gives 'Everyone' permission to write [or re-write] the bucket ACL. It is best practice to restrict WRITE_ACL permission to only principals who require it.
Rationale:
Granting 'Everyone' WRITE_ACL permission allows anyone, including anonymous users from the Internet, to write [or re-write] the bucket ACL. Malicious users can exploit this permission to change a hidden bucket to a public bucket by granting 'READ' and 'WRITE' permission to 'Everyone' – see LW_S3_1 & LW_S3_2.
Remediation:
Perform the following to revoke WRITE_ACL permission for 'Everyone':
1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. From the list of S3 buckets, select S3 bucket you want to change
4. Navigate to the permissions tab
5. Select Access Control List from the permissions tab
6. Under Public access, Select the Group 'Everyone' by clicking the circular button in front of it
7. Uncheck the 'Write bucket permission' under 'Access to this bucket's ACL'
8. Click 'Save' to remove the permission for "Everyone"
9. Repeat steps 3-8 for every bucket for which you want to change permissions
0:52 / 1:37
YouTube

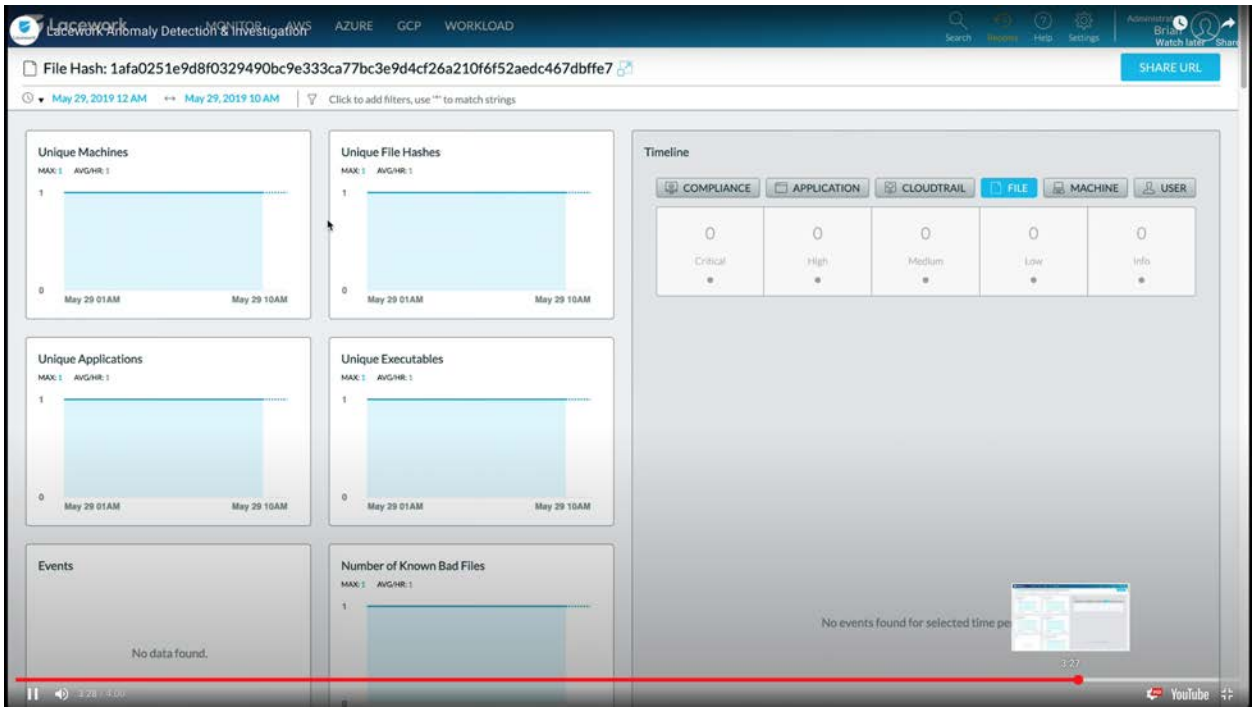

Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Administrator
Brian
Compliance Reports
Recommendation Status
All
RECOMMENDATION SEVERITY
CRITICAL HIGH MEDIUM LOW INFO
CSV
PDF
CC2.1.1. ENTITY'S INFORMATION SYSTEMS PRODUCE DATA THAT IS ACCURATE, COMPLETE, ACCESSIBLE, PROTECTED AND RETAINED.
NON-COMPLIANT
COMPLIANT
SUPPRESSED
ID
RECOMMENDATION
STATUS
SEVERITY
AFFECTED
ASSESSED
OVERFLOW
AWS_CIS_2_8
Ensure rotation for customer created CMKs is enabled
Critical
0
4
AWS_CIS_3_7
Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs
Critical
0
0
LW_S3_14
Ensure all data stored in the S3 bucket is securely encrypted at rest
High
4
5
CC6.1.1. LOGICAL ACCESS TO COMPANY RESOURCES IS LIMITED TO AUTHORIZED PERSONNEL AND ENFORCED THROUGH A ROLE-BASED ACCESS SYSTEM. UNAUTHORIZED ACCESS ATTEMPTS ARE MONITORED AND ALERTS ARE INVESTIGATED BY APPROPRIATE PERSONNEL.
NON-COMPLIANT
COMPLIANT
SUPPRESSED
ID
RECOMMENDATION
STATUS
SEVERITY
AFFECTED
ASSESSED
OVERFLOW
AWS_CIS_1_1
Avoid the use of the "root" account
Critical
0
1
AWS_CIS_1_3
Ensure credentials unused for 90 days or greater are disabled
High
1
9
AWS_CIS_1_4
Ensure access keys are rotated every 90 days or less
Critical
3
10
AWS_CIS_1_5
Ensure IAM password policy requires at least one uppercase letter
Medium
0
0
AWS_CIS_1_6
Ensure IAM password policy require at least one lowercase letter
Medium
0
0
AWS_CIS_1_7
Ensure IAM password policy require at least one symbol
Medium
0
0
AWS_CIS_1_8
Ensure IAM password policy require at least one number
Medium
0
0
AWS_CIS_1_9
Ensure IAM password policy requires minimum length of 14 or greater
Medium
0
0

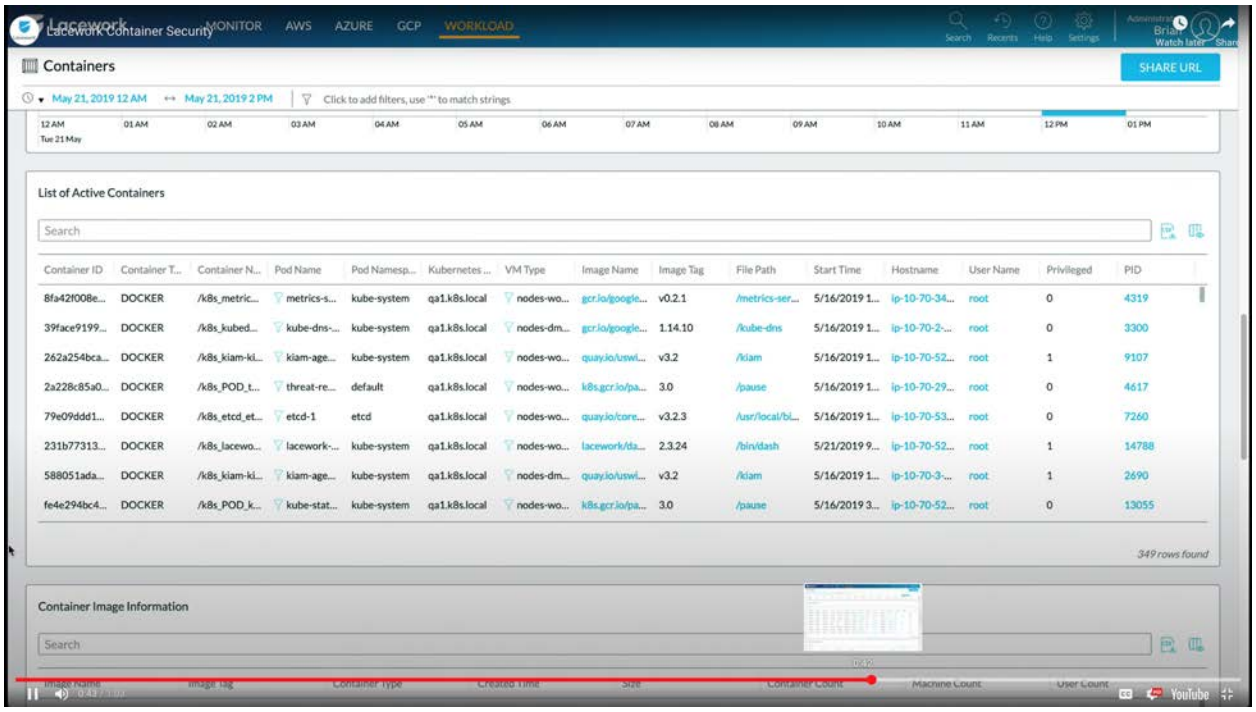

Lacework
Lacework Compliance & Auditing
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Watch later
Share
Files (FIM)
SHARE URL
May 29, 2019 12 AM
May 29, 2019 10 AM
Click to add filters, use "*" to match strings
List of Changed Files
Search
File Path
File Name
Hostname
First Seen File Hash
First Modified Time
Last Seen File Hash
Last Modified Time
Changes
/var/log/messages
messages
ip-172-31-32-92.us-east-2....
bd8b3c6613271e6f9b55...
5/28/2019 12:08 PM
c7f319ddfdd03e3994ea...
5/29/2019 5:45 AM
1
/etc/hosts
hosts
ip-10-70-25-113.us-west-2...
208823146e163df6c07...
5/28/2019 12:45 PM
d58622cee8d16f96651...
5/29/2019 6:22 AM
1
/var/log/dpkg.log
dpkg.log
ip-172-31-37-176
90180d5d42f0dd621b3...
5/22/2019 11:25 PM
197a6c8d18117a82981...
5/28/2019 11:23 PM
1
/var/log/syslog
syslog
ip-172-31-34-128
04824e7ddc9c1cccce611...
5/28/2019 12:26 PM
5c0430c127cb54b1789...
5/29/2019 5:49 AM
1
/var/log/messages
messages
corpintdata.local
cc8aba2f3dca32df7fbd0...
5/28/2019 12:06 PM
e6d643defe9eefe85a22...
5/29/2019 5:43 AM
1
/var/log/auth.log
auth.log
ip-172-31-37-176
281f1207af79f21a1242...
5/28/2019 11:17 AM
6dcfdd1e8b48dc3aff74...
5/29/2019 5:17 AM
1
/var/log/syslog
syslog
ip-172-31-35-138
58c37a57211bba0ec1b...
5/28/2019 11:19 AM
2dd034ca99315295ebf...
5/29/2019 5:17 AM
1
/var/log/auth.log
auth.log
ip-172-31-35-138
fd62b1c9525ba0ec5e02...
5/28/2019 11:17 AM
d89cd6e6e5737fb3cbf8...
5/29/2019 5:18 AM
1
22 rows found
New Files
Search
File Path
File Name
Hostname
File Hash
Modified Time
Status
/etc/ssl/certs/DigiCert_Global_Root_C...
DigiCert_Global_Root_CA.pem
ip-10-70-33-120.us-west-2.compute.i...
File checksum unavailable
5/20/2019 7:04 PM
New File On Machine
/etc/ssl/certs/e73d606e.0
e73d606e.0
ip-10-70-33-120.us-west-2.compute.i...
File checksum unavailable
5/20/2019 7:04 PM
New File On Machine
YouTube

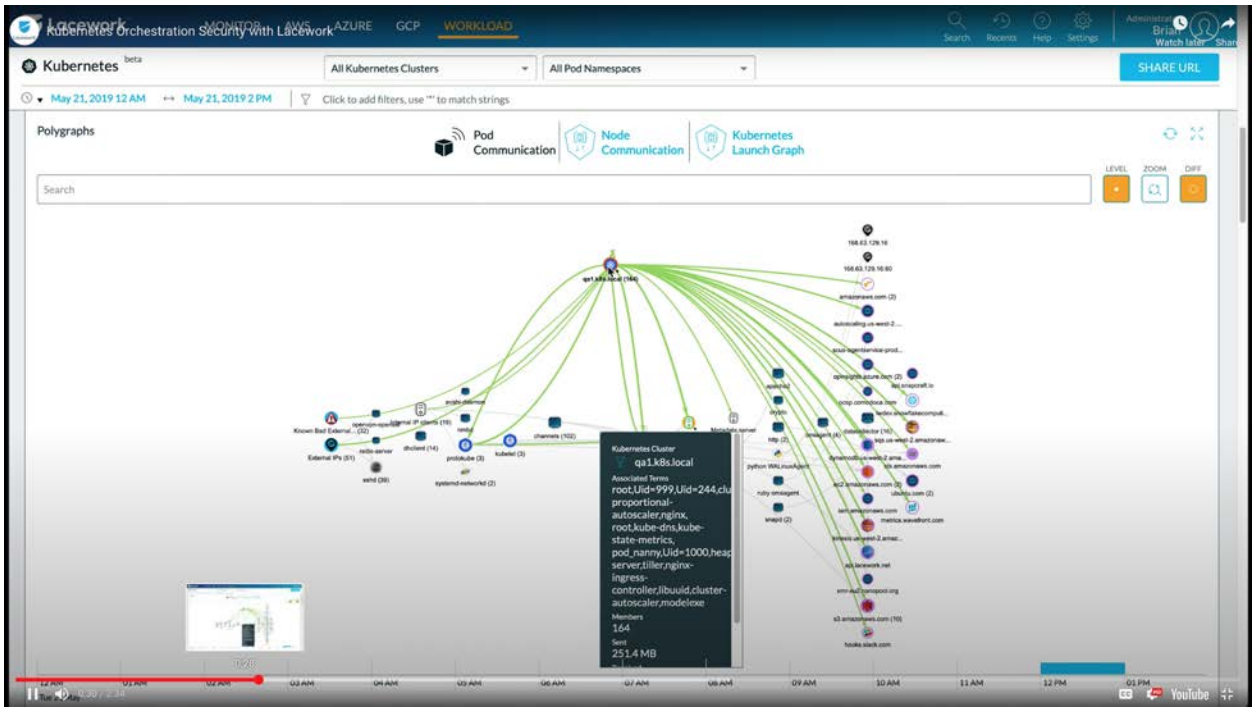

Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Administrator
Brian
Event: 13521
SHARE URL
EVENT ID
13521
SEVERITY
Medium
EVENT NAME
New Internal Connection
FIRST SEEN TIME
11/21/2018 8 AM
WHY
DESCRIPTION
Application hydra running on host ip-172-31-38-102 as user ubuntu connected to application sshd running on host ip-172-31-36-252 as user root
WHO
USER (2)
root
MORE DETAIL
WHAT
APPLICATION
hydra
MACHINE (2)
ip-172-31-36-252
PROCESS
FILE EXE PATH (2)
/usr/sbin/sshd
MORE DETAIL
WHEN
FIRST SEEN TIME
11/21/2018 8 AM
EVENT TIME RANGE
11/21/2018 8 AM - 11/21/2018 9 AM
Investigation
Related Events Timeline
COMPLIANCE
APPLICATION
CLOUDTRAIL
FILE
MACHINE
USER

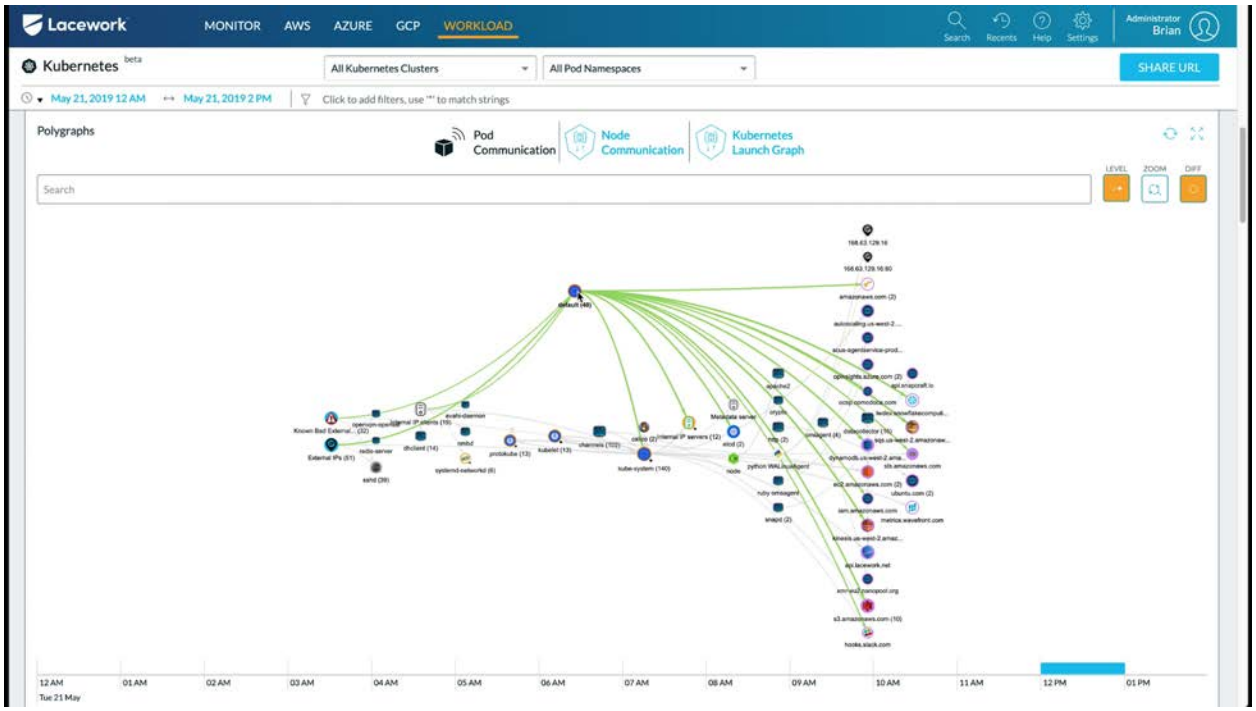

Lacework Anomaly Detection & Investigation
Watch later
Share
Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Administrator
Brian
Event: 13521
SHARE URL
WHAT
APPLICATION
hydra
MACHINE (2)
ip-172-31-36-252
PROCESS
FILE EXE PATH (2)
/usr/sbin/sshd
LESS DETAIL
APPLICATION
APPLICATION
HAS EXTERNAL CONNECTIONS
IS SERVER
IS CLIENT
EARLIEST KNOWN TIME
hydra
false
false
true
11/21/2018 8:00 AM
MACHINE
MACHINE NAME
EXTERNAL IP
AWS INSTANCE ID
AWS INSTANCE NAME
CPU USAGE
INTERNAL IP
IS EXTERNAL
ip-172-31-36-252
34.220.160.250
i-0d7bc7b18514c64f2
CustomerDemo - Hydra De...
0.52%
172.31.36.252
true
ip-172-31-38-102
52.27.6.41
i-0be371f6314061551
CustomerDemo - Hydra So...
0.39%
172.31.38.102
true
PROCESS
MACHINE HOSTNAME
PID
PROCESS START TIME
COMMAND LINE
CPU USAGE
ip-172-31-36-252
17639
11/21/2018 8:33 AM
sshd: unknown [priv]
0%
ip-172-31-36-252
17593
11/21/2018 8:29 AM
sshd: unknown [priv]
0%
ip-172-31-36-252
17737
11/21/2018 8:40 AM
sshd: [accepted]
0%
ip-172-31-36-252
17336
11/21/2018 8:11 AM
sshd: unknown [priv]
0%
ip-172-31-36-252
17992
11/21/2018 8:57 AM
sshd: [accepted]
0%
ip-172-31-36-252
17945
11/21/2018 8:54 AM
sshd: unknown [priv]
0%
ip-172-31-36-252
17470
11/21/2018 8:20 AM
sshd: unknown [priv]
0%
ip-172-31-36-252
17909
11/21/2018 8:51 AM
sshd: [accepted]
0%
ip-172-31-36-252
11/21/2018 8:57 AM
sshd: unknown [priv]
0%
ip-172-31-36-252
11/21/2018 8:14 AM
sshd: unknown [priv]
0%
Page 1 of 30
FILE EXE PATH
EXE PATH
FIRST SEEN TIME
LAST FILE DATA HASH
LAST PACKAGE
LAST VERSION
LAST FILE OWNER
/usr/sbin/sshd
10/8/2018 3:00 PM
b638c1fd82d52c9a408b49c74e...
YouTube

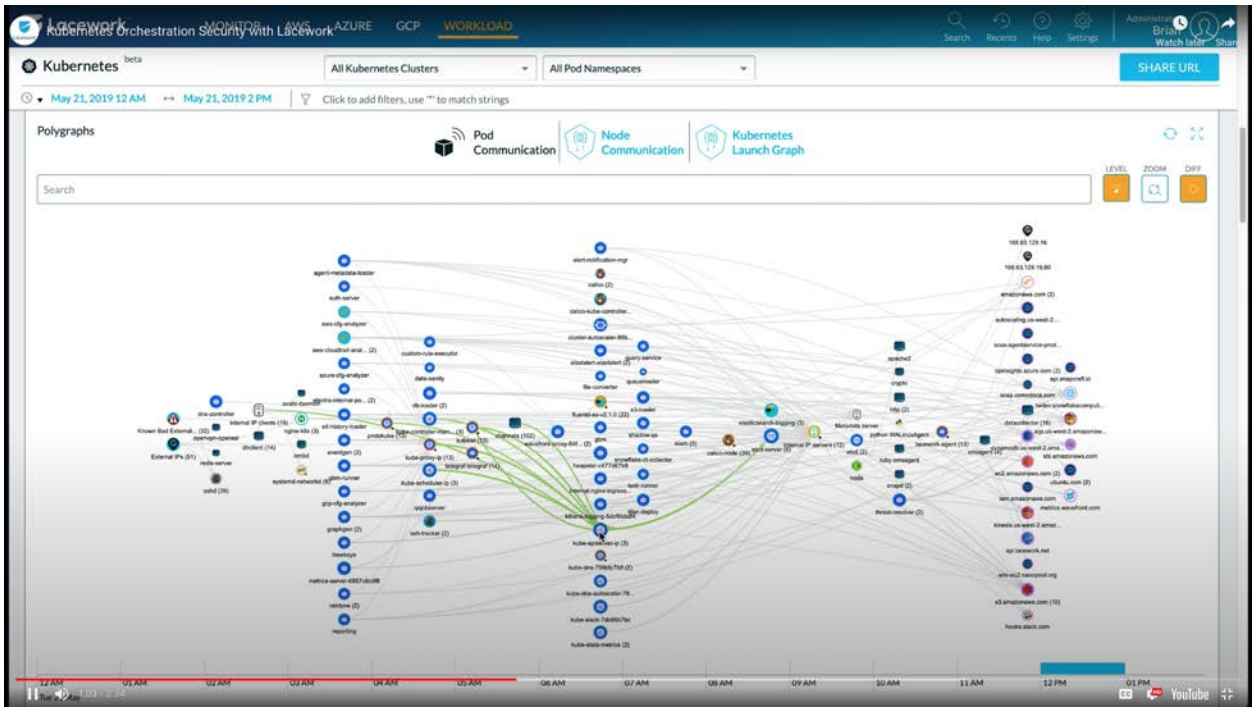

Lacework Anomaly Detection & Investigation
MONITOR
AWS
AZURE
GCP
WORKLOAD
Event: 13521
SHARE URL
EXE PATH
FIRST SEEN TIME
LAST FILEDATA HASH
LAST PACKAGE
LAST VERSION
LAST FILE OWNER
/usr/sbin/sshd
10/8/2018 3:00 PM
b638c1fd82d52c9a408b49c74e...
/usr/local/bin/hydra
10/8/2018 3:00 PM
dfc90d02d95eacc4b3ce4b1f1f0...
WHEN
FIRST SEEN TIME
11/21/2018 8 AM
EVENT TIME RANGE
11/21/2018 8 AM - 11/21/2018 9 AM
Investigation
Question
Answer
Was the application involved in the event from a Packaged Software?
No
Has the application transferred more than the median amount of data compared to the last day?
Yes
Has the DNS involved in this event been involved with any other events in the last 30 days?
Yes
Has the Hash(SHA256) of the application involved in the event changed in the last week?
No
Has the application involved in the event been running as Root?
Yes
Related Events Timeline
COMPLIANCE
APPLICATION
CLOUDTRAIL
FILE
MACHINE
USER
0
Critical
6
High
2
Medium
2
Low
0
Info
NOV 21, 2018
8:00 AM
New Privilege Escalation: Privilege Escalation by ubuntu
8:00 AM
New User: ubuntu
launched New Binary: ubuntu launched sshd
3:00 PM
User Launched New Binary: vagrant launched sshd
YouTube

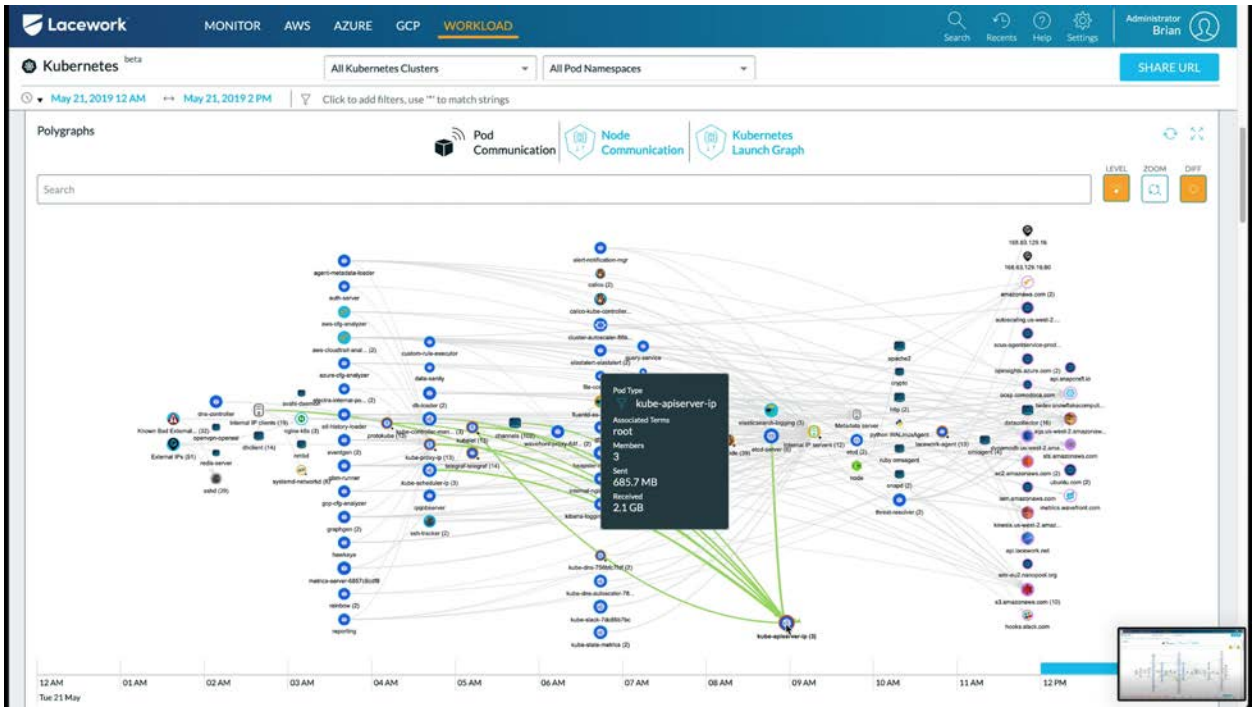

Lacework Anomaly Detection & Investigation
MONITOR
AWS
AZURE
GCP
WORKLOAD
File Hash: 1afa0251e9d8f0329490bc9e333ca77bc3e9d4cf26a210f6f52aedc467dbffe7
SHARE URL
May 29, 2019 12 AM
May 29, 2019 10 AM
Click to add filters, use "*" to match strings
Unique Machines
Unique File Hashes
Unique Applications
Unique Executables
May 29 01AM
May 29 10AM
Events
No data found.
Number of Known Bad Files
Timeline
COMPLIANCE
APPLICATION
CLOUDTRAIL
FILE
MACHINE
USER
0
Critical
0
High
0
Medium
0
Low
0
Info
No events found for selected time pe
YouTube


Lacework Container Security
MONITOR
AWS
AZURE
GCP
WORKLOAD
Containers
SHARE URL
May 21, 2019 12 AM
May 21, 2019 2 PM
Click to add filters, use '*' to match strings
List of Active Containers
Search
Container ID
Container T...
Container N...
Pod Name
Pod Namesp...
Kubernetes ...
VM Type
Image Name
Image Tag
File Path
Start Time
Hostname
User Name
Privileged
PID
8fa42f008e...
DOCKER
/k8s_metric...
metrics-s...
kube-system
qa1.k8s.local
nodes-wo...
gcr.io/google...
v0.2.1
/metrics-ser...
5/16/2019 1...
ip-10-70-34...
root
0
4319
39face9199...
DOCKER
/k8s_kubed...
kube-dns-...
kube-system
qa1.k8s.local
nodes-dm...
gcr.io/google...
1.14.10
/kube-dns
5/16/2019 1...
ip-10-70-2-...
root
0
3300
262a254bca...
DOCKER
/k8s_kiam-ki...
kiam-age...
kube-system
qa1.k8s.local
nodes-wo...
quay.io/uswi...
v3.2
/kiam
5/16/2019 1...
ip-10-70-52...
root
1
9107
2a228c85a0...
DOCKER
/k8s_POD_t...
threat-re...
default
qa1.k8s.local
nodes-wo...
k8s.gcr.io/pa...
3.0
/pause
5/16/2019 1...
ip-10-70-29...
root
0
4617
79e09ddd1...
DOCKER
/k8s_etcd_et...
etcd-1
etcd
qa1.k8s.local
nodes-wo...
quay.io/core...
v3.2.3
/usr/local/bi...
5/16/2019 1...
ip-10-70-53...
root
0
7260
231b77313...
DOCKER
/k8s_lacewo...
lacework-...
kube-system
qa1.k8s.local
nodes-wo...
lacework/da...
2.3.24
/bin/dash
5/21/2019 9...
ip-10-70-52...
root
1
14788
588051ada...
DOCKER
/k8s_kiam-ki...
kiam-age...
kube-system
qa1.k8s.local
nodes-dm...
quay.io/uswi...
v3.2
/kiam
5/16/2019 1...
ip-10-70-3-...
root
1
2690
fe4e294bc4...
DOCKER
/k8s_POD_k...
kube-stat...
kube-system
qa1.k8s.local
nodes-wo...
k8s.gcr.io/pa...
3.0
/pause
5/16/2019 3...
ip-10-70-52...
root
0
13055
349 rows found
Container Image Information
Search
Image Name
Image Tag
Container Type
Created Time
Size
Container Count
Machine Count
User Count
YouTube


Kubernetes Orchestration Security With Lacework
Kubernetes
beta
All Kubernetes Clusters
All Pod Namespaces
SHARE URL
May 21, 2019 12 AM
May 21, 2019 2 PM
Click to add filters, use '*' to match strings
Polygraphs
Pod Communication
Node Communication
Kubernetes Launch Graph
Search
LEVEL
ZOOM
DIFF
Kubernetes Cluster
qa1.k8s.local
Associated Terms
root,Uid=999,Uid=244,clu
proportional-
autoscaler,nginx,
root,kube-dns,kube-
state-metrics,
pod_nanny,Uid=1000,heap
server,tiller,nginx-
ingress-
controller,libuuid,cluster-
autoscaler,modelexe
Members
164
Sent
251.4 MB
YouTube


Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Administrator
Brian
Kubernetes beta
All Kubernetes Clusters
All Pod Namespaces
SHARE URL
May 21, 2019 12 AM
May 21, 2019 2 PM
Click to add filters, use '*' to match strings
Polygraphs
Pod Communication
Node Communication
Kubernetes Launch Graph
Search
LEVEL
ZOOM
DIFF
12 AM
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
Tue 21 May


Kubernetes Orchestration Security With Lacework
Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Administrator
Brian
Watch later
Share
Kubernetes beta
All Kubernetes Clusters
All Pod Namespaces
SHARE URL
May 21, 2019 12 AM
May 21, 2019 2 PM
Click to add filters, use "*" to match strings
Polygraphs
Pod Communication
Node Communication
Kubernetes Launch Graph
Search
LEVEL
ZOOM
DIFF
12 AM
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
YouTube

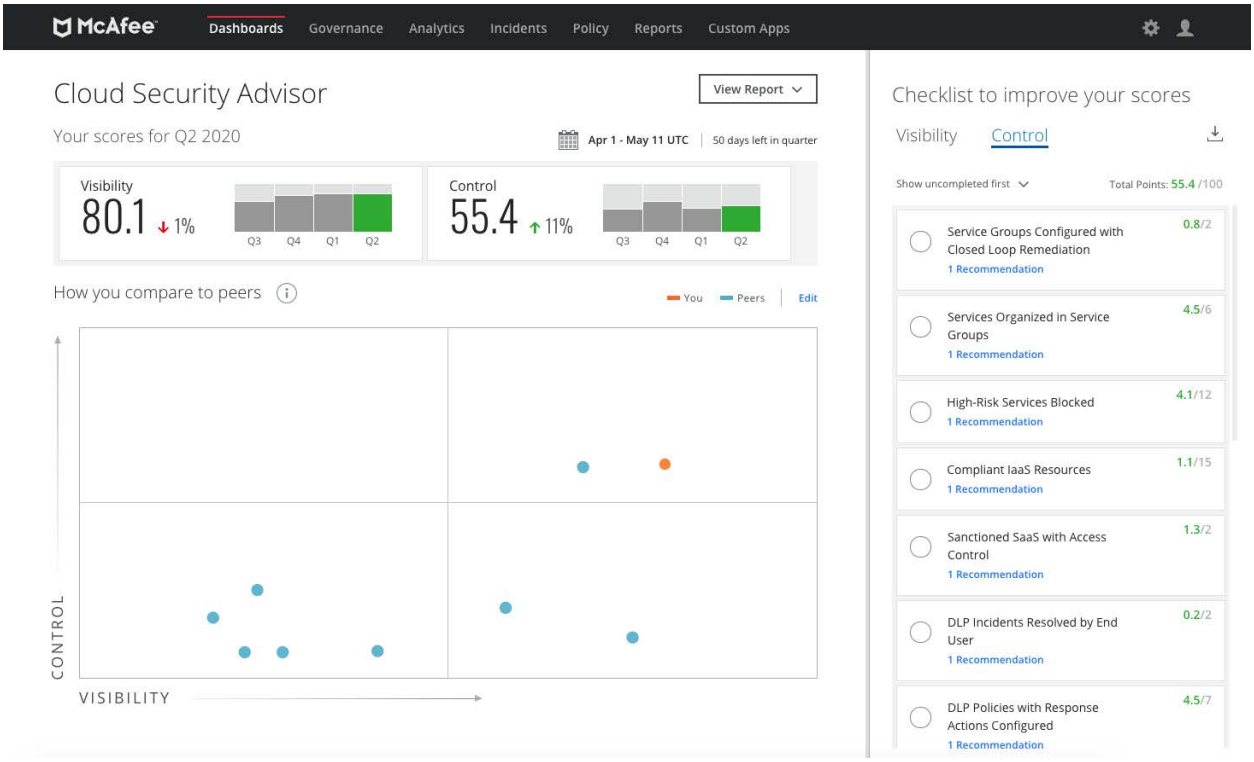

Lacework
MONITOR
AWS
AZURE
GCP
WORKLOAD
Search
Recents
Help
Settings
Administrator
Brian
Kubernetes beta
All Kubernetes Clusters
All Pod Namespaces
SHARE URL
May 21, 2019 12 AM
May 21, 2019 2 PM
Click to add filters, use "*" to match strings
Polygraphs
Pod Communication
Node Communication
Kubernetes Launch Graph
Search
LEVEL
ZOOM
DIFF
Pod Type
kube-apiserver-ip
Associated Terms
root
Members
3
Sent
685.7 MB
Received
2.1 GB
12 AM
Tue 21 May
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM

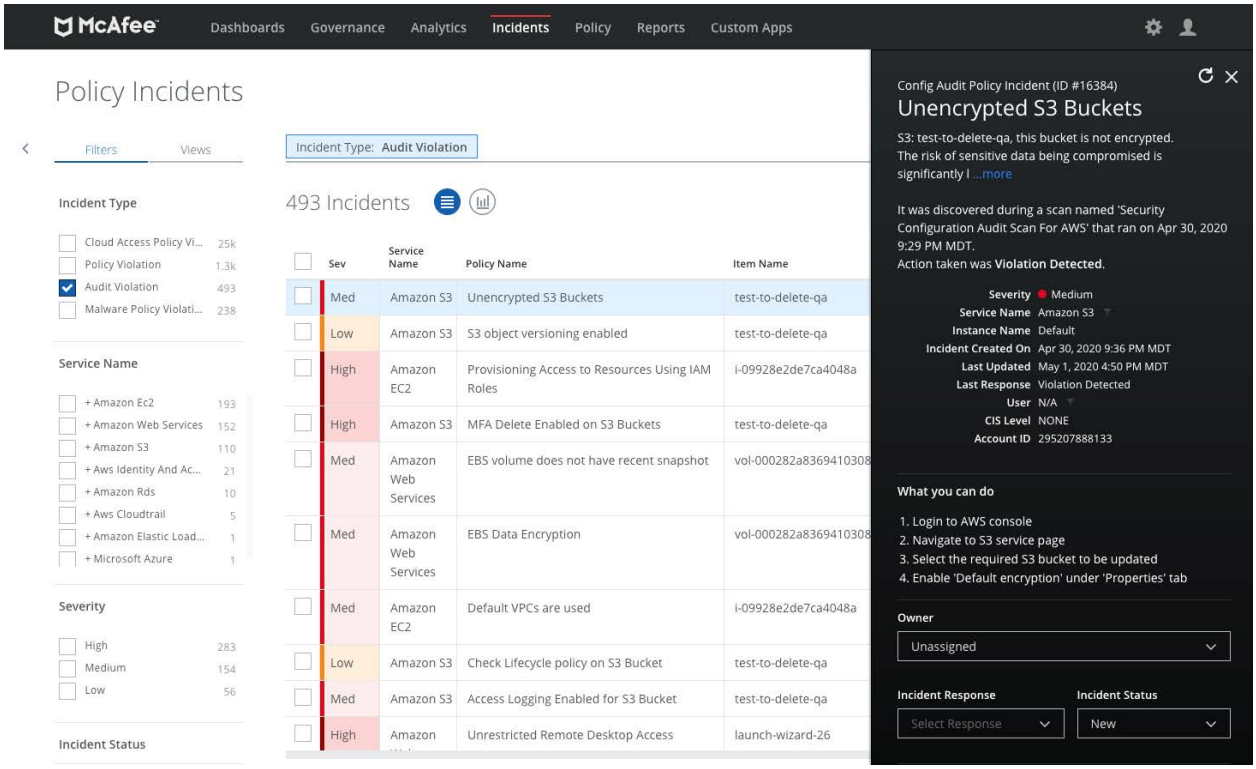
McAfee MVISION Cloud

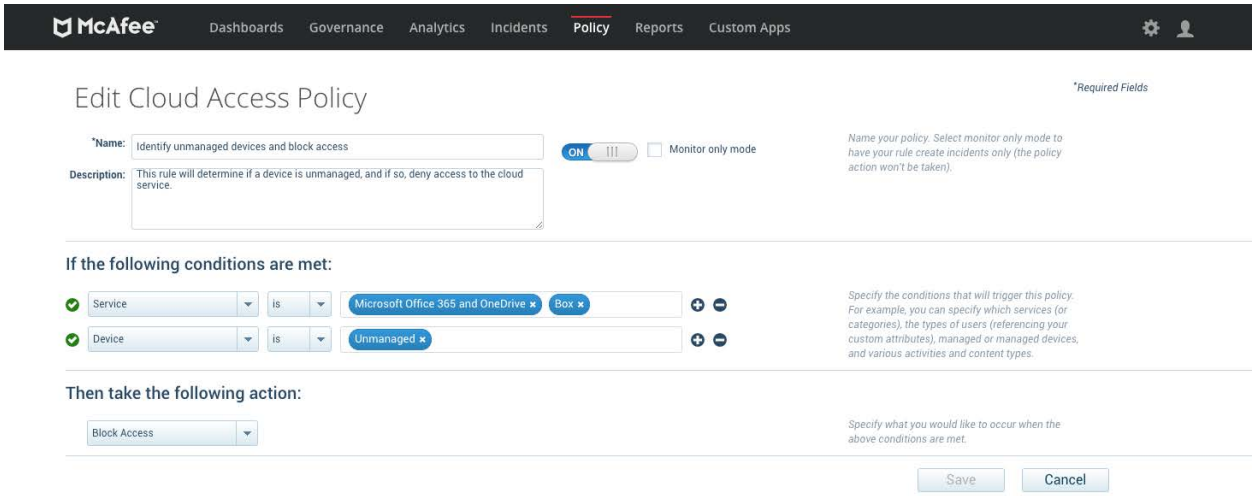
Has a broad set of cloud security capabilities, including CASB, data loss prevention, and threat prevention

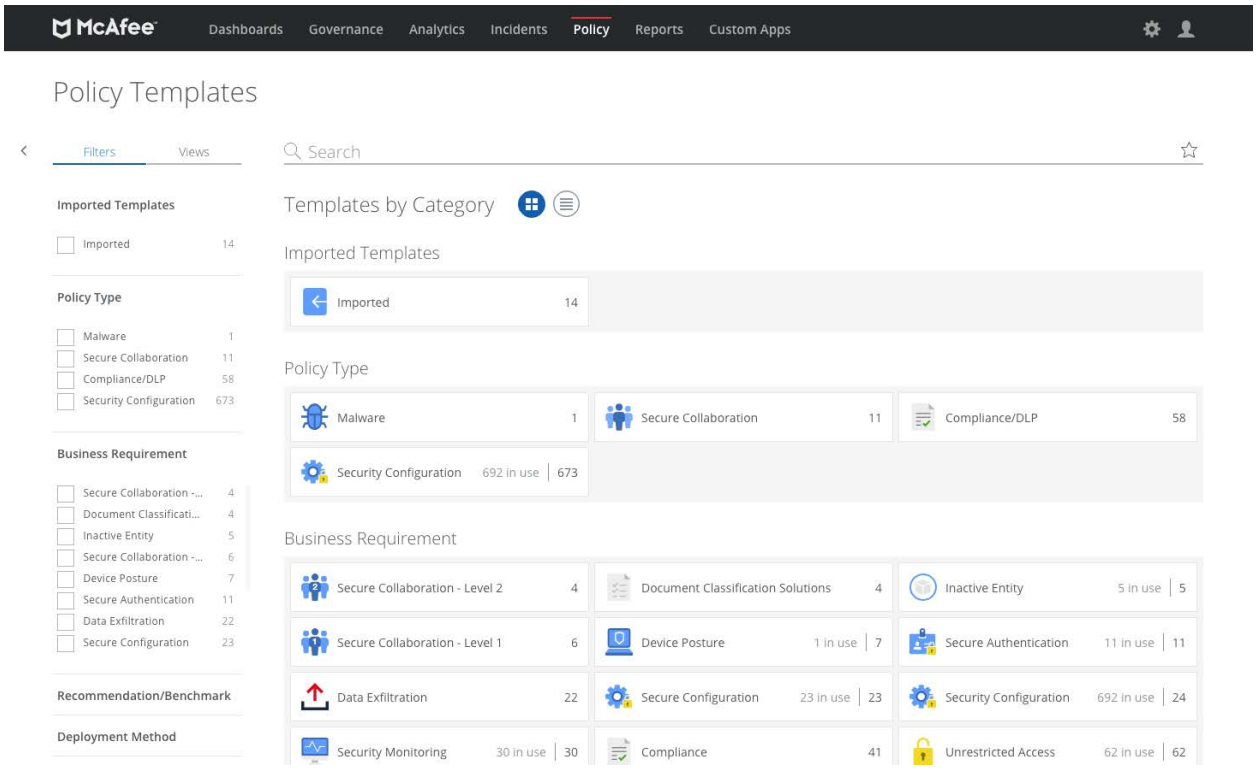
- **Key Values and Differentiators**:
    - MVISION cloud is partnered with Amazon Detective (helps users analyze and identify the root cause of cloud security incidents)
    - CASB capability
    - Strong data loss prevention capabilities; policy control that extends across cloud resources
    - Cloud security risk understanding; trust ratings to help inform security policies
- **Features include:**
    - Cloud registry
    - AI-driven activity mapper
    - Guided learning
    - Cloud activity monitoring
    - Insider threat detection
    - Structured data encryption

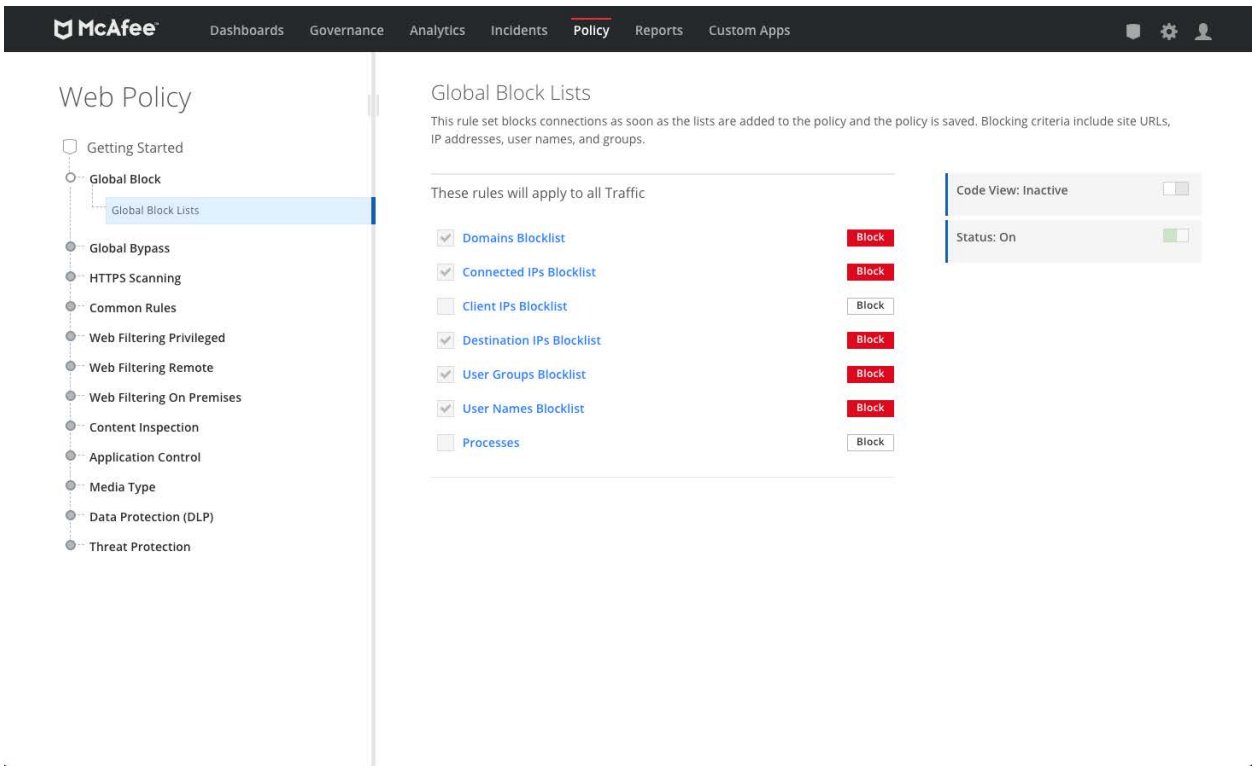
Screenshots of UI:

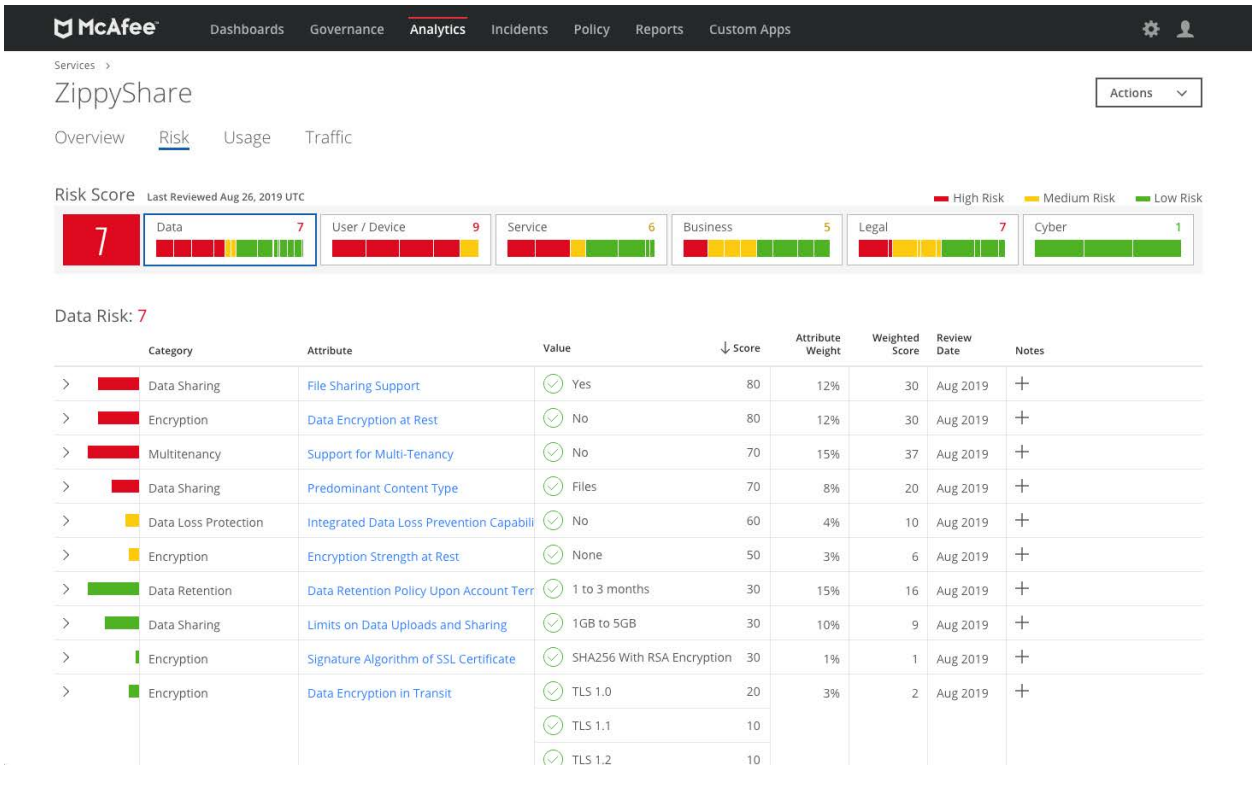


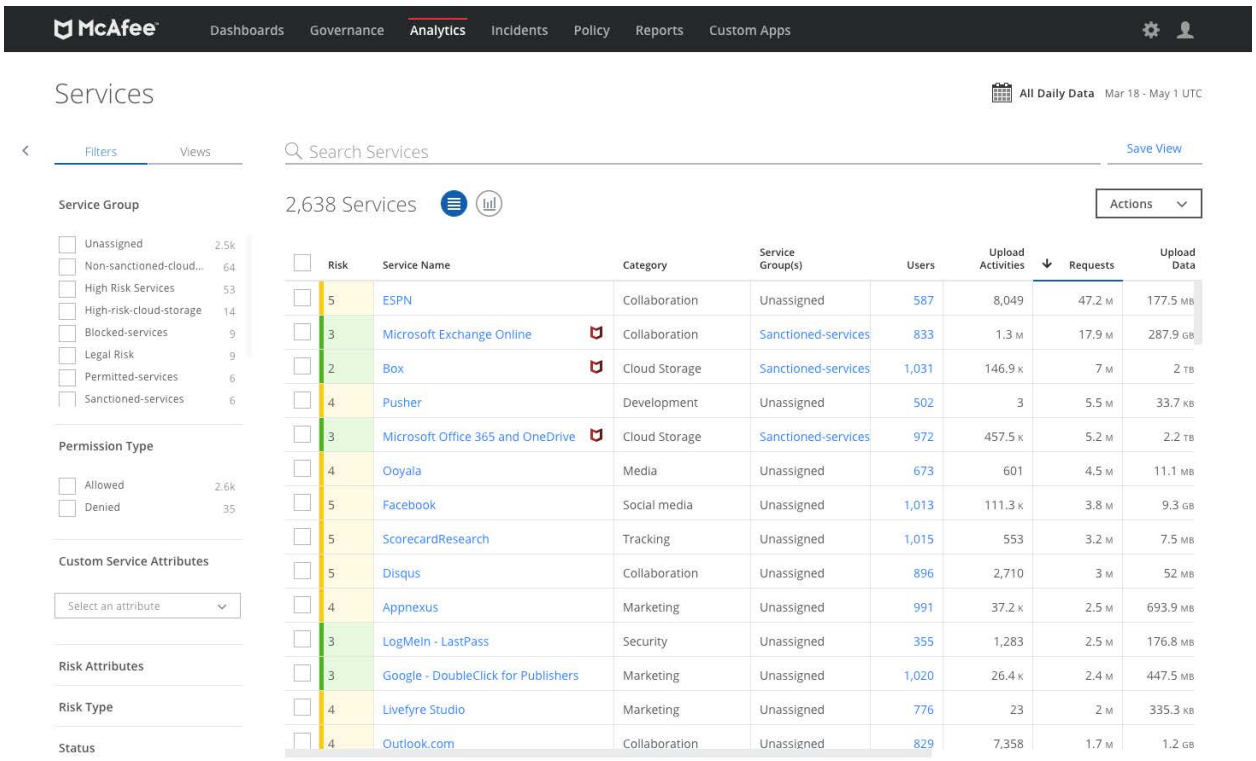

McAfee
Dashboards
Governance
Analytics
Incidents
Policy
Reports
Custom Apps
Policy Incidents
Filters
Views
Incident Type: Audit Violation
493 Incidents
Incident Type
Cloud Access Policy Vi... 25k
Policy Violation 1.3k
Audit Violation 493
Malware Policy Violati... 238
Service Name
+ Amazon Ec2 193
+ Amazon Web Services 152
+ Amazon S3 110
+ Aws Identity And Ac... 21
+ Amazon Rds 10
+ Aws Cloudtrail 5
+ Amazon Elastic Load... 1
+ Microsoft Azure 1
Severity
High 283
Medium 154
Low 56
Incident Status
Sev
Service Name
Policy Name
Item Name
Med Amazon S3 Unencrypted S3 Buckets test-to-delete-qa
Low Amazon S3 S3 object versioning enabled test-to-delete-qa
High Amazon EC2 Provisioning Access to Resources Using IAM Roles i-09928e2de7ca4048a
High Amazon S3 MFA Delete Enabled on S3 Buckets test-to-delete-qa
Med Amazon Web Services EBS volume does not have recent snapshot vol-000282a8369410308
Med Amazon Web Services EBS Data Encryption vol-000282a8369410308
Med Amazon EC2 Default VPCs are used i-09928e2de7ca4048a
Low Amazon S3 Check Lifecycle policy on S3 Bucket test-to-delete-qa
Med Amazon S3 Access Logging Enabled for S3 Bucket test-to-delete-qa
High Amazon Unrestricted Remote Desktop Access launch-wizard-26
Config Audit Policy Incident (ID #16384)
Unencrypted S3 Buckets
S3: test-to-delete-qa, this bucket is not encrypted. The risk of sensitive data being compromised is significantly I ...more
It was discovered during a scan named 'Security Configuration Audit Scan For AWS' that ran on Apr 30, 2020 9:29 PM MDT.
Action taken was Violation Detected.
Severity Medium
Service Name Amazon S3
Instance Name Default
Incident Created On Apr 30, 2020 9:36 PM MDT
Last Updated May 1, 2020 4:50 PM MDT
Last Response Violation Detected
User N/A
CIS Level NONE
Account ID 295207888133
What you can do
1. Login to AWS console
2. Navigate to S3 service page
3. Select the required S3 bucket to be updated
4. Enable 'Default encryption' under 'Properties' tab
Owner
Unassigned
Incident Response
Select Response
Incident Status
New


McAfee
Dashboards
Governance
Analytics
Incidents
Policy
Reports
Custom Apps
Edit Cloud Access Policy
*Required Fields
*Name: Identify unmanaged devices and block access
ON
Monitor only mode
Description: This rule will determine if a device is unmanaged, and if so, deny access to the cloud service.
Name your policy. Select monitor only mode to have your rule create incidents only (the policy action won't be taken).
If the following conditions are met:
Service is Microsoft Office 365 and OneDrive Box
Device is Unmanaged
Specify the conditions that will trigger this policy. For example, you can specify which services (or categories), the types of users (referencing your custom attributes), managed or managed devices, and various activities and content types.
Then take the following action:
Block Access
Specify what you would like to occur when the above conditions are met.
Save
Cancel


McAfee
Dashboards
Governance
Analytics
Incidents
Policy
Reports
Custom Apps
Policy Templates
Filters
Views
Search
Imported Templates
Imported 14
Policy Type
Malware 1
Secure Collaboration 11
Compliance/DLP 58
Security Configuration 673
Business Requirement
Secure Collaboration -... 4
Document Classificati... 4
Inactive Entity 5
Secure Collaboration -... 6
Device Posture 7
Secure Authentication 11
Data Exfiltration 22
Secure Configuration 23
Recommendation/Benchmark
Deployment Method
Templates by Category
Imported Templates
Imported 14
Policy Type
Malware 1
Secure Collaboration 11
Compliance/DLP 58
Security Configuration 692 in use 673
Business Requirement
Secure Collaboration - Level 2 4
Document Classification Solutions 4
Inactive Entity 5 in use 5
Secure Collaboration - Level 1 6
Device Posture 1 in use 7
Secure Authentication 11 in use 11
Data Exfiltration 22
Secure Configuration 23 in use 23
Security Configuration 692 in use 24
Security Monitoring 30 in use 30
Compliance 41
Unrestricted Access 62 in use 62


McAfee
Dashboards
Governance
Analytics
Incidents
Policy
Reports
Custom Apps
Web Policy
Getting Started
Global Block
Global Block Lists
Global Bypass
HTTPS Scanning
Common Rules
Web Filtering Privileged
Web Filtering Remote
Web Filtering On Premises
Content Inspection
Application Control
Media Type
Data Protection (DLP)
Threat Protection
Global Block Lists
This rule set blocks connections as soon as the lists are added to the policy and the policy is saved. Blocking criteria include site URLs, IP addresses, user names, and groups.
These rules will apply to all Traffic
Domains Blocklist Block
Connected IPs Blocklist Block
Client IPs Blocklist Block
Destination IPs Blocklist Block
User Groups Blocklist Block
User Names Blocklist Block
Processes Block
Code View: Inactive
Status: On


McAfee
Dashboards
Governance
Analytics
Incidents
Policy
Reports
Custom Apps
Services ›
ZippyShare
Actions
Overview
Risk
Usage
Traffic
Risk Score
Last Reviewed Aug 26, 2019 UTC
High Risk
Medium Risk
Low Risk
7
Data 7
User / Device 9
Service 6
Business 5
Legal 7
Cyber 1
Data Risk: 7
Category
Attribute
Value
Score
Attribute Weight
Weighted Score
Review Date
Notes
Data Sharing
File Sharing Support
Yes
80
12%
30
Aug 2019
Encryption
Data Encryption at Rest
No
80
12%
30
Aug 2019
Multitenancy
Support for Multi-Tenancy
No
70
15%
37
Aug 2019
Data Sharing
Predominant Content Type
Files
70
8%
20
Aug 2019
Data Loss Protection
Integrated Data Loss Prevention Capabili
No
60
4%
10
Aug 2019
Encryption
Encryption Strength at Rest
None
50
3%
6
Aug 2019
Data Retention
Data Retention Policy Upon Account Terr
1 to 3 months
30
15%
16
Aug 2019
Data Sharing
Limits on Data Uploads and Sharing
1GB to 5GB
30
10%
9
Aug 2019
Encryption
Signature Algorithm of SSL Certificate
SHA256 With RSA Encryption
30
1%
1
Aug 2019
Encryption
Data Encryption in Transit
TLS 1.0
20
3%
2
Aug 2019
TLS 1.1
10
TLS 1.2
10


McAfee
Dashboards
Governance
Analytics
Incidents
Policy
Reports
Custom Apps
Services
All Daily Data Mar 18 - May 1 UTC
Filters
Views
Search Services
Save View
Service Group
Unassigned 2.5k
Non-sanctioned-cloud... 64
High Risk Services 53
High-risk-cloud-storage 14
Blocked-services 9
Legal Risk 9
Permitted-services 6
Sanctioned-services 6
Permission Type
Allowed 2.6k
Denied 35
Custom Service Attributes
Select an attribute
Risk Attributes
Risk Type
Status
2,638 Services
Actions
Risk
Service Name
Category
Service Group(s)
Users
Upload Activities
Requests
Upload Data
5 ESPN Collaboration Unassigned 587 8,049 47.2 M 177.5 MB
3 Microsoft Exchange Online Collaboration Sanctioned-services 833 1.3 M 17.9 M 287.9 GB
2 Box Cloud Storage Sanctioned-services 1,031 146.9 K 7 M 2 TB
4 Pusher Development Unassigned 502 3 5.5 M 33.7 KB
3 Microsoft Office 365 and OneDrive Cloud Storage Sanctioned-services 972 457.5 K 5.2 M 2.2 TB
4 Ooyala Media Unassigned 673 601 4.5 M 11.1 MB
5 Facebook Social media Unassigned 1,013 111.3 K 3.8 M 9.3 GB
5 ScorecardResearch Tracking Unassigned 1,015 553 3.2 M 7.5 MB
5 Disqus Collaboration Unassigned 896 2,710 3 M 52 MB
4 Appnexus Marketing Unassigned 991 37.2 K 2.5 M 693.9 MB
3 LogMeIn - LastPass Security Unassigned 355 1,283 2.5 M 176.8 MB
3 Google - DoubleClick for Publishers Marketing Unassigned 1,020 26.4 K 2.4 M 447.5 MB
4 Livefyre Studio Marketing Unassigned 776 23 2 M 335.3 KB
4 Outlook.com Collaboration Unassigned 829 7,358 1.7 M 1.2 GB

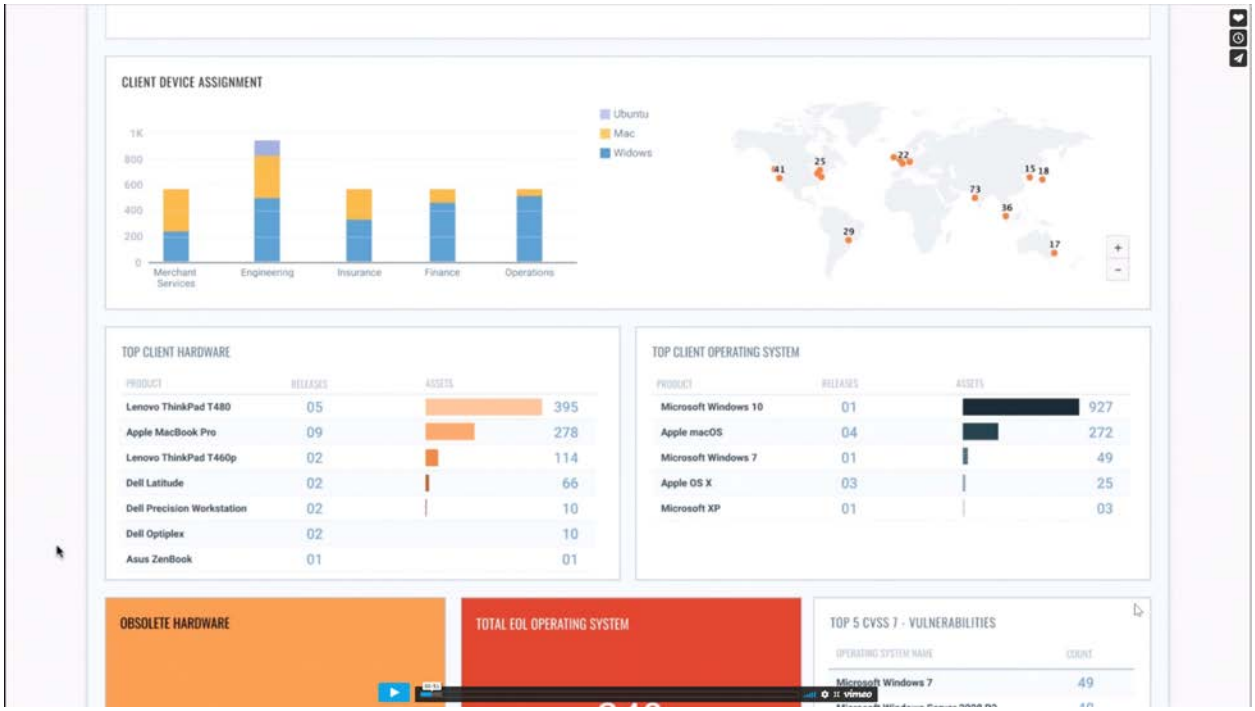
Qualys

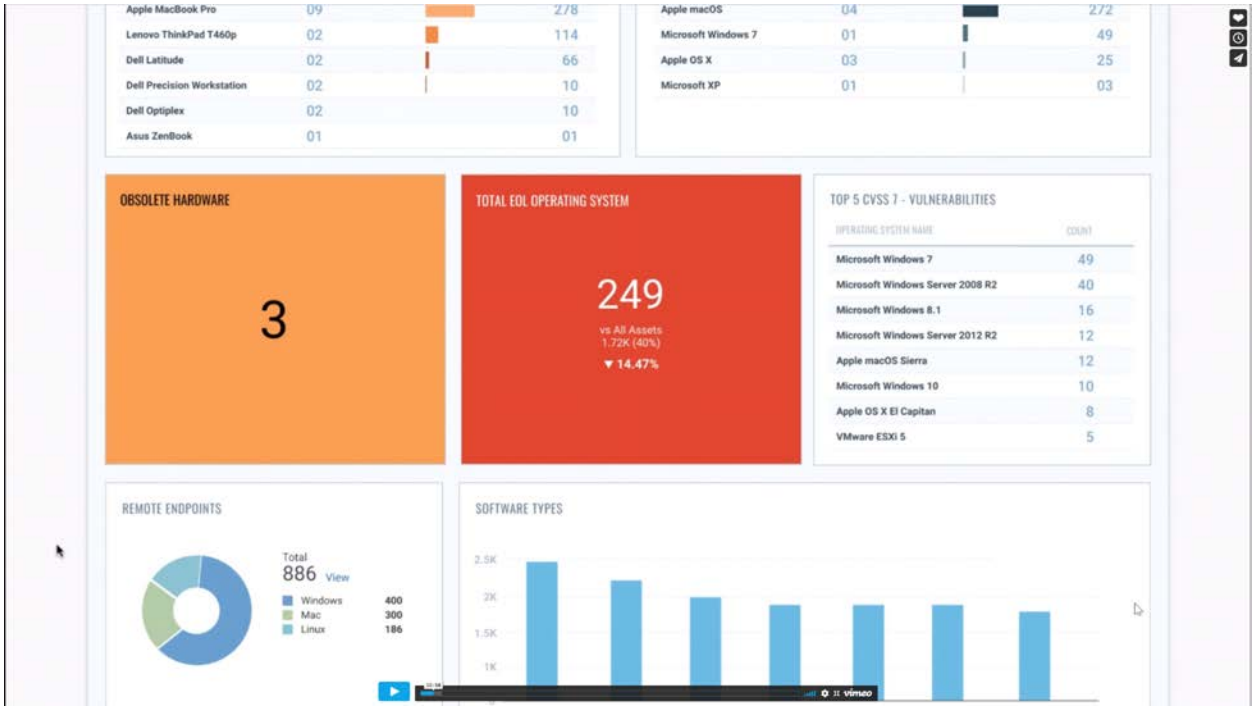
The Qualys cloud platform has multiple modules that can enable different facets of cloud security, including compliance, vulnerability scanning and cloud workload protection. Qualys has the best looking UI in my opinion, it is the most visual.

Product Demo - Deep-Dive Demo (27 min)

- **Key Values and Differentiators**:
    - Web Application Scanning module, provides automatic scanning capabilities for web apps to help detect and rank security vulnerabilities
    - Compliance; PCI-DSS compliance module scans all devices to identify compliance status
    - Policy Compliance module enables automated security configuration assessments across on-prem and cloud assets
- **Features include:**
    - Asset Management
    - IT Security
    - Cloud/Container Security
    - Web App Security
    - Compliance
    - How they incorporate the Network Topology is great

Screenshots of UI:

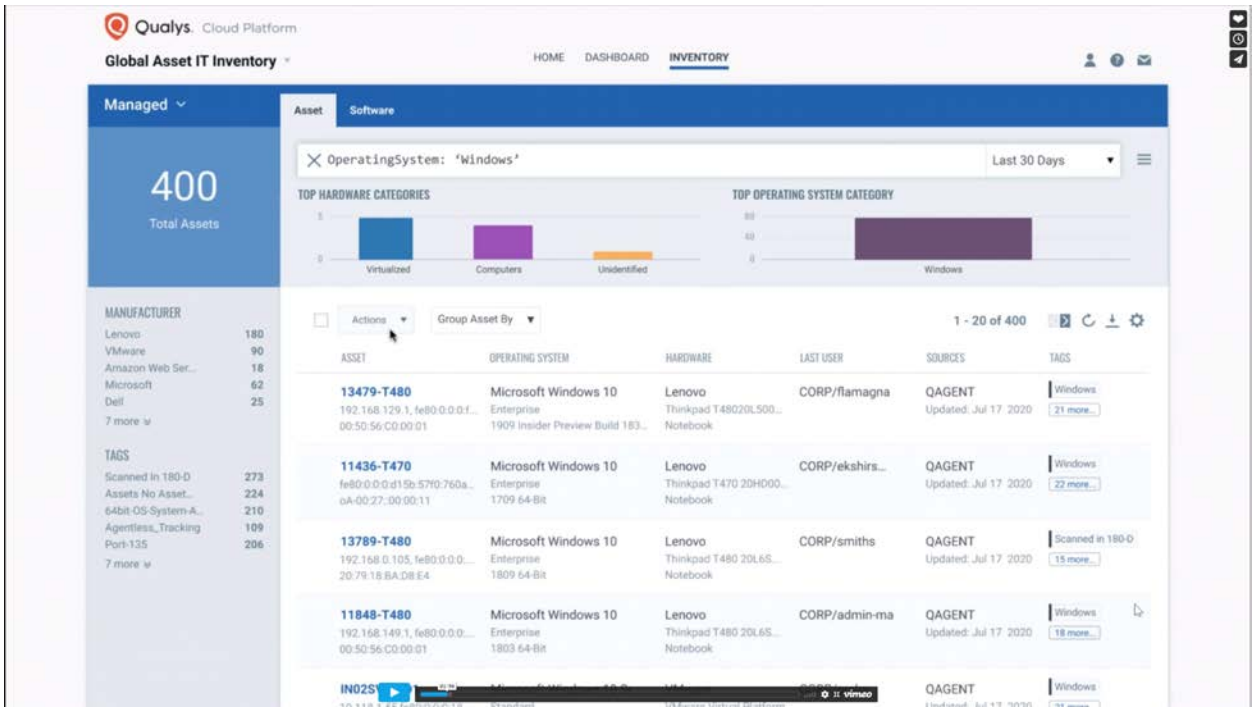

CLIENT DEVICE ASSIGNMENT
Ubuntu
Mac
Widows
1K
800
600
400
200
0
Merchant Services
Engineering
Insurance
Finance
Operations
41
25
22
15
18
73
36
29
17
TOP CLIENT HARDWARE
PRODUCT
RELEASES
ASSETS
Lenovo ThinkPad T480 05 395
Apple MacBook Pro 09 278
Lenovo ThinkPad T460p 02 114
Dell Latitude 02 66
Dell Precision Workstation 02 10
Dell Optiplex 02 10
Asus ZenBook 01 01
TOP CLIENT OPERATING SYSTEM
PRODUCT
RELEASES
ASSETS
Microsoft Windows 10 01 927
Apple macOS 04 272
Microsoft Windows 7 01 49
Apple OS X 03 25
Microsoft XP 01 03
OBSOLETE HARDWARE
TOTAL EOL OPERATING SYSTEM
TOP 5 CVSS 7 - VULNERABILITIES
OPERATING SYSTEM NAME
COUNT
Microsoft Windows 7 49

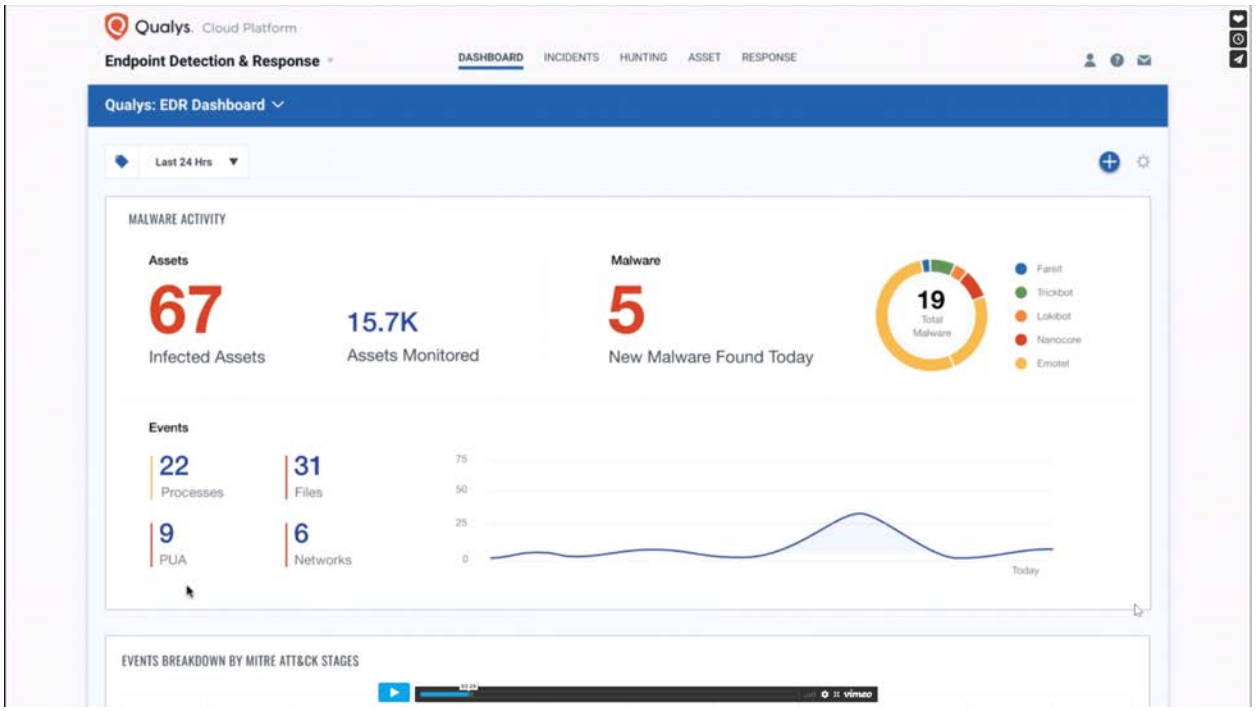

Apple MacBook Pro 09 278
Lenovo ThinkPad T460p 02 114
Dell Latitude 02 66
Dell Precision Workstation 02 10
Dell Optiplex 02 10
Asus ZenBook 01 01
Apple macOS 04 272
Microsoft Windows 7 01 49
Apple OS X 03 25
Microsoft XP 01 03
OBSOLETE HARDWARE
3
TOTAL EOL OPERATING SYSTEM
249
vs All Assets
1.72K (40%)
▼ 14.47%
TOP 5 CVSS 7 - VULNERABILITIES
OPERATING SYSTEM NAME
COUNT
Microsoft Windows 7 49
Microsoft Windows Server 2008 R2 40
Microsoft Windows 8.1 16
Microsoft Windows Server 2012 R2 12
Apple macOS Sierra 12
Microsoft Windows 10 10
Apple OS X El Capitan 8
VMware ESXi 5
REMOTE ENDPOINTS
Total
886 View
Windows 400
Mac 300
Linux 186
SOFTWARE TYPES
2.5K
2K
1.5K
1K

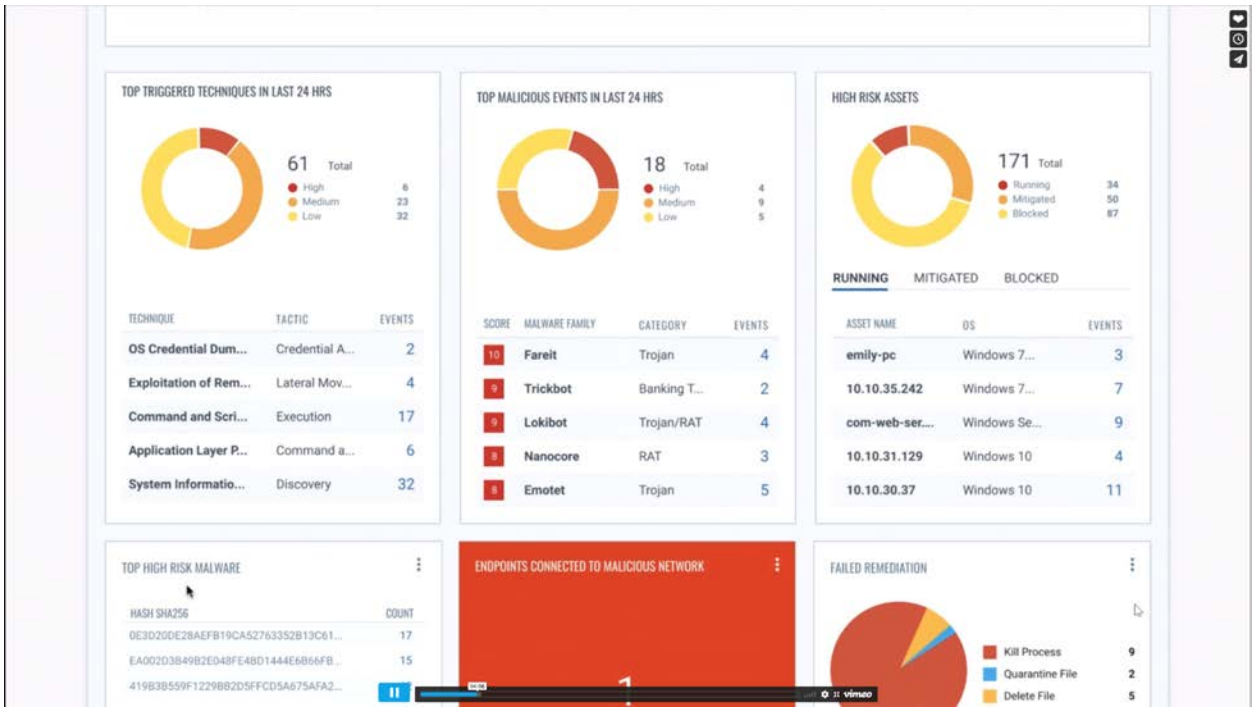

REMOTE ENDPOINTS
Total
886 View
Windows 400
Mac 300
Linux 186
SOFTWARE TYPES
Device Drivers
Utilities
Firmware
Applications
Plugins
Other
Setup Software
TOP SOFTWARE PUBLISHERS
Microsoft
Symantec
Qualys
Apple
Adobe
Oracle
VMware
Google
Mozilla
LICENSE CATEGORY
Open Source
Commercial
TOP CLIENT APPLICATION CATEGORIES
Commercial License
Open Source License
5.66K
4.57K
3.58K
3.35K
3.01K
TOP SERVER APPLICATION CATEGORIES
240
101
32
15
7

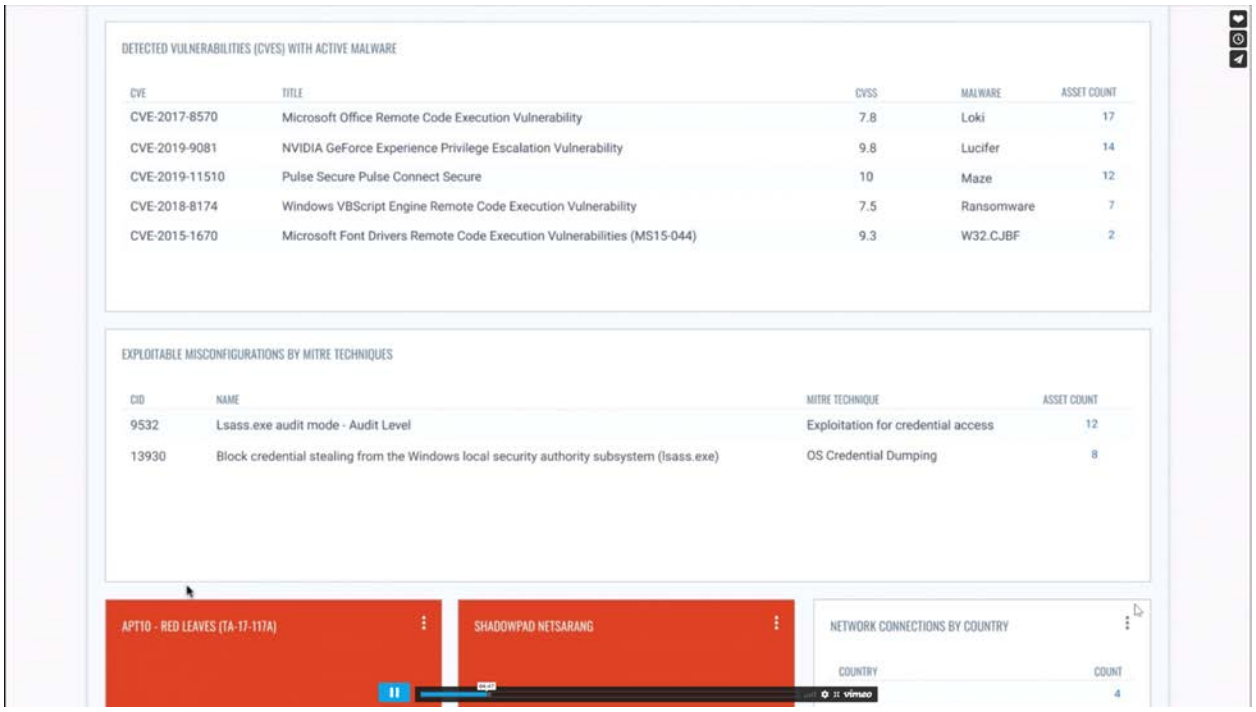

Microsoft
Symantec
Qualys
Apple
Adobe
Oracle
VMware
Google
Mozilla
Open Source
Commercial
TOP CLIENT APPLICATION CATEGORIES
Commercial License
Open Source License
5.66K
4.57K
3.58K
3.35K
3.01K
Productivity
Network Application
Digital Content
Application Development
Scurity
TOP SERVER APPLICATION CATEGORIES
240
101
32
15
7
Databases
Networking
Application Development
Data Management and Quality
Network Application
END-OF-LIFE (EOL) SOFTWARE
4.55k
vs
99.2k (5%)
▼ 4.58%
END-OF-LIFE SOFTWARE
EOL within 3 months
EOL 3 to 6 months
EOL 6 to 9 months
EOL 9 to 12 months
Application Development
Security
Digital Content

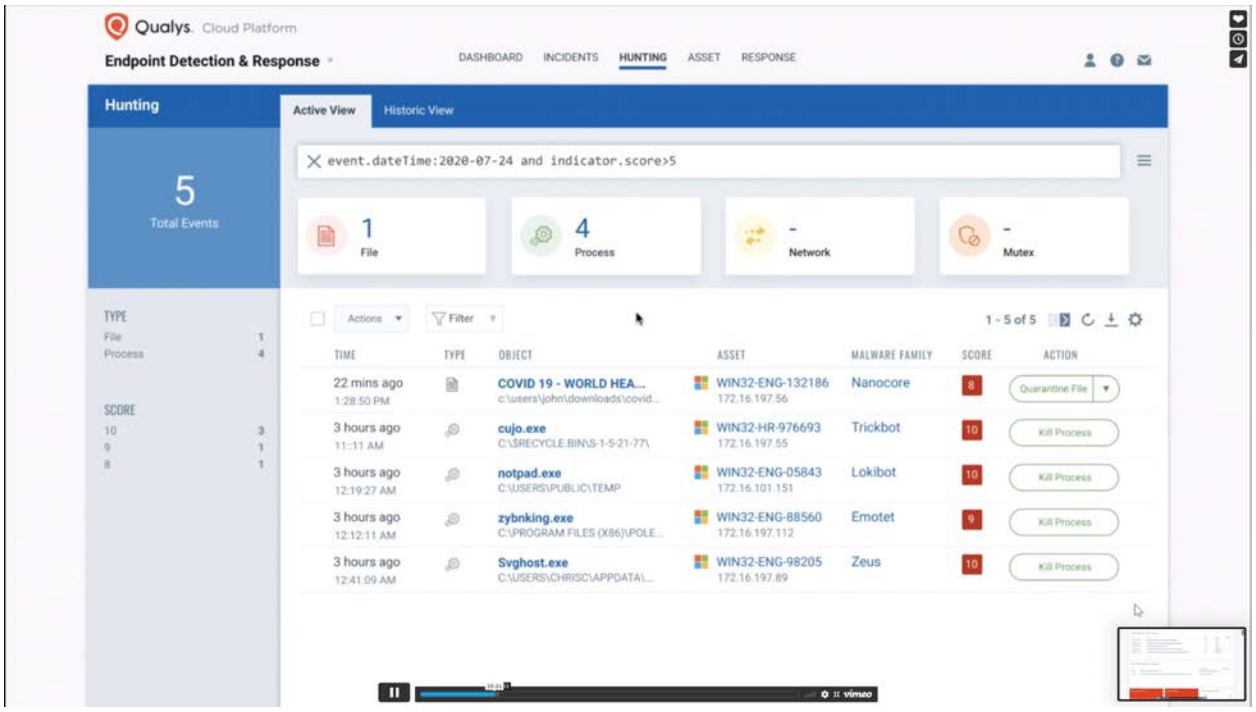

EOL ENDPOINT PROTECTION
SOFTWARE PUBLISHER
COUNT
Symantec 209
Malwarebytes 97
Cisco Systems 32
Pulse Secure 30
TrueCrypt 14
GNU Project 2
Support.com 2
EOL STORAGE APPS
SOFTWARE PRODUCT
COUNT
iCloud 425
WinRAR 122
Tivoli Storage Manager Client 39
EMC NetWorker 23
Data Protector 21
Tivoli Storage Manager Server 15
Tivoli Storage Manager 11
EOL BROWSERS
SOFTWARE PRODUCT
COUNT
Chrome 798
Safari 706
Internet Explorer 671
Firefox 539
Opera 38
UNUSED SOFTWARE CATEGORY
Digital Content
Storage
Design
Productivity
SOFTWARE RECLAMATION CANDIDATES
Microsoft Visio
Adobe Acrobat
Lucid Charts
Microsoft Project
Adobe Photoshop
0
50
100
150
200
1.2K
BLACKLISTED INSTALLATIONS
TOP BLACKLISTED CATEGORIES

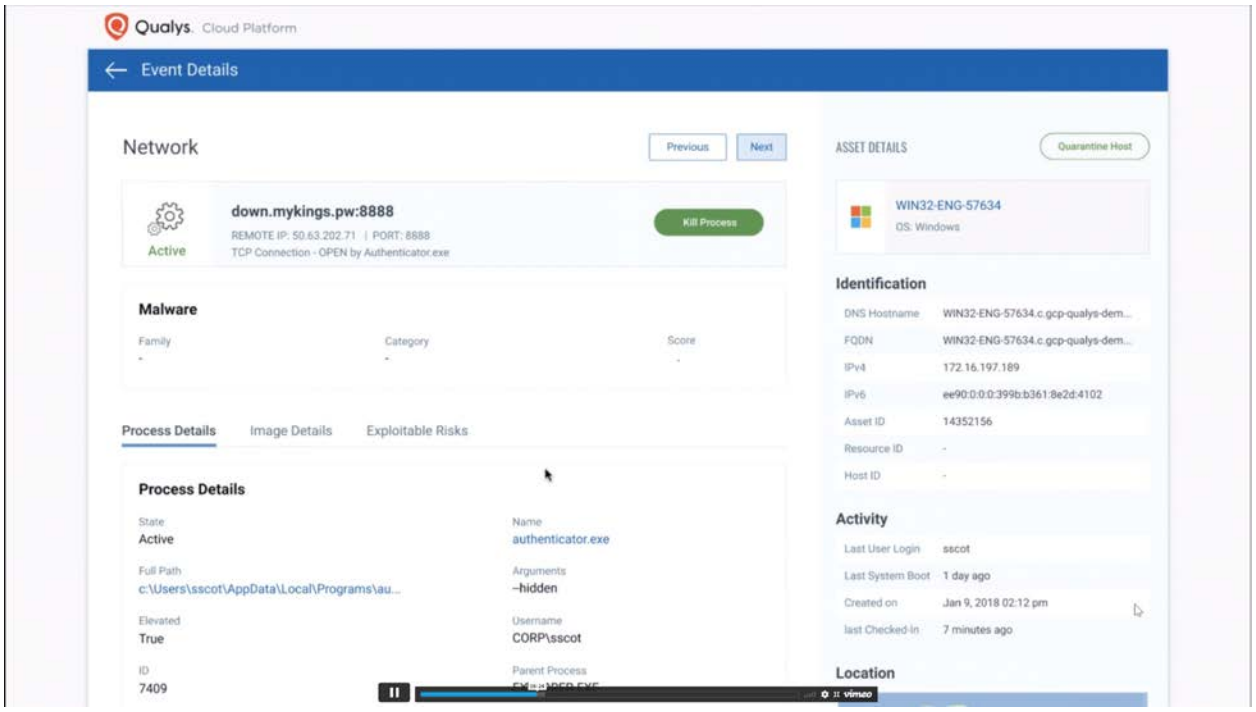

Qualys. Cloud Platform
Global Asset IT Inventory
HOME
DASHBOARD
INVENTORY
Managed
Asset
Software
400
Total Assets
OperatingSystem: 'Windows'
Last 30 Days
TOP HARDWARE CATEGORIES
Virtualized
Computers
Unidentified
TOP OPERATING SYSTEM CATEGORY
Windows
MANUFACTURER
Lenovo 180
VMware 90
Amazon Web Ser... 18
Microsoft 62
Dell 25
7 more
TAGS
Scanned in 180-D 273
Assets No Asset... 224
64bit-OS-System-A... 210
Agentless_Tracking 109
Port-135 206
7 more
Actions
Group Asset By
1 - 20 of 400
ASSET
OPERATING SYSTEM
HARDWARE
LAST USER
SOURCES
TAGS
13479-T480
Microsoft Windows 10 Enterprise
1909 Insider Preview Build 183...
Lenovo Thinkpad T480 20L500... Notebook
CORP/flamagna
QAGENT Updated: Jul 17 2020
Windows 21 more...
11436-T470
Microsoft Windows 10 Enterprise
1709 64-Bit
Lenovo Thinkpad T470 20HD00... Notebook
CORP/ekshirs...
QAGENT Updated: Jul 17 2020
Windows 22 more...
13789-T480
Microsoft Windows 10 Enterprise
1809 64-Bit
Lenovo Thinkpad T480 20L6S... Notebook
CORP/smiths
QAGENT Updated: Jul 17 2020
Scanned in 180-D 15 more...
11848-T480
Microsoft Windows 10 Enterprise
1803 64-Bit
Lenovo Thinkpad T480 20L6S... Notebook
CORP/admin-ma
QAGENT Updated: Jul 17 2020
Windows 18 more...

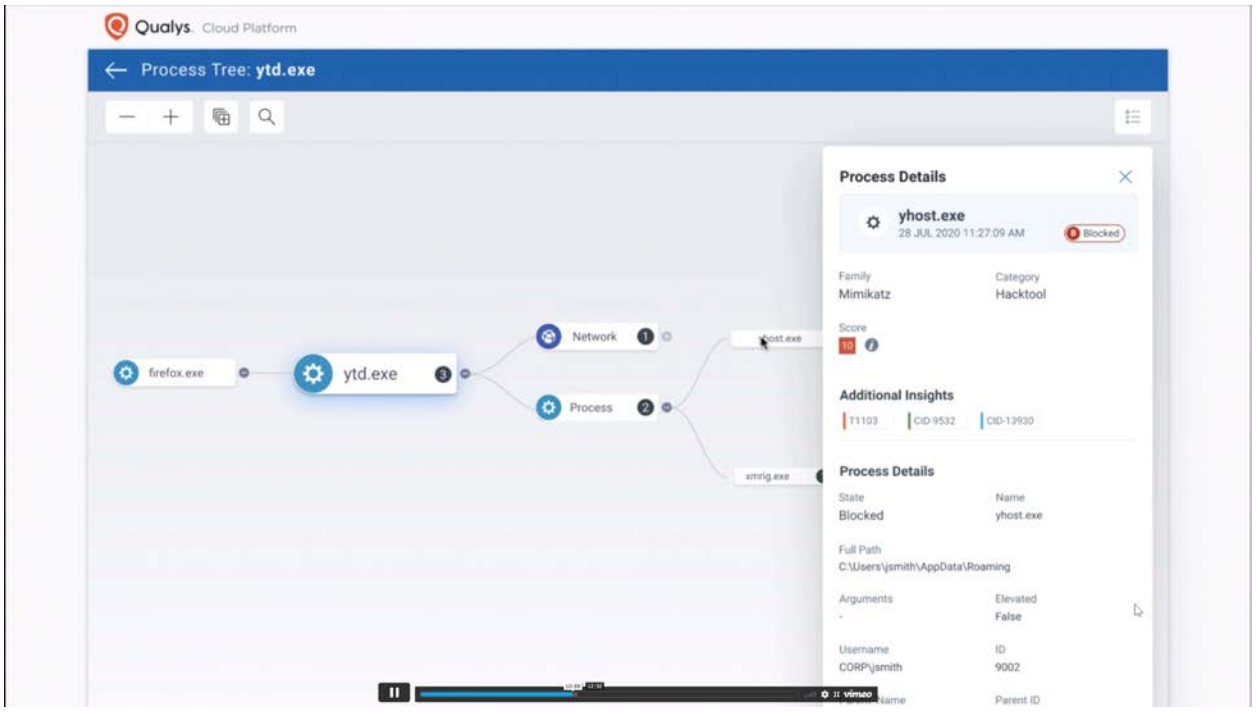

Qualys. Cloud Platform
Endpoint Detection & Response
DASHBOARD
INCIDENTS
HUNTING
ASSET
RESPONSE
Qualys: EDR Dashboard
Last 24 Hrs
MALWARE ACTIVITY
Assets
67
Infected Assets
15.7K
Assets Monitored
Malware
5
New Malware Found Today
19
Total Malware
Fareit
Trickbot
Lokibot
Nanocore
Emotet
Events
22
Processes
31
Files
9
PUA
6
Networks
75
50
25
0
Today
EVENTS BREAKDOWN BY MITRE ATT&CK STAGES

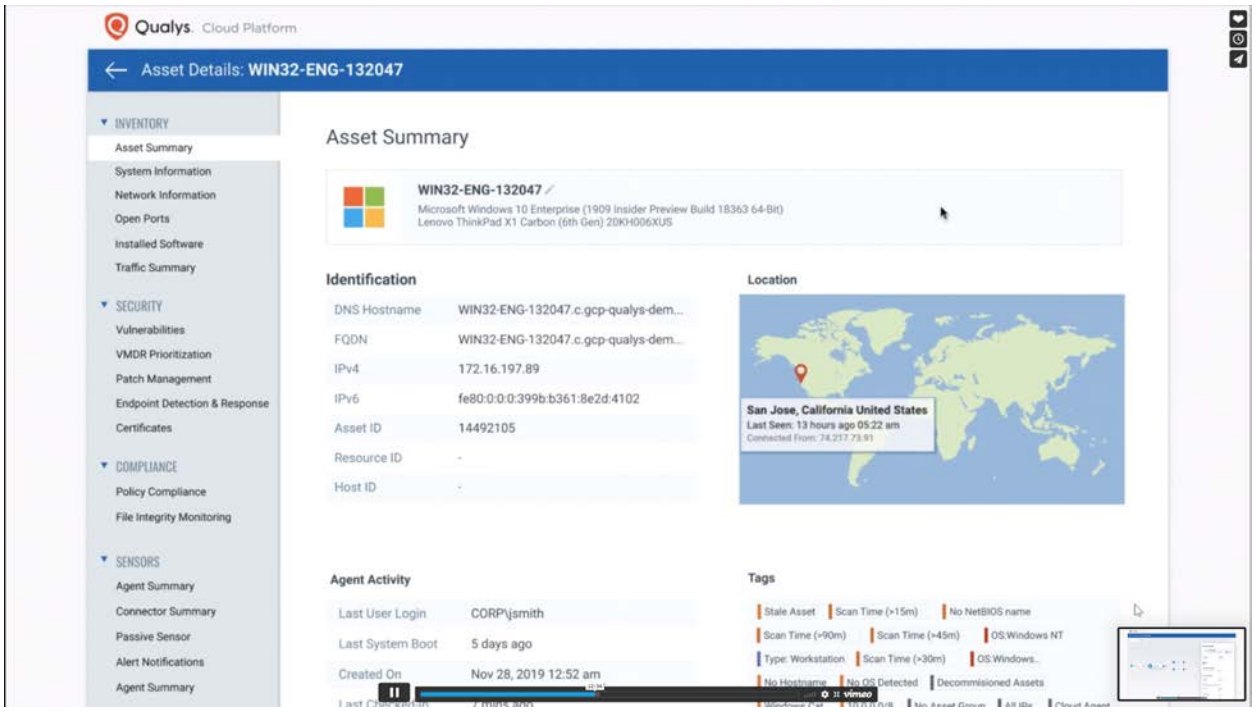

TOP TRIGGERED TECHNIQUES IN LAST 24 HRS
61 Total
High 6
Medium 23
Low 32
TECHNIQUE
TACTIC
EVENTS
OS Credential Dum...
Credential A...
2
Exploitation of Rem...
Lateral Mov...
4
Command and Scri...
Execution
17
Application Layer P...
Command a...
6
System Informatio...
Discovery
32
TOP MALICIOUS EVENTS IN LAST 24 HRS
18 Total
High 4
Medium 9
Low 5
SCORE
MALWARE FAMILY
CATEGORY
EVENTS
10
Fareit
Trojan
4
9
Trickbot
Banking T...
2
9
Lokibot
Trojan/RAT
4
8
Nanocore
RAT
3
8
Emotet
Trojan
5
HIGH RISK ASSETS
171 Total
Running 34
Mitigated 50
Blocked 87
RUNNING
MITIGATED
BLOCKED
ASSET NAME
OS
EVENTS
emily-pc
Windows 7...
3
10.10.35.242
Windows 7...
7
com-web-ser...
Windows Se...
9
10.10.31.129
Windows 10
4
10.10.30.37
Windows 10
11
TOP HIGH RISK MALWARE
HASH SHA256
COUNT
0E3D20DE28AEFB19CA52763352B13C61...
17
EA002D3B49B2E048FE4BD1444E6B66FB...
15
419B3B559F1229BB2D5FFCD5A675AFA2...
ENDPOINTS CONNECTED TO MALICIOUS NETWORK
FAILED REMEDIATION
Kill Process 9
Quarantine File 2
Delete File 5

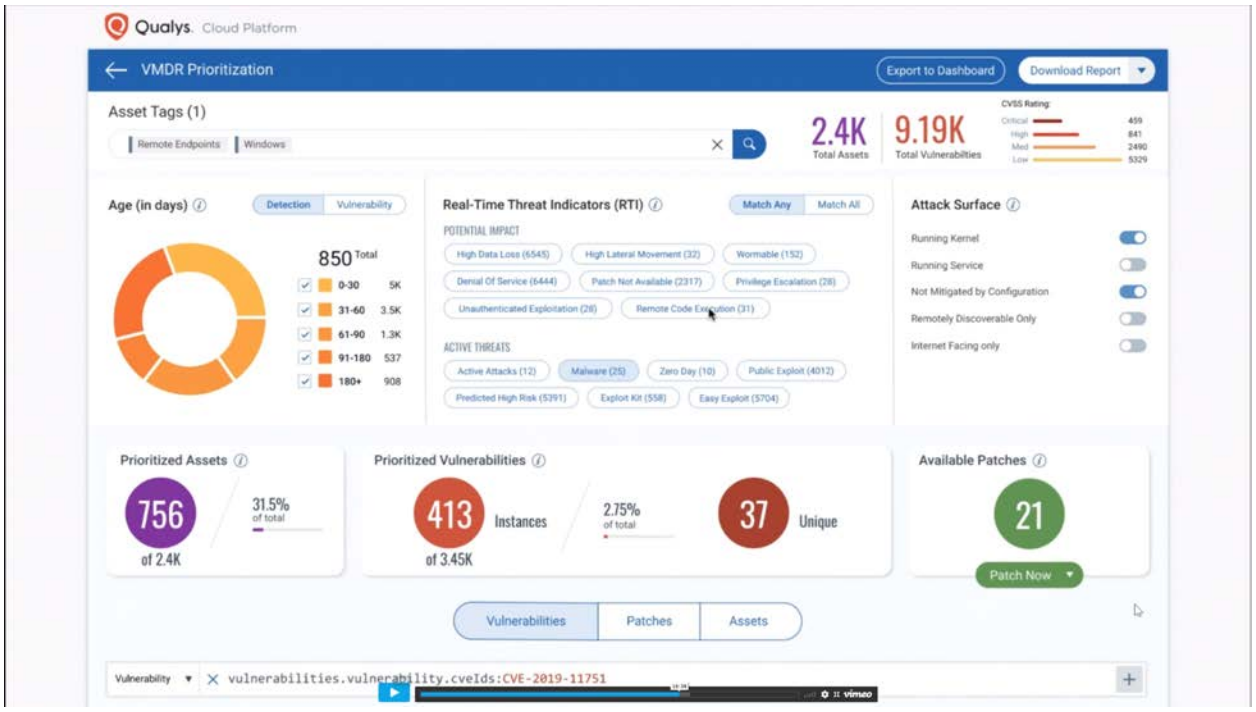

DETECTED VULNERABILITIES (CVES) WITH ACTIVE MALWARE
CVE
TITLE
CVSS
MALWARE
ASSET COUNT
CVE-2017-8570
Microsoft Office Remote Code Execution Vulnerability
7.8
Loki
17
CVE-2019-9081
NVIDIA GeForce Experience Privilege Escalation Vulnerability
9.8
Lucifer
14
CVE-2019-11510
Pulse Secure Pulse Connect Secure
10
Maze
12
CVE-2018-8174
Windows VBScript Engine Remote Code Execution Vulnerability
7.5
Ransomware
7
CVE-2015-1670
Microsoft Font Drivers Remote Code Execution Vulnerabilities (MS15-044)
9.3
W32.CJBF
2
EXPLOITABLE MISCONFIGURATIONS BY MITRE TECHNIQUES
CID
NAME
MITRE TECHNIQUE
ASSET COUNT
9532
Lsass.exe audit mode - Audit Level
Exploitation for credential access
12
13930
Block credential stealing from the Windows local security authority subsystem (lsass.exe)
OS Credential Dumping
8
APT10 - RED LEAVES (TA-17-117A)
SHADOWPAD NETSARANG
NETWORK CONNECTIONS BY COUNTRY
COUNTRY
COUNT
4

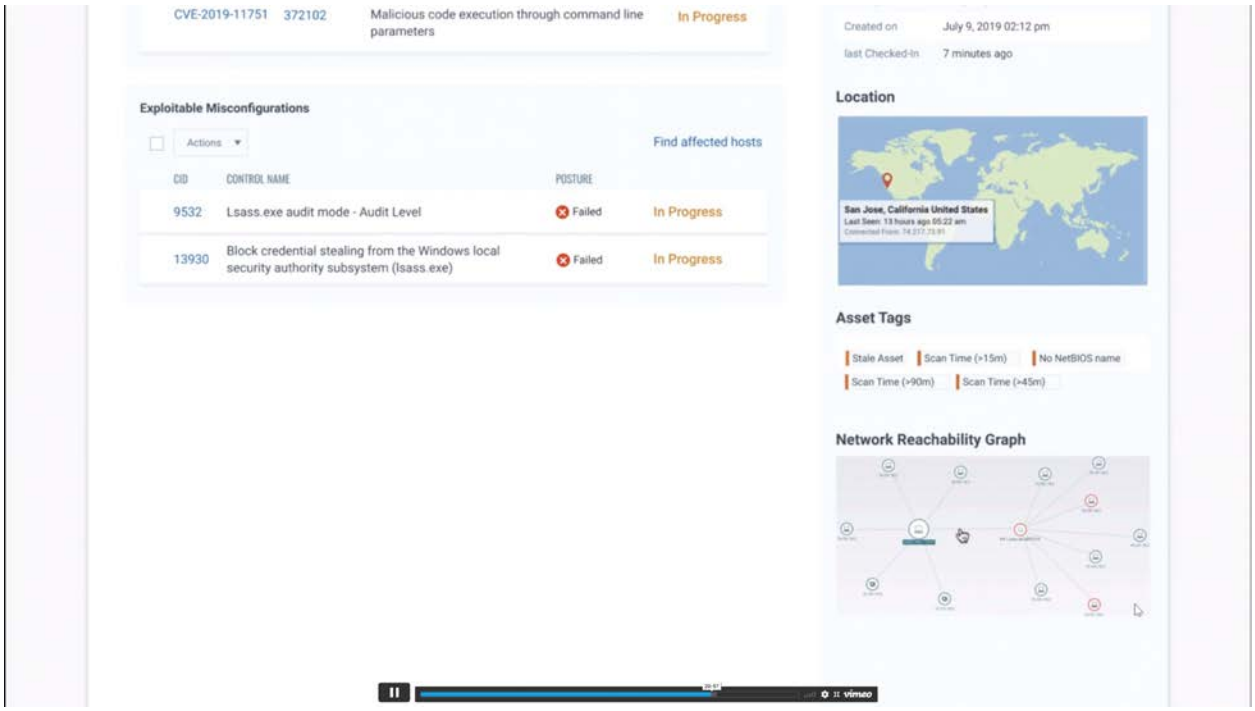

Qualys. Cloud Platform
Endpoint Detection & Response
DASHBOARD
INCIDENTS
HUNTING
ASSET
RESPONSE
Hunting
Active View
Historic View
event.dateTime:2020-07-24 and indicator.score>5
5
Total Events
1
File
4
Process
-
Network
-
Mutex
TYPE
File 1
Process 4
SCORE
10 3
9 1
8 1
Actions
Filter
1 - 5 of 5
TIME
TYPE
OBJECT
ASSET
MALWARE FAMILY
SCORE
ACTION
22 mins ago
1:28:50 PM
COVID 19 - WORLD HEA...
c:\users\john\downloads\covid...
WIN32-ENG-132186
172.16.197.56
Nanocore
8
Quarantine File
3 hours ago
11::11 AM
cujo.exe
C:\$RECYCLE.BIN\S-1-5-21-77\
WIN32-HR-976693
172.16.197.55
Trickbot
10
Kill Process
3 hours ago
12:19:27 AM
notpad.exe
C:\USERS\PUBLIC\TEMP
WIN32-ENG-05843
172.16.101.151
Lokibot
10
Kill Process
3 hours ago
12:12:11 AM
zybnking.exe
C:\PROGRAM FILES (X86)\POLE...
WIN32-ENG-88560
172.16.197.112
Emotet
9
Kill Process
3 hours ago
12:41:09 AM
Svghost.exe
C:\USERS\CHRISC\APPDATA\...
WIN32-ENG-98205
172.16.197.89
Zeus
10
Kill Process

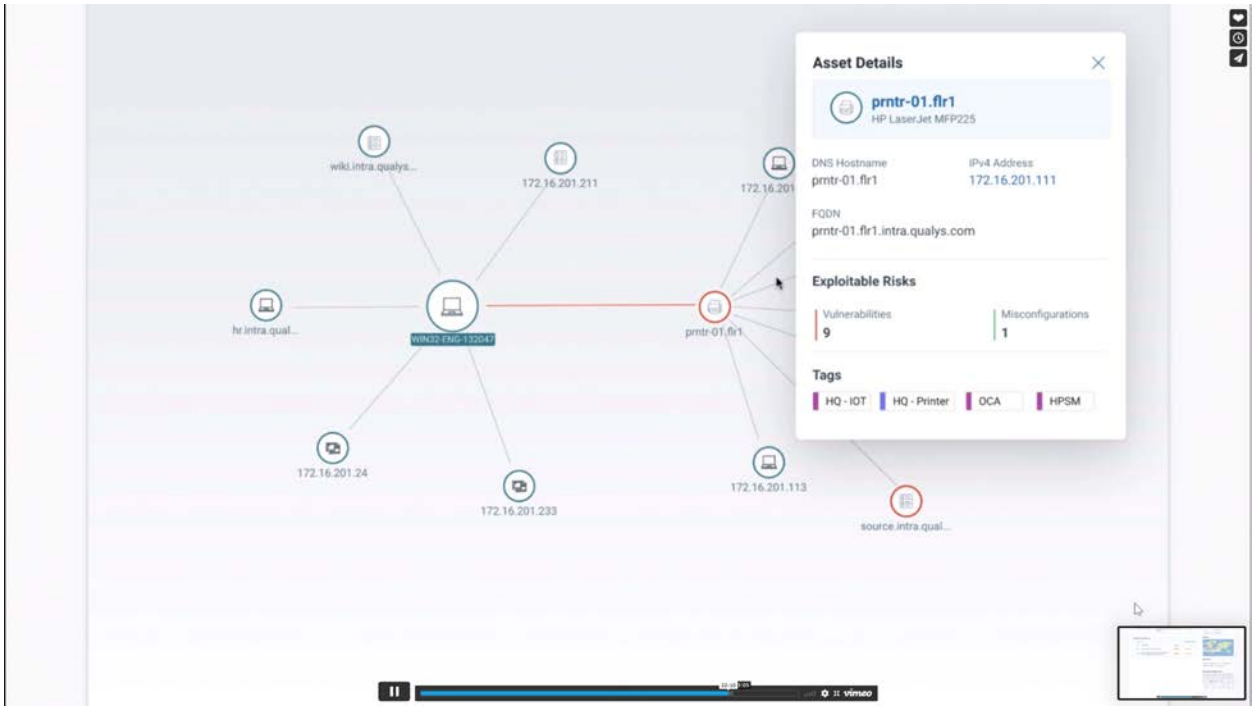

Qualys. Cloud Platform
Event Details
Network
Previous
Next
down.mykings.pw:8888
REMOTE IP: 50.63.202.71 | PORT: 8888
TCP Connection - OPEN by Authenticator.exe
Active
Kill Process
Malware
Family
Category
Score
Process Details
Image Details
Exploitable Risks
Process Details
State
Active
Name
authenticator.exe
Full Path
c:\Users\sscot\AppData\Local\Programs\au...
Arguments
–hidden
Elevated
True
Username
CORP\sscot
ID
7409
Parent Process
ASSET DETAILS
Quarantine Host
WIN32-ENG-57634
OS: Windows
Identification
DNS Hostname
WIN32-ENG-57634.c.gcp-qualys-dem...
FQDN
WIN32-ENG-57634.c.gcp-qualys-dem...
IPv4
172.16.197.189
IPv6
ee90:0:0:0:399b:b361:8e2d:4102
Asset ID
14352156
Resource ID
Host ID
Activity
Last User Login
sscot
Last System Boot
1 day ago
Created on
Jan 9, 2018 02:12 pm
last Checked-In
7 minutes ago
Location
vimeo

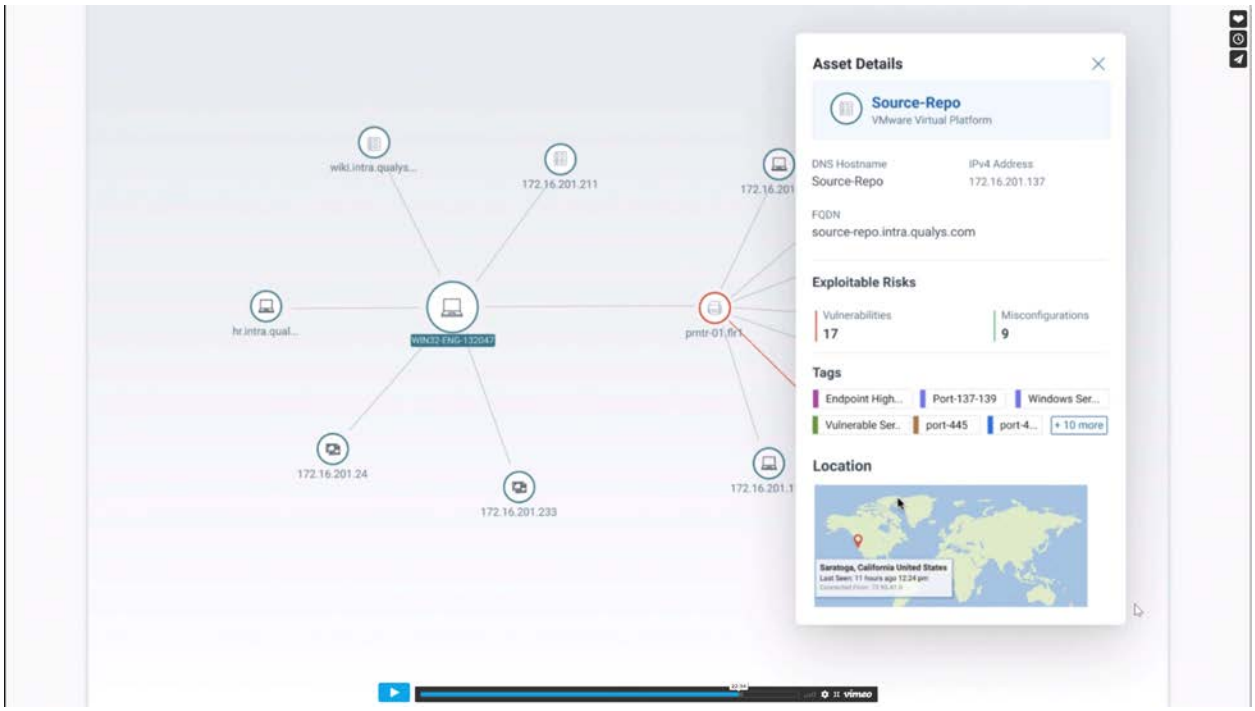

Qualys. Cloud Platform
Process Tree: ytd.exe
firefox.exe
ytd.exe
Network
Process
Process Details
yhost.exe
28 JUL 2020 11:27:09 AM
Blocked
Family
Mimikatz
Category
Hacktool
Score
Additional Insights
T1103
CID-9532
CID-13930
Process Details
State
Blocked
Name
yhost.exe
Full Path
C:\Users\jsmith\AppData\Roaming
Arguments
Elevated
False
Username
CORP\jsmith
ID
9002
Parent ID
vimeo


Qualys. Cloud Platform
Asset Details: WIN32-ENG-132047
INVENTORY
Asset Summary
System Information
Network Information
Open Ports
Installed Software
Traffic Summary
SECURITY
Vulnerabilities
VMDR Prioritization
Patch Management
Endpoint Detection & Response
Certificates
COMPLIANCE
Policy Compliance
File Integrity Monitoring
SENSORS
Agent Summary
Connector Summary
Passive Sensor
Alert Notifications
Agent Summary
Asset Summary
WIN32-ENG-132047
Microsoft Windows 10 Enterprise (1909 insider Preview Build 18363 64-Bit)
Lenovo ThinkPad X1 Carbon (6th Gen) 20KH006XUS
Identification
DNS Hostname WIN32-ENG-132047.c.gcp-qualys-dem...
FQDN WIN32-ENG-132047.c.gcp-qualys-dem...
IPv4 172.16.197.89
IPv6 fe80:0:0:0:399b:b361:8e2d:4102
Asset ID 14492105
Resource ID -
Host ID -
Location
San Jose, California United States
Last Seen: 13 hours ago 05:22 am
Agent Activity
Last User Login CORP\jsmith
Last System Boot 5 days ago
Created On Nov 28, 2019 12:52 am
Tags
Stale Asset
Scan Time (>15m)
No NetBIOS name
Scan Time (>90m)
Scan Time (>45m)
OS:Windows NT
Type: Workstation
Scan Time (>30m)
OS:Windows..
No Hostname
No OS Detected
Decommisioned Assets

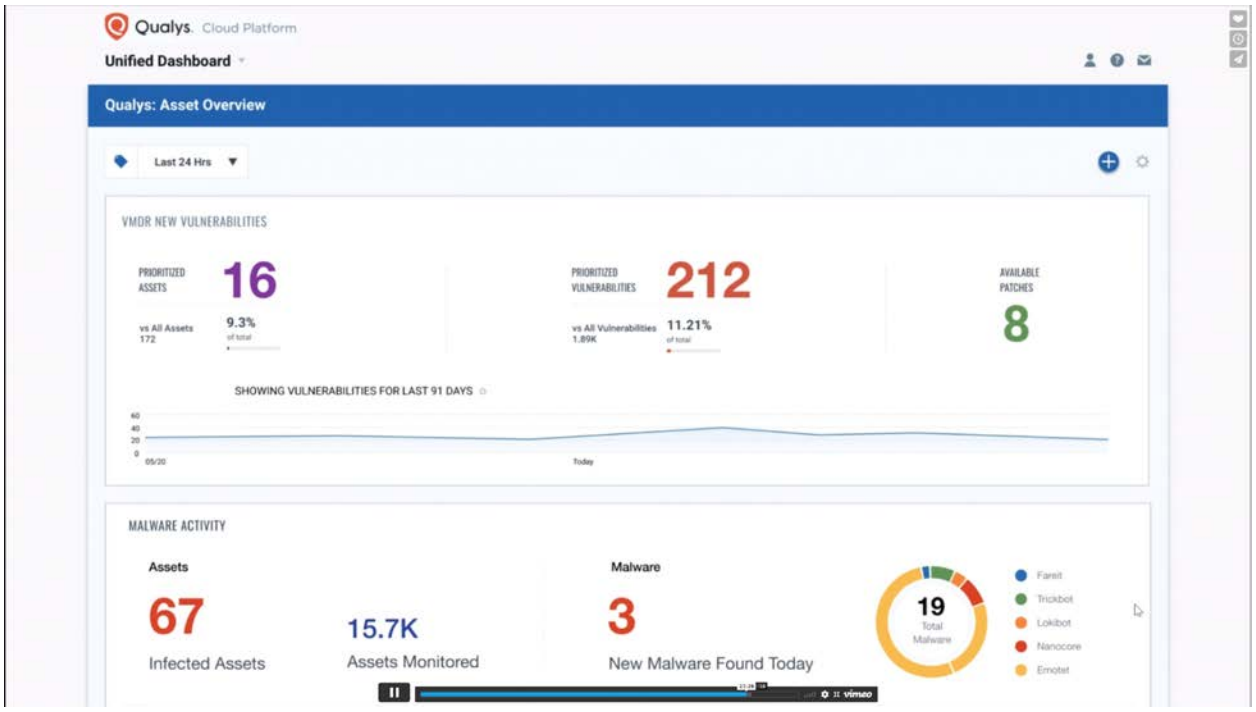

Qualys. Cloud Platform
VMDR Prioritization
Export to Dashboard
Download Report
Asset Tags (1)
Remote Endpoints
Windows
2.4K
Total Assets
9.19K
Total Vulnerabilities
CVSS Rating:
Critical 459
High 841
Med 2490
Low 5329
Age (in days)
Detection
Vulnerability
850 Total
0-30 5K
31-60 3.5K
61-90 1.3K
91-180 537
180+ 908
Real-Time Threat Indicators (RTI)
Match Any
Match All
POTENTIAL IMPACT
High Data Loss (6545)
High Lateral Movement (32)
Wormable (152)
Denial Of Service (6444)
Patch Not Available (2317)
Privilege Escalation (28)
Unauthenticated Exploitation (28)
Remote Code Execution (31)
ACTIVE THREATS
Active Attacks (12)
Malware (25)
Zero Day (10)
Public Exploit (4012)
Predicted High Risk (5391)
Exploit Kit (558)
Easy Exploit (5704)
Attack Surface
Running Kernel
Running Service
Not Mitigated by Configuration
Remotely Discoverable Only
Internet Facing only
Prioritized Assets
756
of 2.4K
31.5%
of total
Prioritized Vulnerabilities
413
Instances
of 3.45K
2.75%
of total
37
Unique
Available Patches
21
Patch Now
Vulnerabilities
Patches
Assets
Vulnerability
vulnerabilities.vulnerability.cveIds:CVE-2019-11751


CVE-2019-11751 372102
Malicious code execution through command line parameters
In Progress
Exploitable Misconfigurations
Actions
Find affected hosts
CID
CONTROL NAME
POSTURE
9532
Lsass.exe audit mode - Audit Level
Failed
In Progress
13930
Block credential stealing from the Windows local security authority subsystem (lsass.exe)
Failed
In Progress
Created on
July 9, 2019 02:12 pm
last Checked-In
7 minutes ago
Location
San Jose, California United States
Asset Tags
Stale Asset
Scan Time (>15m)
No NetBIOS name
Scan Time (>90m)
Scan Time (>45m)
Network Reachability Graph


Asset Details
prntr-01.flr1
HP LaserJet MFP225
DNS Hostname
prntr-01.flr1
IPv4 Address
172.16.201.111
FQDN
prntr-01.flr1.intra.qualys.com
Exploitable Risks
Vulnerabilities
9
Misconfigurations
1
Tags
HQ - IOT
HQ - Printer
OCA
HPSM
wiki.intra.qualys...
172.16.201.211
hr.intra.qual...
WIN32-ENG-132047
prntr-01.flr1
172.16.201.24
172.16.201.233
172.16.201.113
source.intra.qual...


Asset Details
Source-Repo
VMware Virtual Platform
DNS Hostname
Source-Repo
IPv4 Address
172.16.201.137
FQDN
source-repo.intra.qualys.com
Exploitable Risks
Vulnerabilities
17
Misconfigurations
9
Tags
Endpoint High...
Port-137-139
Windows Ser...
Vulnerable Ser...
port-445
port-4...
+ 10 more
Location
Saratoga, California United States
wiki.intra.qualys...
172.16.201.211
hr.intra.qual...
WIN32-ENG-132047
172.16.201.24
172.16.201.233
vimeo


Qualys. Cloud Platform
Network Reachability Graph
wiki.intra.qualys...
172.16.201.211
172.16.201.245
172.16.201.32
HR SharePoint
hr.intra.qual...
WIN32-ENG-132047
pmtr-01.fir1
172.16.201.13
172.16.201.234
172.16.201.24
172.16.201.233
172.16.201.113


Qualys. Cloud Platform
Unified Dashboard
Qualys: Asset Overview
Last 24 Hrs
VMDR NEW VULNERABILITIES
PRIORITIZED ASSETS
16
vs All Assets 172
9.3%
PRIORITIZED VULNERABILITIES
212
vs All Vulnerabilities 1.89K
11.21%
AVAILABLE PATCHES
8
SHOWING VULNERABILITIES FOR LAST 91 DAYS
MALWARE ACTIVITY
Assets
67
Infected Assets
15.7K
Assets Monitored
Malware
3
New Malware Found Today
19
Total Malware
Farsit
Trickbot
Lokibot
Nanocore
Emotet

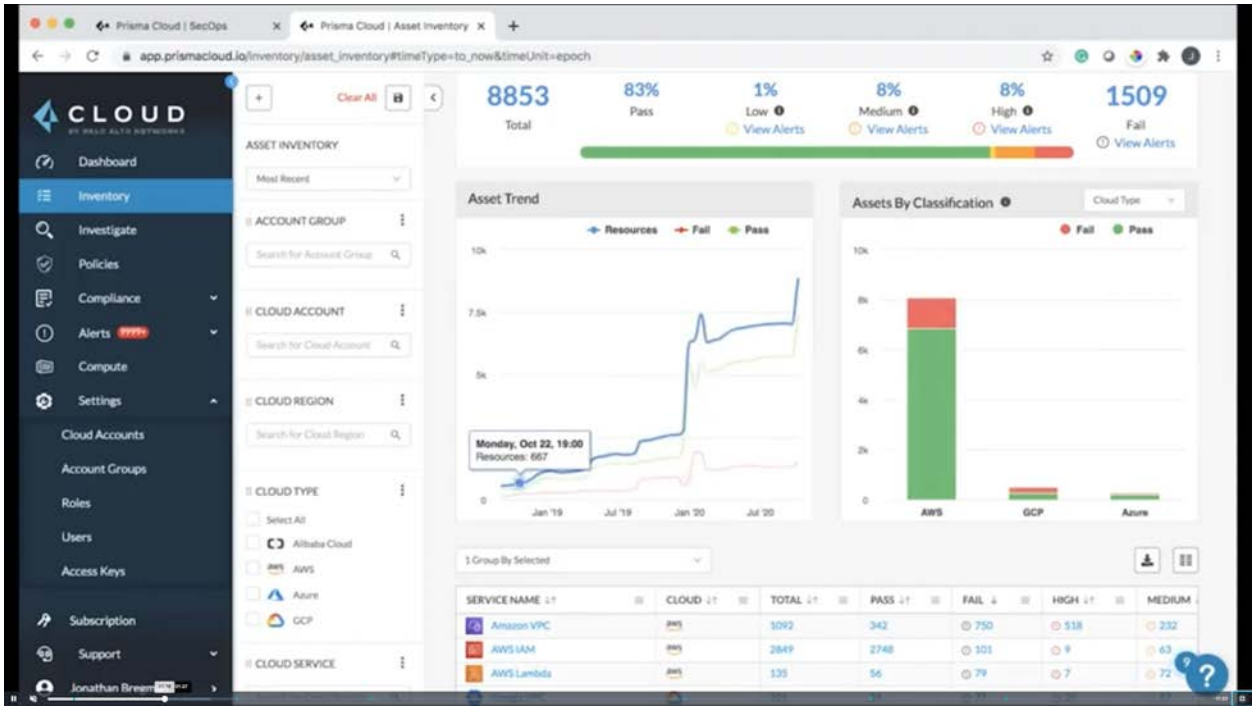
Palo Alto Networks - Prisma Cloud platform

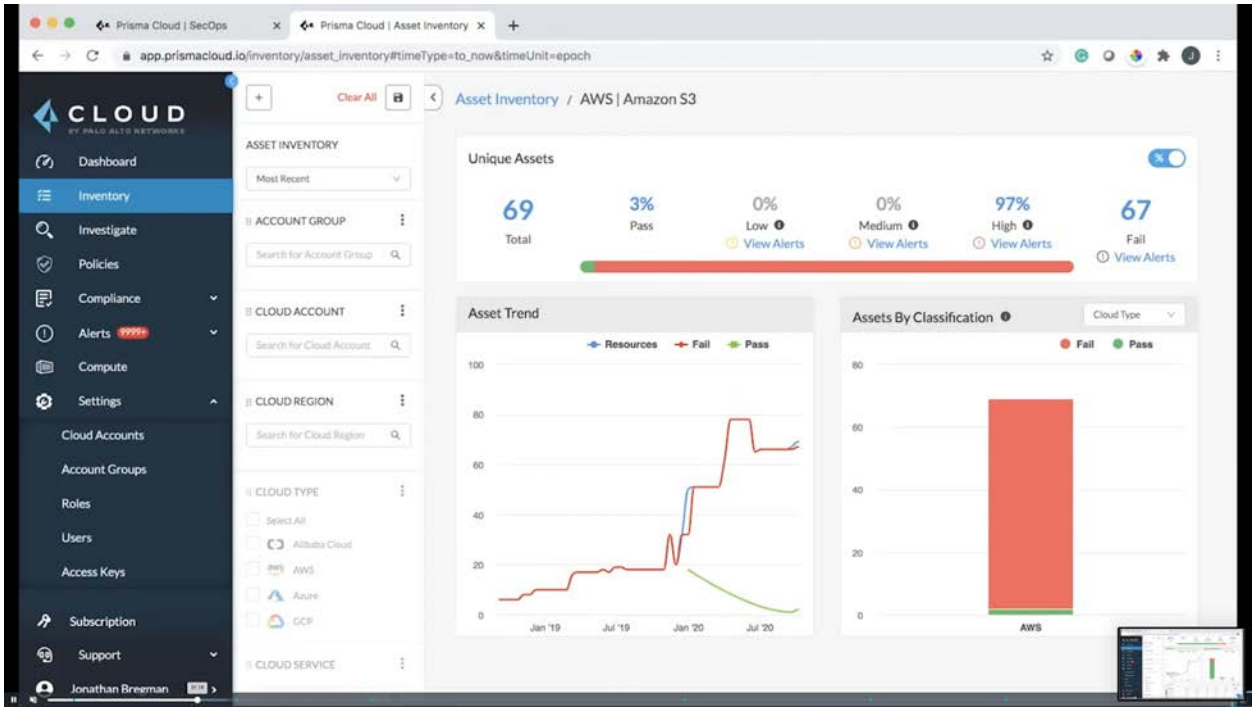
One of the most comprehensive cloud native security platforms in the market, with deep capabilities to help organizations with workload security. Under Prisma Cloud there is: Cloud Security Posture Management, Cloud Workload Protection, Cloud Infrastructure Entitlement Management, and Cloud Network Security.

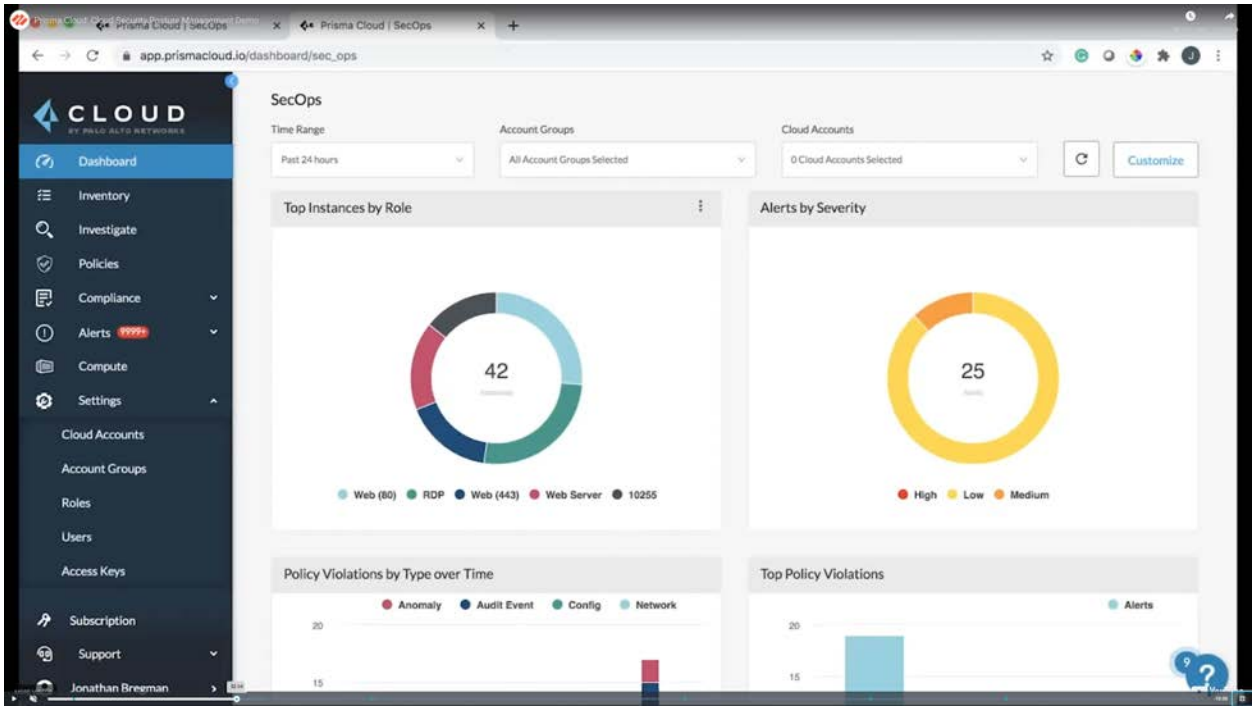
[Product Demo]

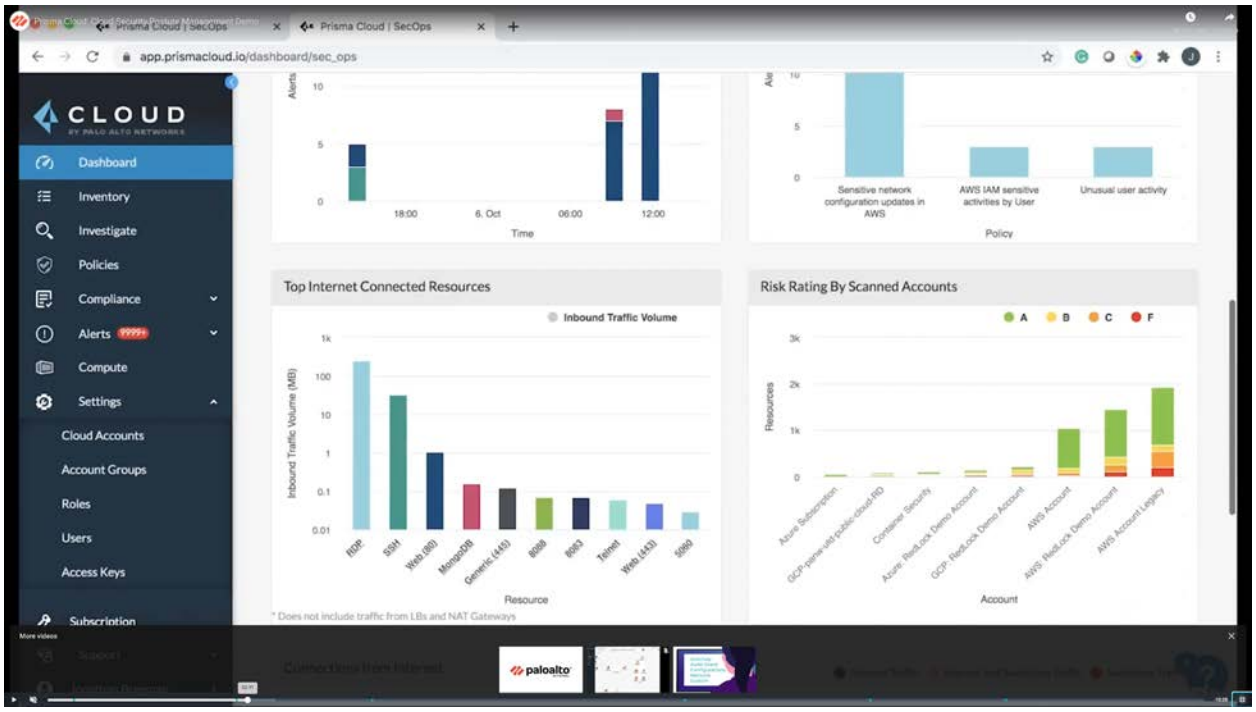
- **Key Values and Differentiators**:
    - Prisma Cloud platform is a new effort by Palo Alto Networks defined as a Cloud Native Security Platform
    - Provides container and cloud workload policy, threat detection, and control
    - Full cloud workload visibility, including serverless functions
    - Capabilities to secure an end-to-end cloud native deployment
    - Vulnerability management and runtime protection against threats
- **Features include:**
    - Visibility, Compliance, and Governance
    - Data, host, IAM, container, serverless, and web app/API security
    - Maintain compliance across AWS, Azure, GCP, and Alibaba Cloud
    - Identity-based microsegmentation

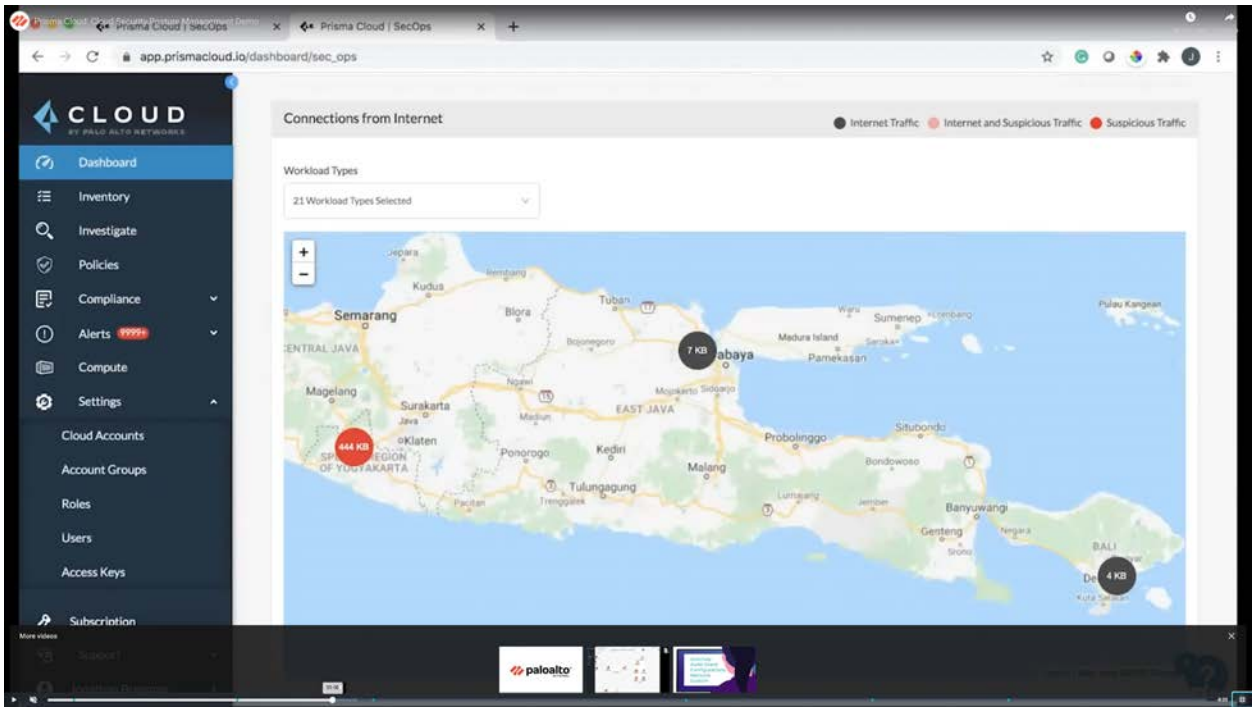
Screenshots of UI:

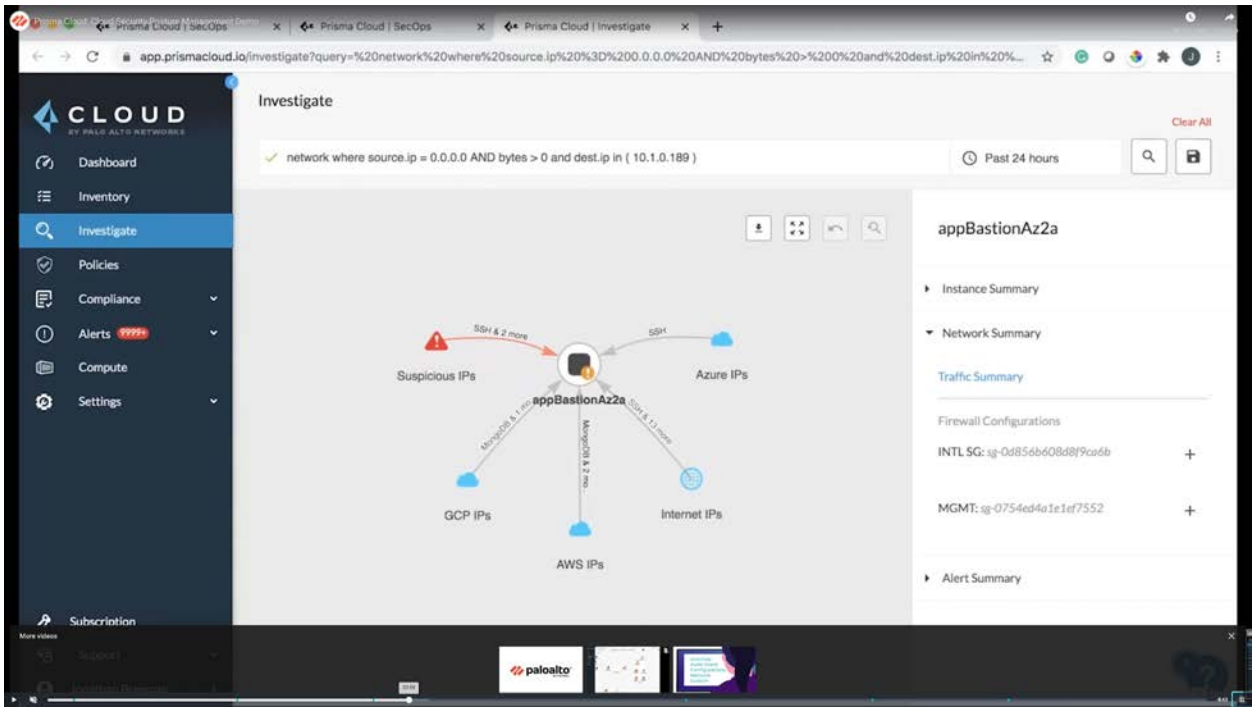


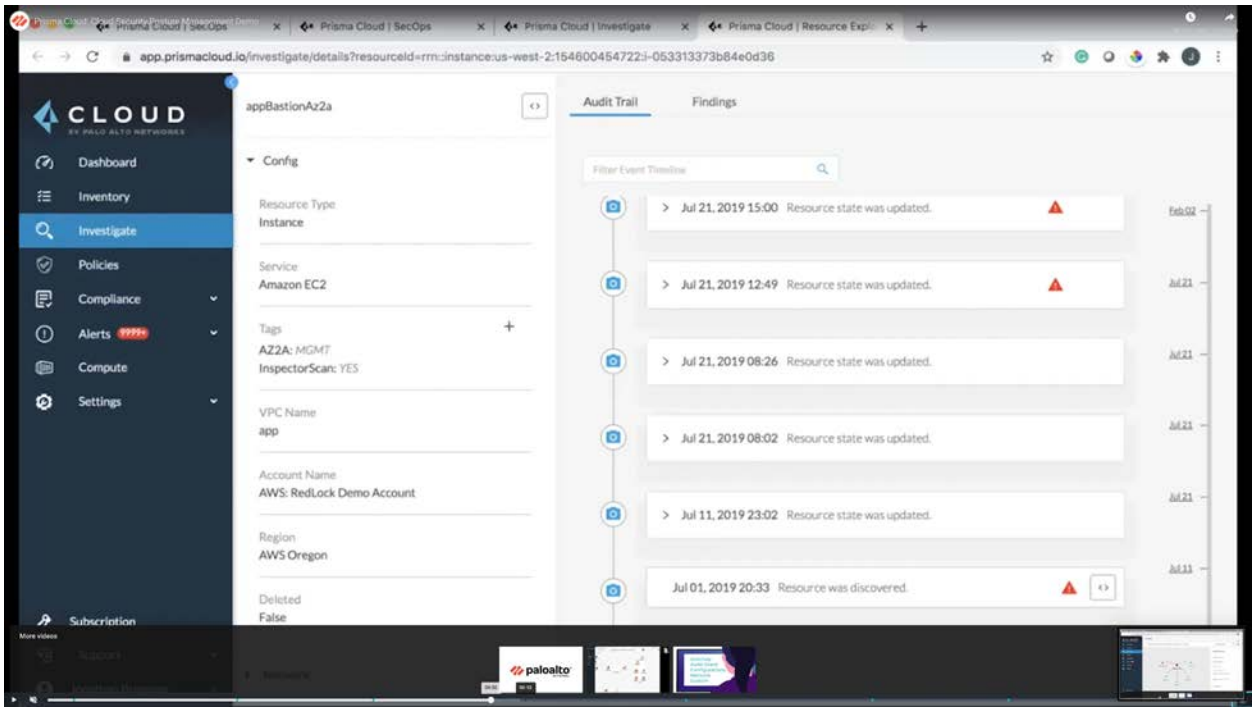

Prisma Cloud | SecOps
Prisma Cloud | Asset Inventory
app.prismacloud.io/inventory/asset_inventory#timeType=to_now&timeUnit=epoch
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Compute
Settings
Cloud Accounts
Account Groups
Roles
Users
Access Keys
Subscription
Support
Jonathan Breeman
Clear All
Asset Inventory / AWS | Amazon S3
ASSET INVENTORY
Most Recent
ACCOUNT GROUP
CLOUD ACCOUNT
CLOUD REGION
CLOUD TYPE
CLOUD SERVICE
Unique Assets
69
Total
3%
Pass
0%
Low
View Alerts
0%
Medium
View Alerts
97%
High
View Alerts
67
Fail
View Alerts
Asset Trend
Resources
Fail
Pass
Jan '19
Jul '19
Jan '20
Jul '20
Assets By Classification
Cloud Type
AWS

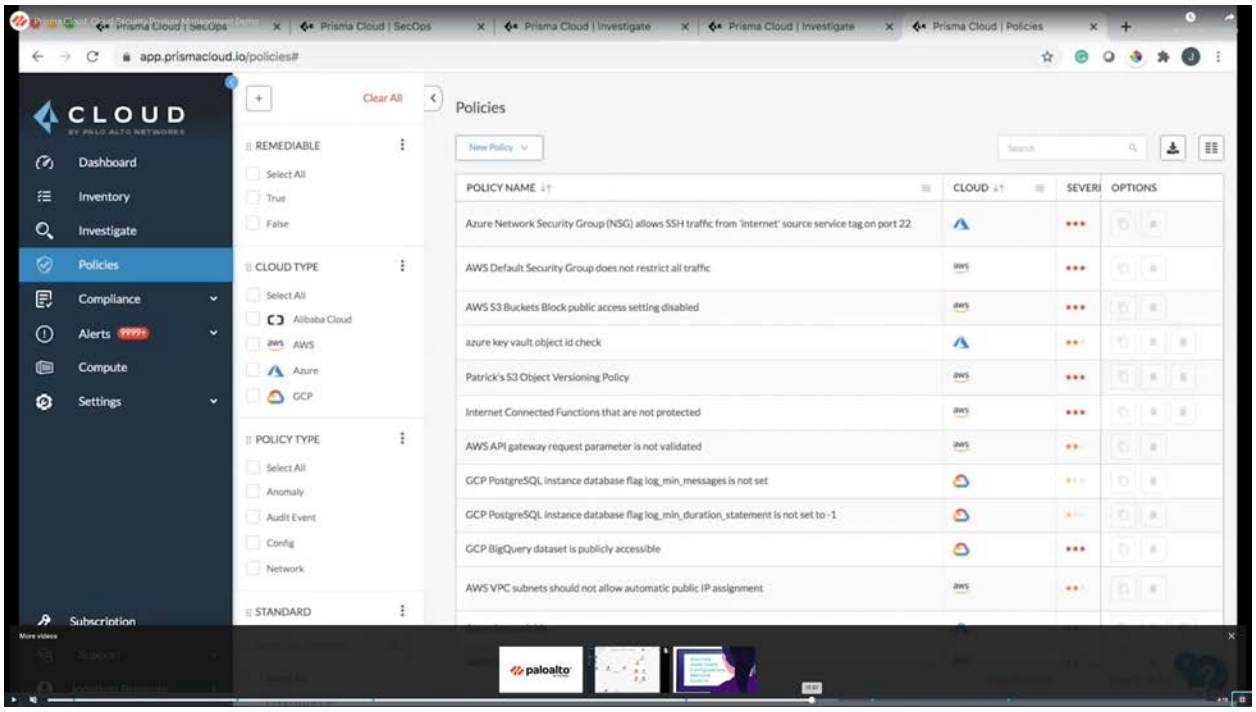

Prisma Cloud | SecOps
app.prismacloud.io/dashboard/sec_ops
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Compute
Settings
Cloud Accounts
Account Groups
Roles
Users
Access Keys
Subscription
Support
Jonathan Breeman
SecOps
Time Range
Past 24 hours
Account Groups
All Account Groups Selected
Cloud Accounts
0 Cloud Accounts Selected
Customize
Top Instances by Role
42
Web (80)
RDP
Web (443)
Web Server
10255
Alerts by Severity
25
High
Low
Medium
Policy Violations by Type over Time
Anomaly
Audit Event
Config
Network
Top Policy Violations
Alerts

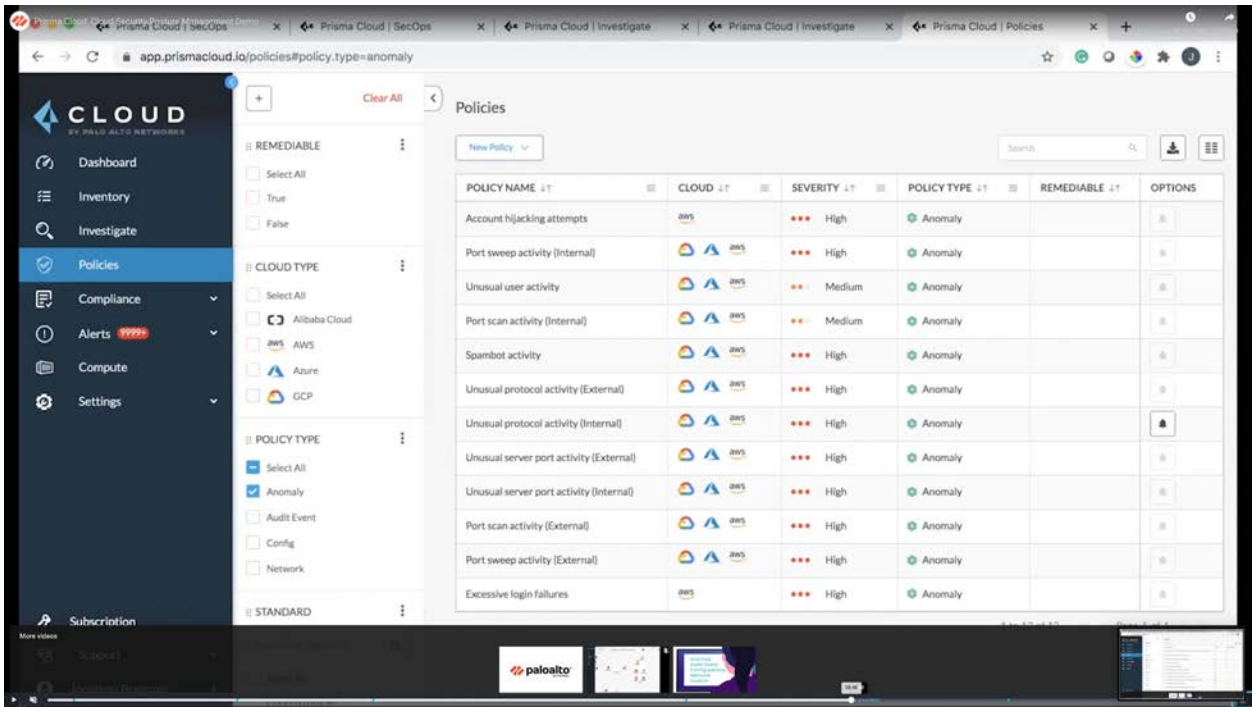

Prisma Cloud | SecOps
app.prismacloud.io/dashboard/sec_ops
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Compute
Settings
Cloud Accounts
Account Groups
Roles
Users
Access Keys
Subscription
Alerts
Time
Sensitive network configuration updates in AWS
AWS IAM sensitive activities by User
Unusual user activity
Policy
Top Internet Connected Resources
Inbound Traffic Volume
Inbound Traffic Volume (MB)
Resource
* Does not include traffic from LBs and NAT Gateways
Risk Rating By Scanned Accounts
A
B
C
F
Resources
Account

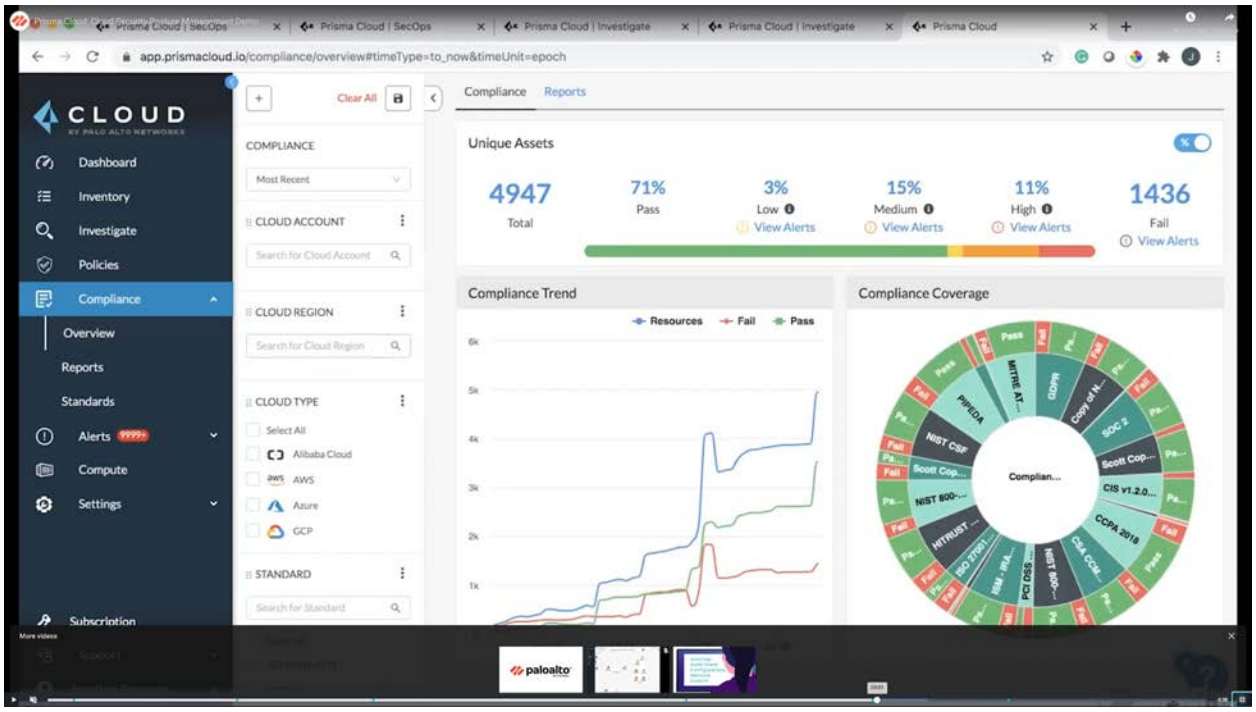

Prisma Cloud | SecOps
app.prismacloud.io/dashboard/sec_ops
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Compute
Settings
Cloud Accounts
Account Groups
Roles
Users
Access Keys
Subscription
Connections from Internet
Internet Traffic
Internet and Suspicious Traffic
Suspicious Traffic
Workload Types
21 Workload Types Selected
Semarang
Surakarta
Magelang
Klaten
Tulungagung
Malang
Kediri
Ponorogo
Probolinggo
Banyuwangi
Genteng
Pamekasan
Madura Island
Sumenep
Situbondo
Bondowoso
Pulau Kangean
BALI
7 KB
444 KB
4 KB

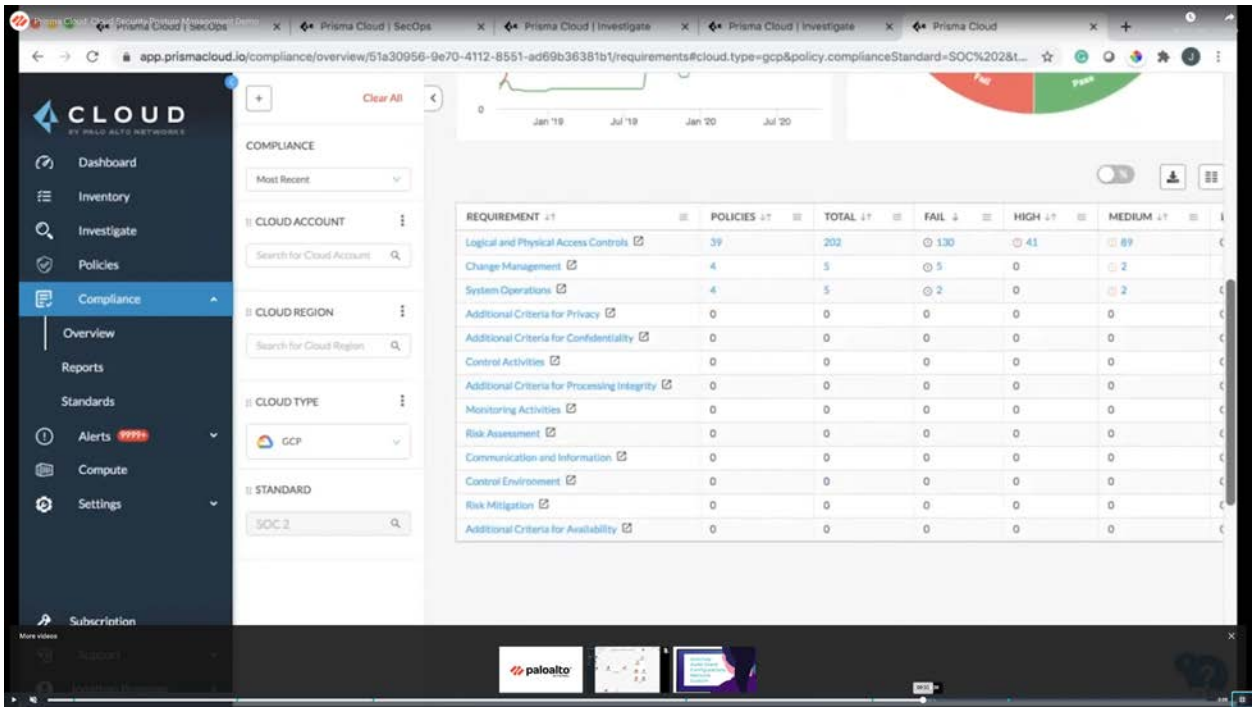

Prisma Cloud | SecOps
Prisma Cloud | Investigate
app.prismacloud.io/investigate?query=%20network%20where%20source.ip%20%3D%200.0.0.0%20AND%20bytes%20>%200%20and%20dest.ip%20in%20%...
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Compute
Settings
Subscription
Investigate
Clear All
network where source.ip = 0.0.0.0 AND bytes > 0 and dest.ip in (10.1.0.189)
Past 24 hours
appBastionAz2a
Instance Summary
Network Summary
Traffic Summary
Firewall Configurations
INTL SG: sg-0d856b608d8f9ca6b
MGMT: sg-0754ed4a1e1ef7552
Alert Summary
SSH & 2 more
SSH
Suspicious IPs
Azure IPs
appBastionAz2a
GCP IPs
Internet IPs
AWS IPs

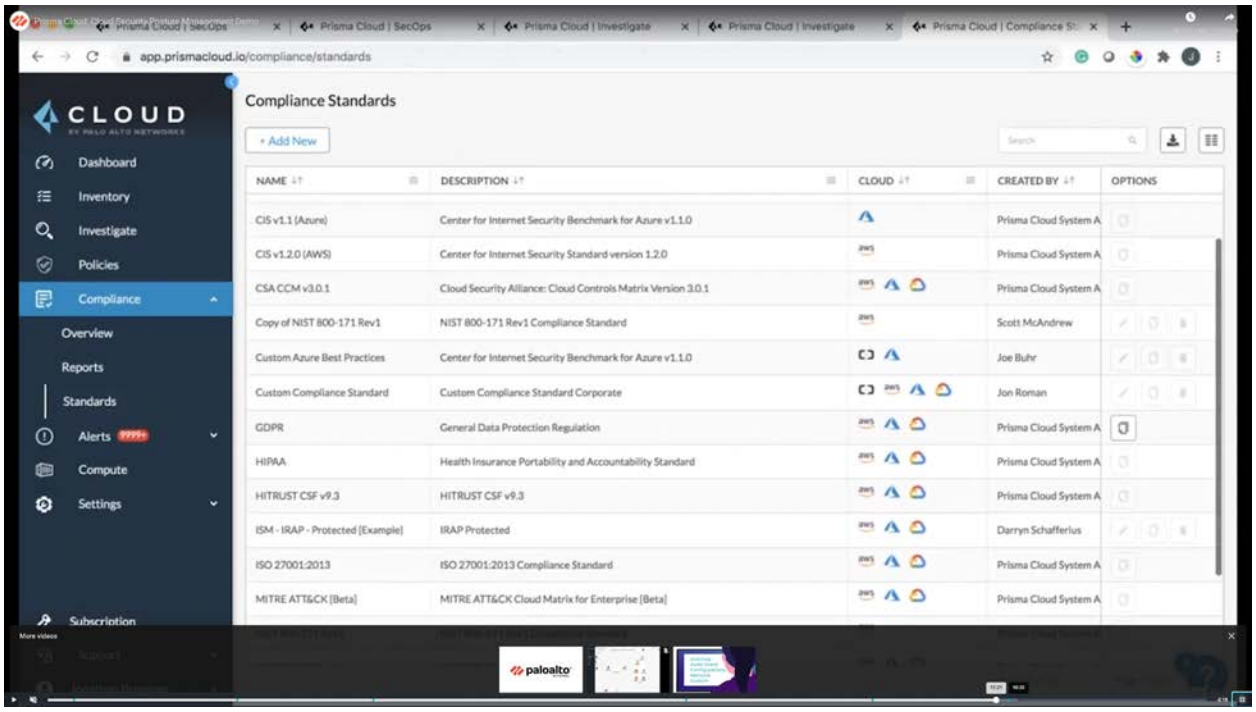

Prisma Cloud | SecOps
Prisma Cloud | Investigate
Prisma Cloud | Resource Exp...
app.prismacloud.io/investigate/details?resourceId=rrn::instance:us-west-2:154600454722:i-053313373b84e0d36
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Compute
Settings
Subscription
appBastionAz2a
Config
Resource Type
Instance
Service
Amazon EC2
Tags
AZ2A: MGMT
InspectorScan: YES
VPC Name
app
Account Name
AWS: RedLock Demo Account
Region
AWS Oregon
Deleted
False
Audit Trail
Findings
Filter Event Timeline
Jul 21, 2019 15:00 Resource state was updated.
Jul 21, 2019 12:49 Resource state was updated.
Jul 21, 2019 08:26 Resource state was updated.
Jul 21, 2019 08:02 Resource state was updated.
Jul 11, 2019 23:02 Resource state was updated.
Jul 01, 2019 20:33 Resource was discovered.

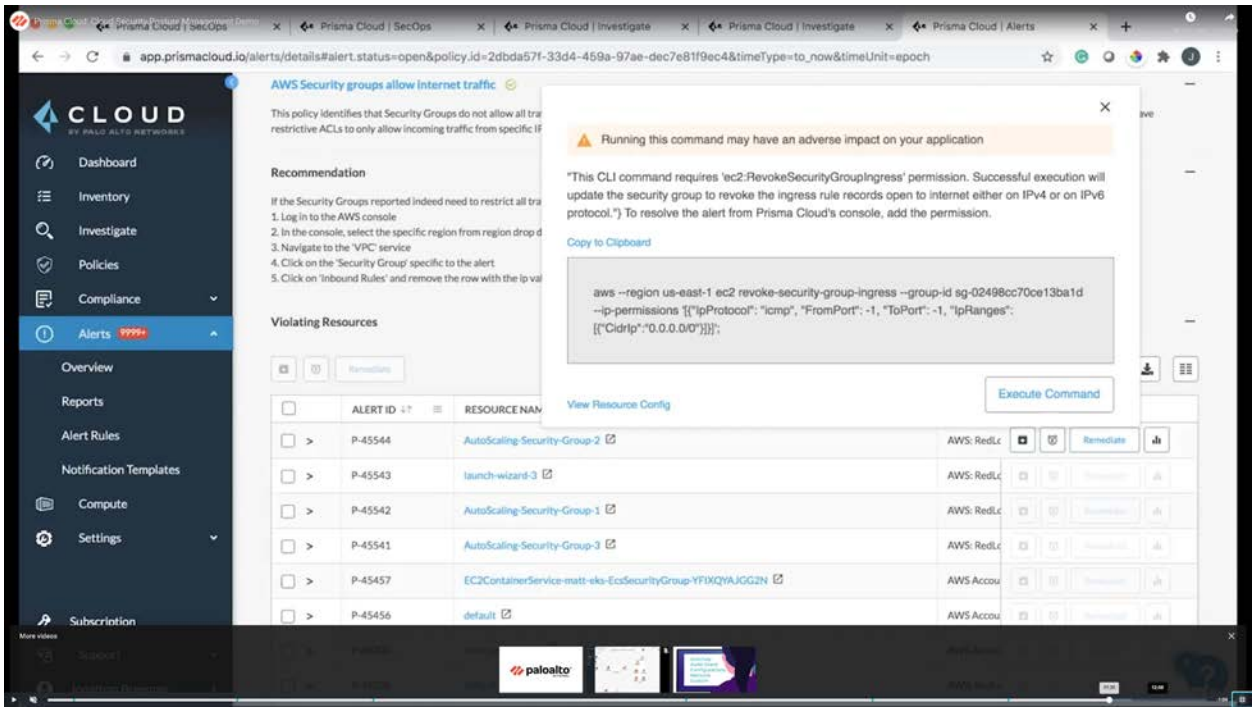

Prisma Cloud | SecOps
Prisma Cloud | Investigate
Prisma Cloud | Policies
app.prismacloud.io/policies#
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Compute
Settings
Subscription
Clear All
REMEDIABLE
Select All
True
False
CLOUD TYPE
Alibaba Cloud
AWS
Azure
GCP
POLICY TYPE
Anomaly
Audit Event
Config
Network
STANDARD
Policies
New Policy
POLICY NAME
CLOUD
SEVERI
OPTIONS
Azure Network Security Group (NSG) allows SSH traffic from 'internet' source service tag on port 22
AWS Default Security Group does not restrict all traffic
AWS S3 Buckets Block public access setting disabled
azure key vault object id check
Patrick's S3 Object Versioning Policy
Internet Connected Functions that are not protected
AWS API gateway request parameter is not validated
GCP PostgreSQL instance database flag log_min_messages is not set
GCP PostgreSQL instance database flag log_min_duration_statement is not set to -1
GCP BigQuery dataset is publicly accessible
AWS VPC subnets should not allow automatic public IP assignment
More videos

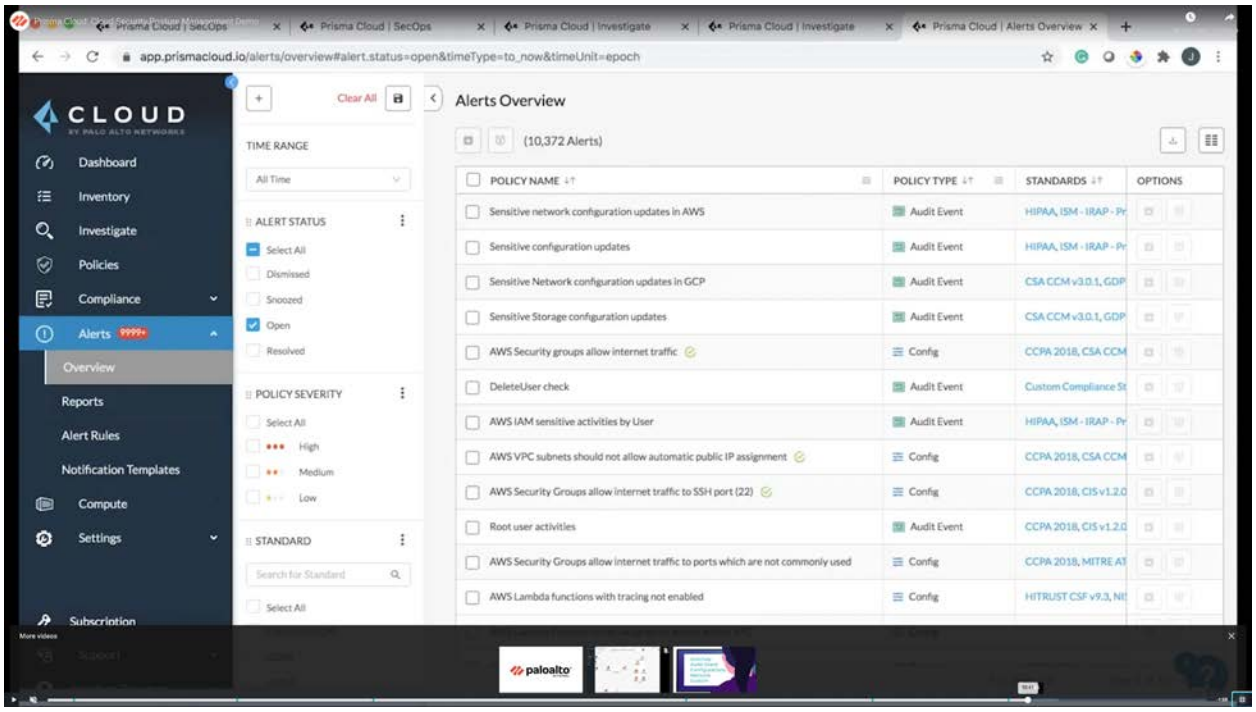

Prisma Cloud | SecOps
Prisma Cloud | Investigate
Prisma Cloud | Policies
app.prismacloud.io/policies#policy.type=anomaly
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Compute
Settings
Subscription
Clear All
REMEDIABLE
Select All
True
False
CLOUD TYPE
Alibaba Cloud
AWS
Azure
GCP
POLICY TYPE
Select All
Anomaly
Audit Event
Config
Network
STANDARD
Policies
New Policy
POLICY NAME
CLOUD
SEVERITY
POLICY TYPE
REMEDIABLE
OPTIONS
Account hijacking attempts
Port sweep activity (Internal)
Unusual user activity
Port scan activity (Internal)
Spambot activity
Unusual protocol activity (External)
Unusual protocol activity (Internal)
Unusual server port activity (External)
Unusual server port activity (Internal)
Port scan activity (External)
Port sweep activity (External)
Excessive login failures
High
Medium
Anomaly
More videos


Prisma Cloud | SecOps
Prisma Cloud | Investigate
Prisma Cloud | Investigate
Prisma Cloud
app.prismacloud.io/compliance/overview#timeType=to_now&timeUnit=epoch
CLOUD
BY PALO ALTO NETWORKS
Dashboard
Inventory
Investigate
Policies
Compliance
Overview
Reports
Standards
Alerts 9999+
Compute
Settings
Subscription
Clear All
Compliance
Reports
COMPLIANCE
Most Recent
CLOUD ACCOUNT
Search for Cloud Account
CLOUD REGION
Search for Cloud Region
CLOUD TYPE
Select All
Alibaba Cloud
AWS
Azure
GCP
STANDARD
Search for Standard
Unique Assets
4947
Total
71%
Pass
3%
Low
View Alerts
15%
Medium
View Alerts
11%
High
View Alerts
1436
Fail
View Alerts
Compliance Trend
Resources
Fail
Pass
6k
5k
4k
3k
2k
1k
Compliance Coverage
GDPR
SOC 2
CIS v1.2.0...
CCPA 2018
NIST 800-...
PCI DSS
ISO 27001...
HITRUST ...
NIST 800-...
Scott Cop...
NIST CSF
PIPEDA
MITRE AT...
Compliance...
More videos
paloalto


Prisma Cloud | SecOps
Prisma Cloud | Investigate
Prisma Cloud | Investigate
Prisma Cloud
app.prismacloud.io/compliance/overview/51a30956-9e70-4112-8551-ad69b36381b1/requirements#cloud.type=gcp&policy.complianceStandard=SOC%202&t...
CLOUD
BY PALO ALTO NETWORKS
Dashboard
Inventory
Investigate
Policies
Compliance
Overview
Reports
Standards
Alerts 9999+
Compute
Settings
Subscription
Clear All
COMPLIANCE
Most Recent
CLOUD ACCOUNT
Search for Cloud Account
CLOUD REGION
Search for Cloud Region
CLOUD TYPE
GCP
STANDARD
SOC 2
Jan '19
Jul '19
Jan '20
Jul '20
REQUIREMENT
POLICIES
TOTAL
FAIL
HIGH
MEDIUM
Logical and Physical Access Controls 39 202 130 41 89
Change Management 4 5 5 0 2
System Operations 4 5 2 0 2
Additional Criteria for Privacy 0 0 0 0 0
Additional Criteria for Confidentiality 0 0 0 0 0
Control Activities 0 0 0 0 0
Additional Criteria for Processing Integrity 0 0 0 0 0
Monitoring Activities 0 0 0 0 0
Risk Assessment 0 0 0 0 0
Communication and Information 0 0 0 0 0
Control Environment 0 0 0 0 0
Risk Mitigation 0 0 0 0 0
Additional Criteria for Availability 0 0 0 0 0
More videos
paloalto


Prisma Cloud | SecOps
Prisma Cloud | Investigate
Prisma Cloud | Investigate
Prisma Cloud | Compliance St
app.prismacloud.io/compliance/standards
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Overview
Reports
Standards
Alerts
Compute
Settings
Subscription
Compliance Standards
+ Add New
NAME
DESCRIPTION
CLOUD
CREATED BY
OPTIONS
CIS v1.1 (Azure)
Center for Internet Security Benchmark for Azure v1.1.0
Prisma Cloud System A
CIS v1.2.0 (AWS)
Center for Internet Security Standard version 1.2.0
Prisma Cloud System A
CSA CCM v3.0.1
Cloud Security Alliance: Cloud Controls Matrix Version 3.0.1
Prisma Cloud System A
Copy of NIST 800-171 Rev1
NIST 800-171 Rev1 Compliance Standard
Scott McAndrew
Custom Azure Best Practices
Center for Internet Security Benchmark for Azure v1.1.0
Joe Buhr
Custom Compliance Standard
Custom Compliance Standard Corporate
Jon Roman
GDPR
General Data Protection Regulation
Prisma Cloud System A
HIPAA
Health Insurance Portability and Accountability Standard
Prisma Cloud System A
HITRUST CSF v9.3
HITRUST CSF v9.3
Prisma Cloud System A
ISM - IRAP - Protected [Example]
IRAP Protected
Darryn Schafferius
ISO 27001:2013
ISO 27001:2013 Compliance Standard
Prisma Cloud System A
MITRE ATT&CK [Beta]
MITRE ATT&CK Cloud Matrix for Enterprise [Beta]
Prisma Cloud System A
paloalto


Prisma Cloud | SecOps
Prisma Cloud | Investigate
Prisma Cloud | Alerts
app.prismacloud.io/alerts/details#alert.status=open&policy.id=2dbda57f-33d4-459a-97ae-dec7e81f9ec4&timeType=to_now&timeUnit=epoch
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Overview
Reports
Alert Rules
Notification Templates
Compute
Settings
Subscription
AWS Security groups allow internet traffic
Recommendation
Violating Resources
Running this command may have an adverse impact on your application
"This CLI command requires 'ec2:RevokeSecurityGroupIngress' permission. Successful execution will update the security group to revoke the ingress rule records open to internet either on IPv4 or on IPv6 protocol.") To resolve the alert from Prisma Cloud's console, add the permission.
Copy to Clipboard
aws --region us-east-1 ec2 revoke-security-group-ingress --group-id sg-02498cc70ce13ba1d --ip-permissions '[{"IpProtocol": "icmp", "FromPort": -1, "ToPort": -1, "IpRanges": [{"CidrIp":"0.0.0.0/0"}]}]';
View Resource Config
Execute Command
ALERT ID
RESOURCE NAME
P-45544 AutoScaling-Security-Group-2
P-45543 launch-wizard-3
P-45542 AutoScaling-Security-Group-1
P-45541 AutoScaling-Security-Group-3
P-45457 EC2ContainerService-matt-eks-EcsSecurityGroup-YFIXQYAJGG2N
P-45456 default
Remediate

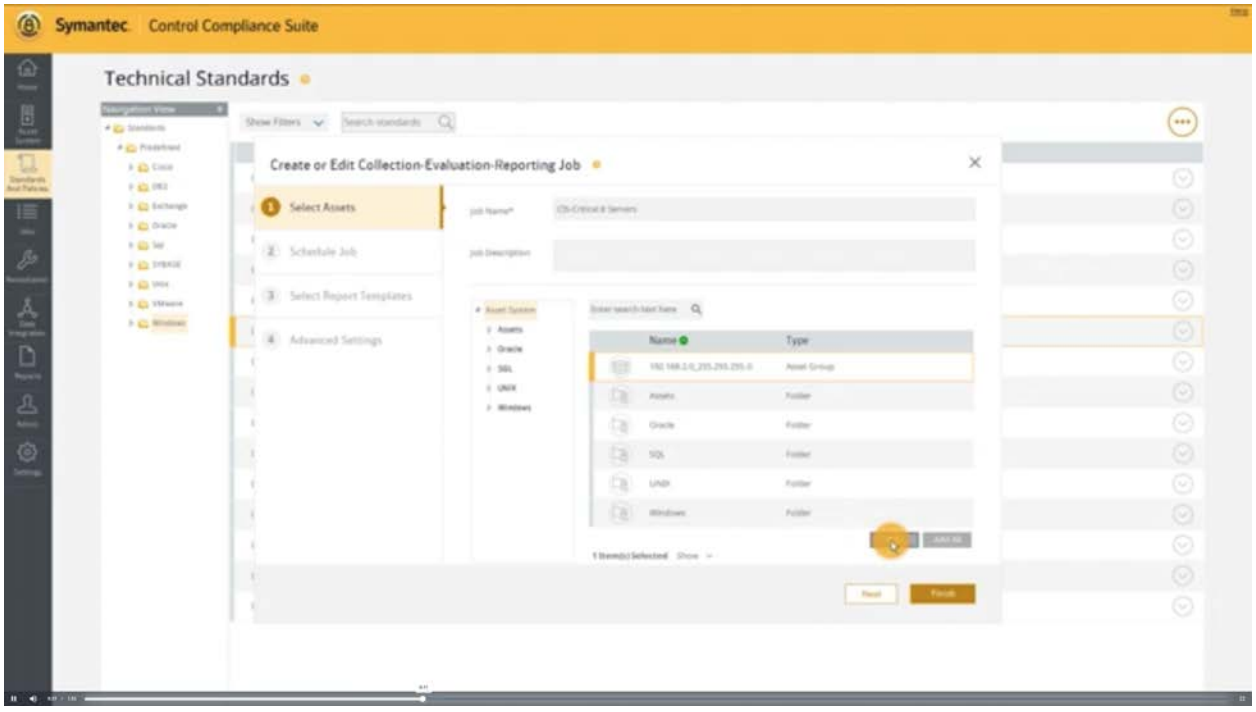

Prisma Cloud | SecOps
Prisma Cloud | Investigate
Prisma Cloud | Alerts Overview
app.prismacloud.io/alerts/overview#alert.status=open&timeType=to_now&timeUnit=epoch
CLOUD
Dashboard
Inventory
Investigate
Policies
Compliance
Alerts
Overview
Reports
Alert Rules
Notification Templates
Compute
Settings
Subscription
Clear All
Alerts Overview
(10,372 Alerts)
TIME RANGE
All Time
ALERT STATUS
Select All
Dismissed
Snoozed
Open
Resolved
POLICY SEVERITY
Select All
High
Medium
Low
STANDARD
Search for Standard
Select All
POLICY NAME
POLICY TYPE
STANDARDS
OPTIONS
Sensitive network configuration updates in AWS
Audit Event
HIPAA, ISM - IRAP - Pr
Sensitive configuration updates
Audit Event
HIPAA, ISM - IRAP - Pr
Sensitive Network configuration updates in GCP
Audit Event
CSA CCM v3.0.1, GDP
Sensitive Storage configuration updates
Audit Event
CSA CCM v3.0.1, GDP
AWS Security groups allow internet traffic
Config
CCPA 2018, CSA CCM
DeleteUser check
Audit Event
Custom Compliance St
AWS IAM sensitive activities by User
Audit Event
HIPAA, ISM - IRAP - Pr
AWS VPC subnets should not allow automatic public IP assignment
Config
CCPA 2018, CSA CCM
AWS Security Groups allow internet traffic to SSH port (22)
Config
CCPA 2018, CIS v1.2.0
Root user activities
Audit Event
CCPA 2018, CIS v1.2.0
AWS Security Groups allow internet traffic to ports which are not commonly used
Config
CCPA 2018, MITRE AT
AWS Lambda functions with tracing not enabled
Config
HITRUST CSF v9.3, NI

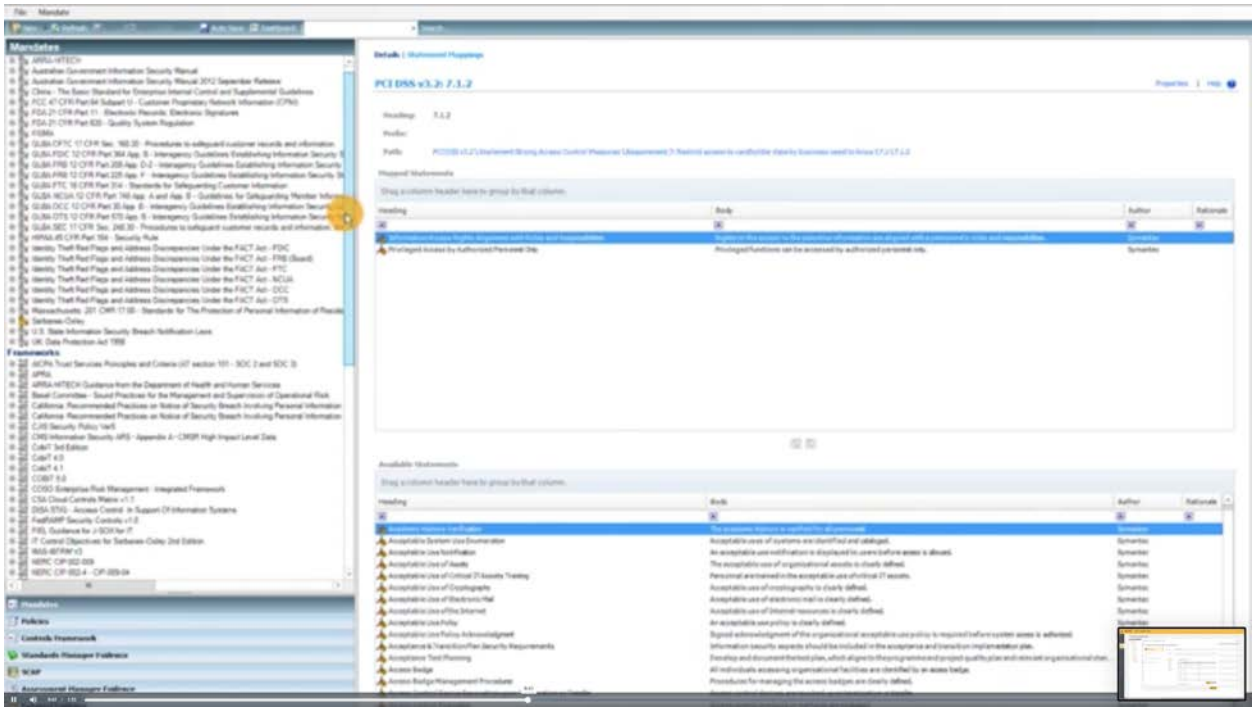
Symantec

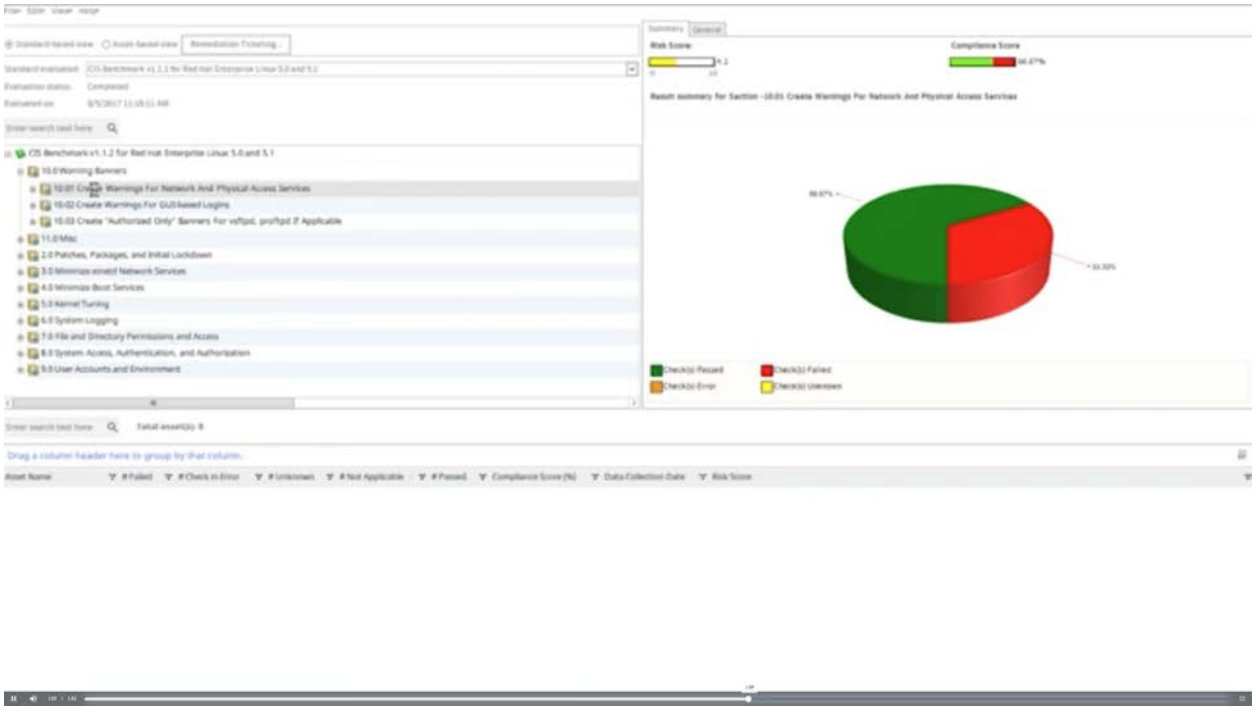
Symantec has multiple cloud security functions within its portfolio, including workload protection and CASB. There are a few different products that make up their Security product. UI seems less than impressive, not modern.

- **Key Values and Differentiators**:
    - The Cloud Workload Protection suite is able to identify and evaluate security risks for workloads running in the public cloud
    - Cloud Workload Assurance; automatic compliance reporting and remediation including the ability to benchmark security posture for a given configuration
- **Features include:**
    - Monitor, log, analyze user and admin activity
    - Enforce access controls
    - Detect and remediate risky exposures
    - Detect compromised accounts with User Behavior Analytics
    - Detect and restrict misuse and “Shadow” AWS instances

Screenshots of UI:




Mandates
PCI DSS v3.2: 7.1.2
Frameworks
Policies
Controls Framework
Standards Manager Fedlexic
SCAP
Assessment Manager Fedlexic


CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 5.0 and 5.1
Risk Score
Compliance Score
Result summary for Section -10.01 Create Warnings For Network And Physical Access Services
Check(s) Passed
Check(s) Failed
Check(s) Error
Check(s) Unknown

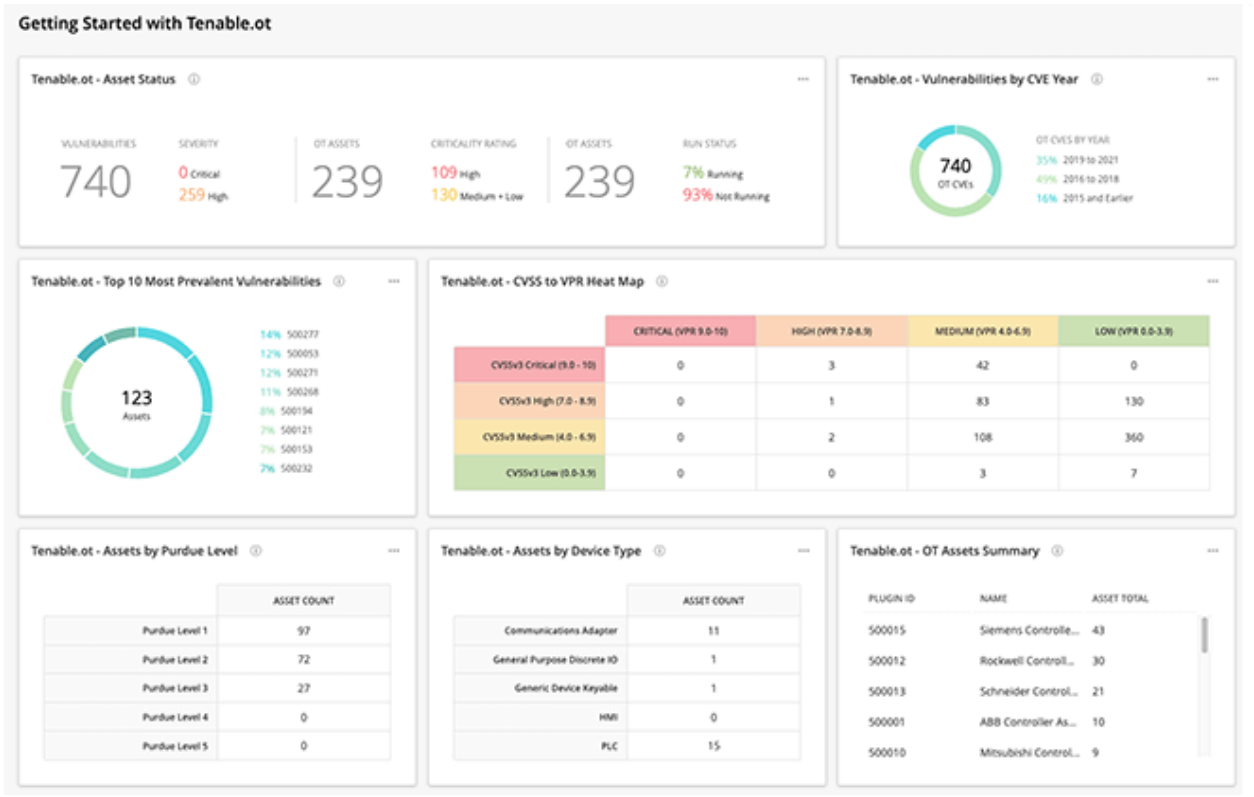
Tenable

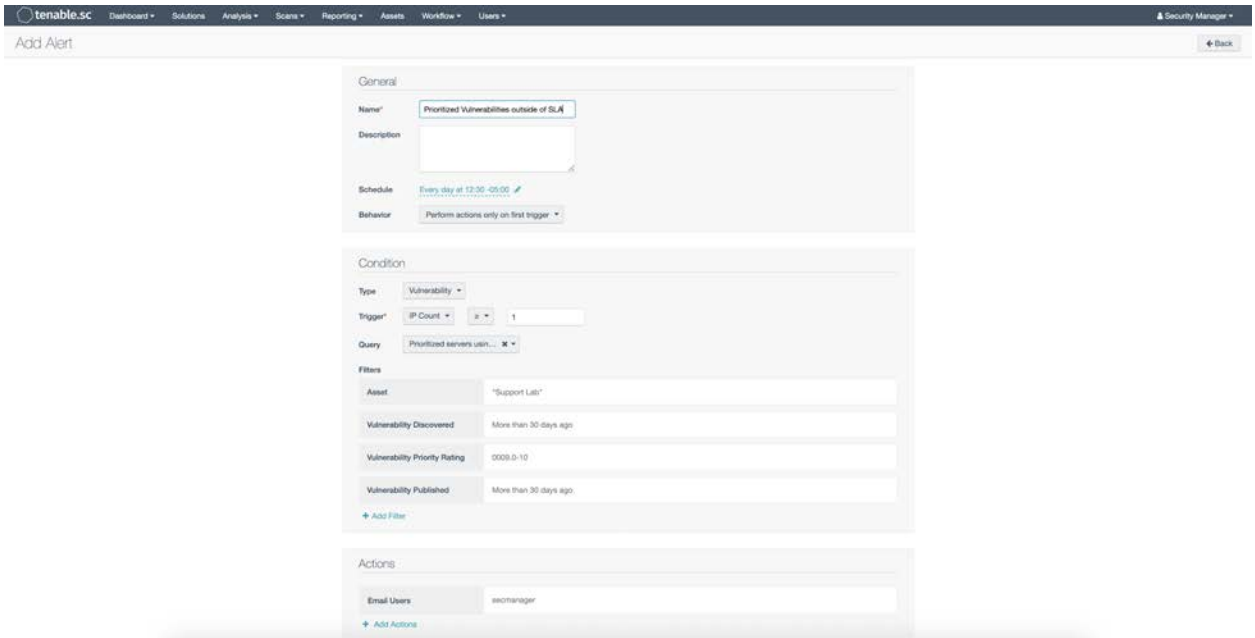
Tenable has a long history in the vulnerability management space, which now extends into the cloud to help organizations of all sizes protect their workloads. Tenable delivers coverage and comprehensive insight to enable you to detect vulnerabilities, assess risk, and prioritize remediation for every asset, in every environment.

Product Demo - Just for the Container Security product

- **Key Values and Differentiators**:
    - Multiple services on its cloud-based tenable.io platform, including web application scanning, container security, and asset management
    - Ability to identify assets and their vulnerabilities
    - Ability to identify potential misconfigurations
- **Features include:**
    - Discover, Assess, Prioritize
    - Risk-based view of entire attack surface on main dashboard (critical vulnerabilities that should be investigated immediately and high risk vulnerabilities to address next)

Screenshots of UI:

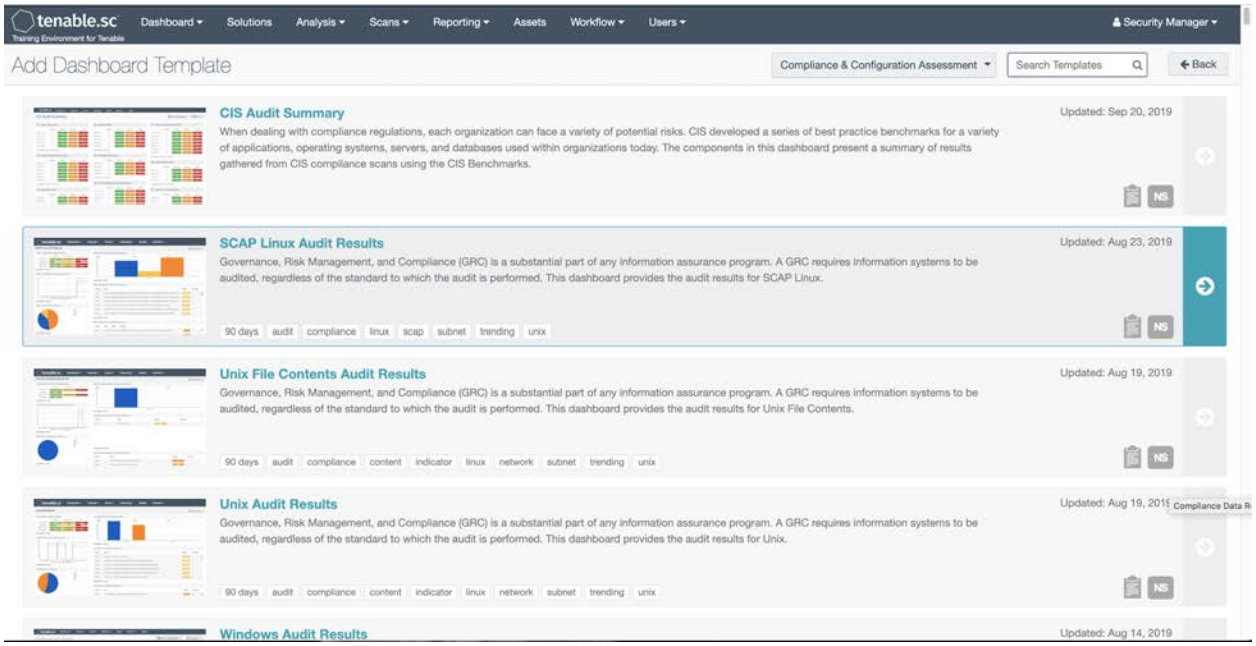

Getting Started with Tenable.ot
Tenable.ot - Asset Status
VULNERABILITIES
740
SEVERITY
0 Critical
259 High
OT ASSETS
239
CRITICALITY RATING
109 High
130 Medium + Low
OT ASSETS
239
RUN STATUS
7% Running
93% Not Running
Tenable.ot - Vulnerabilities by CVE Year
740
OT CVEs
OT CVES BY YEAR
35% 2019 to 2021
49% 2016 to 2018
16% 2015 and Earlier
Tenable.ot - Top 10 Most Prevalent Vulnerabilities
123
Assets
14% 500277
12% 500053
12% 500271
11% 500268
8% 500194
7% 500121
7% 500153
7% 500232
Tenable.ot - CVSS to VPR Heat Map
CRITICAL (VPR 9.0-10)
HIGH (VPR 7.0-8.9)
MEDIUM (VPR 4.0-6.9)
LOW (VPR 0.0-3.9)
CVSSv3 Critical (9.0 - 10)
0
3
42
0
CVSSv3 High (7.0 - 8.9)
0
1
83
130
CVSSv3 Medium (4.0 - 6.9)
0
2
108
360
CVSSv3 Low (0.0-3.9)
0
0
3
7
Tenable.ot - Assets by Purdue Level
ASSET COUNT
Purdue Level 1
97
Purdue Level 2
72
Purdue Level 3
27
Purdue Level 4
0
Purdue Level 5
0
Tenable.ot - Assets by Device Type
ASSET COUNT
Communications Adapter
11
General Purpose Discrete IO
1
Generic Device Keyable
1
HMI
0
PLC
15
Tenable.ot - OT Assets Summary
PLUGIN ID
NAME
ASSET TOTAL
500015
Siemens Controlle...
43
500012
Rockwell Controll...
30
500013
Schneider Control...
21
500001
ABB Controller As...
10
500010
Mitsubishi Control...
9

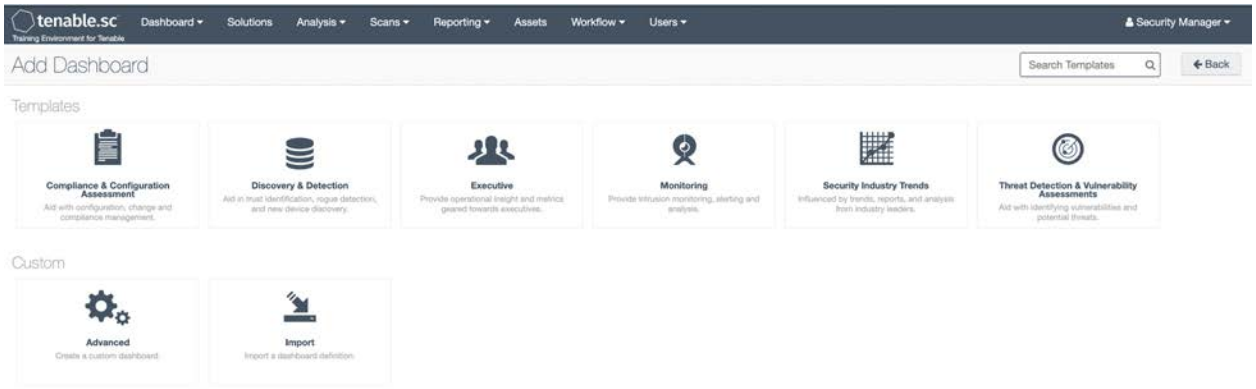

tenable.sc
Dashboard
Solutions
Analysis
Scans
Reporting
Assets
Workflow
Users
Security Manager
Add Alert
Back
General
Name*
Prioritized Vulnerabilities outside of SLA
Description
Schedule
Every day at 12:00 -05:00
Behavior
Perform actions only on first trigger
Condition
Type
Vulnerability
Trigger*
IP Count
≥
1
Query
Prioritized servers usin...
Filters
Asset
"Support Lab"
Vulnerability Discovered
More than 30 days ago
Vulnerability Priority Rating
0009.0-10
Vulnerability Published
More than 30 days ago
+ Add Filter
Actions
Email Users
secmanager
+ Add Actions

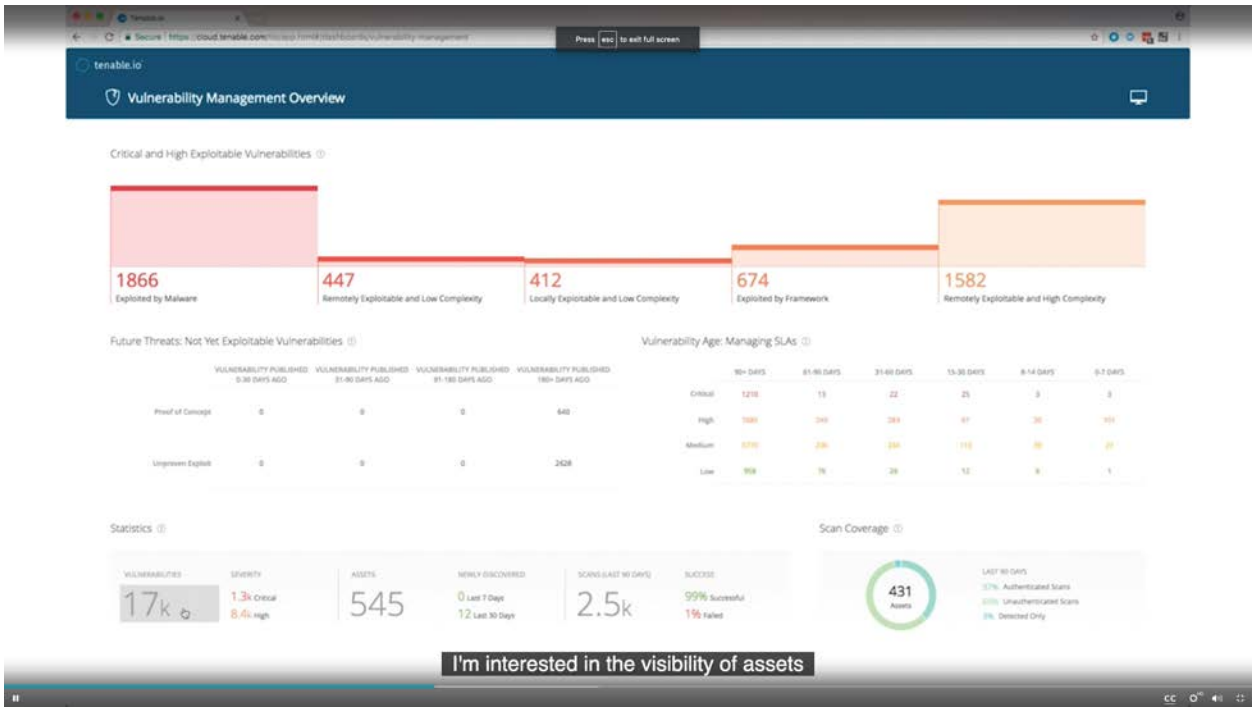
Compliance Summary - CIS, DOD, and NIST Bar Ratio

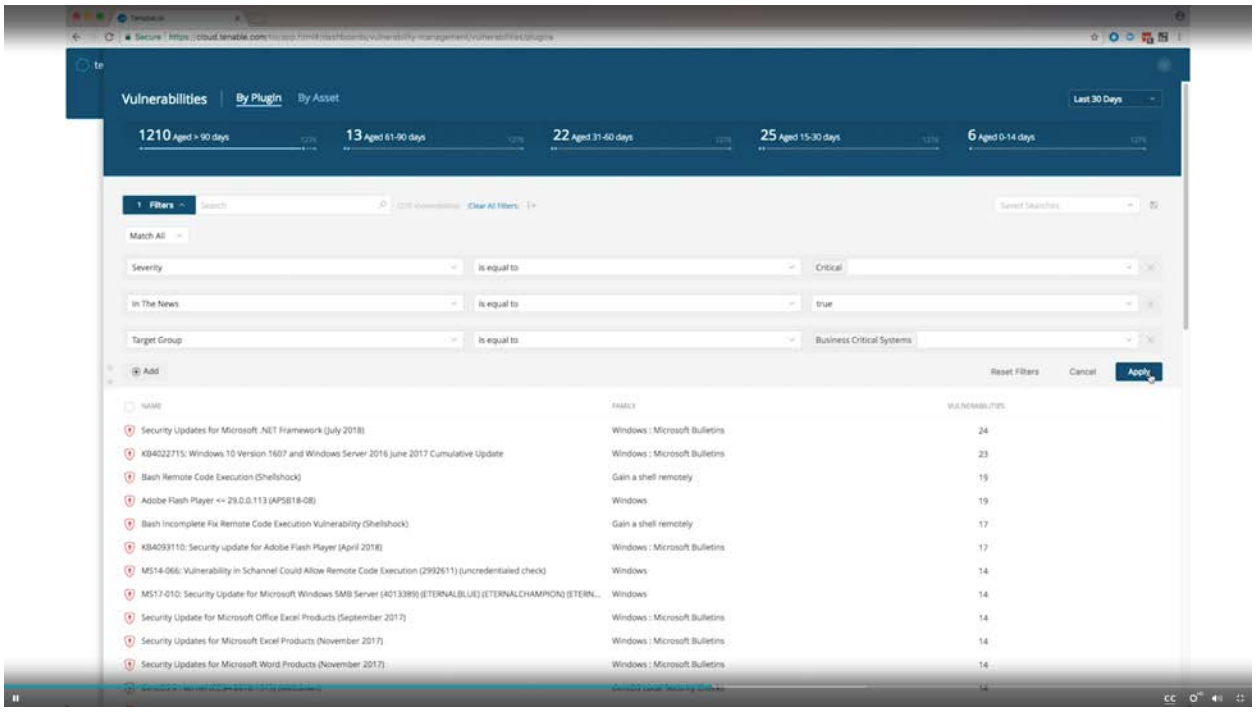
	Systems	Passed	Manual Check	Failed
800-53	3	33%	39%	28%
8500.2	0	0	0	0
CAT	0	0	0	0
CCE	0	0	0	0
CCI	0	0	0	0
CSF	3	32%	40%	28%
ITSG-33	3	28%	39%	32%
Level	3	33%	39%	28%
NIST_800-125a	0	0	0	0
CIS CSC	3	36%	43%	21%

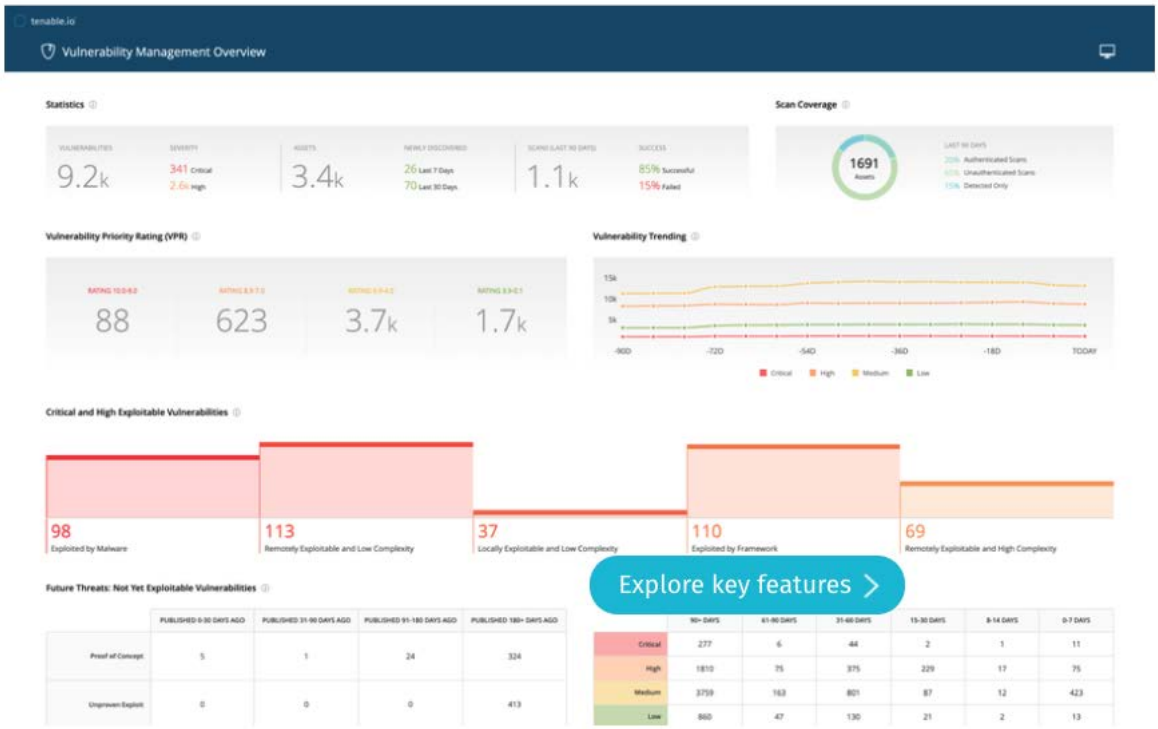
Last Updated: Feb 24, 2020 09:47

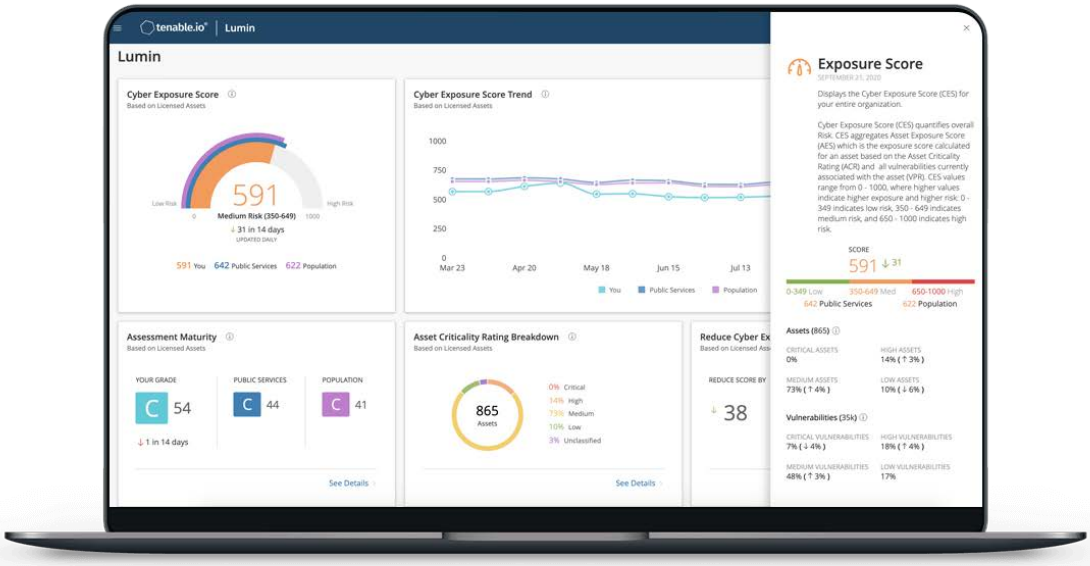


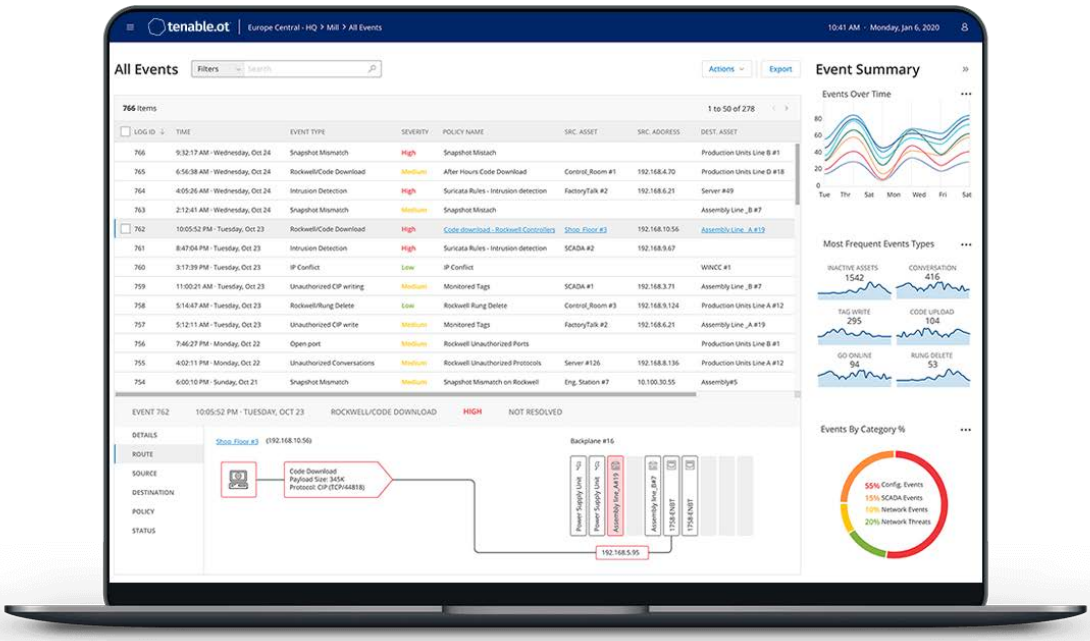


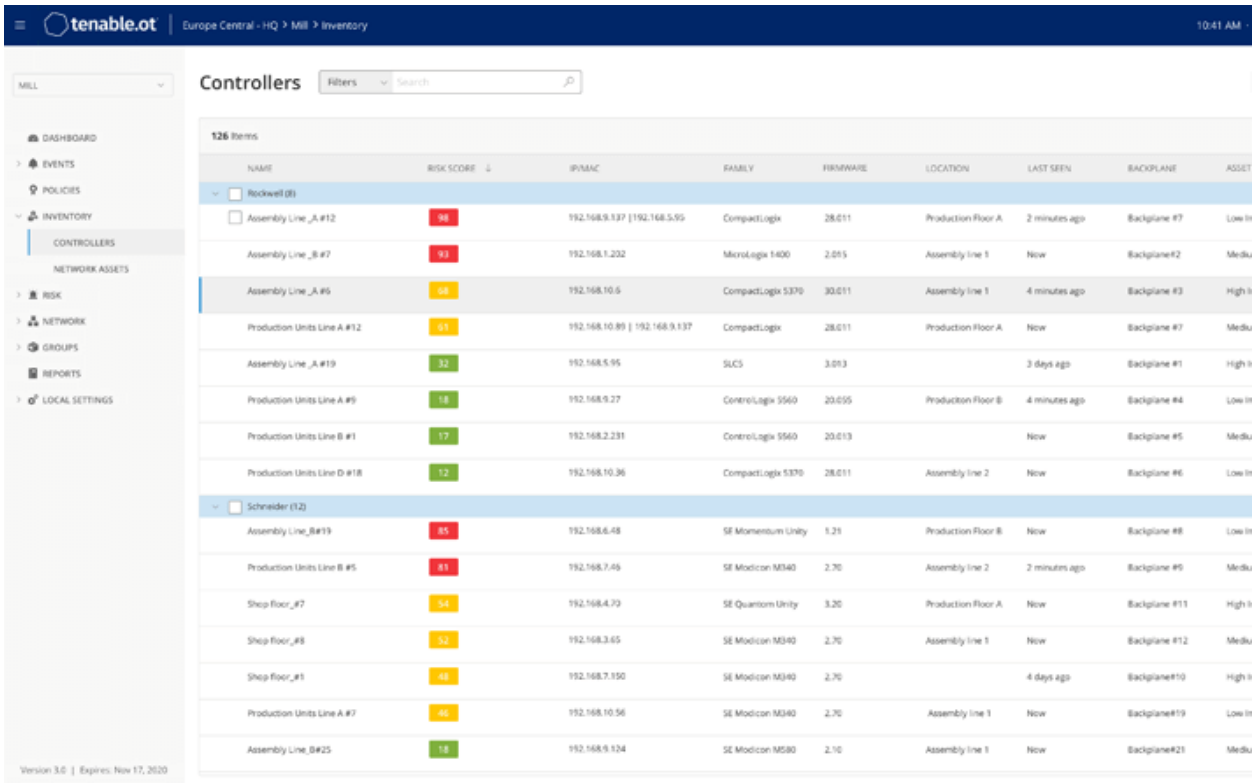

Press esc to exit full screen
tenable.io
Vulnerability Management Overview
Critical and High Exploitable Vulnerabilities
1866
Exploited by Malware
447
Remotely Exploitable and Low Complexity
412
Locally Exploitable and Low Complexity
674
Exploited by Framework
1582
Remotely Exploitable and High Complexity
Future Threats: Not Yet Exploitable Vulnerabilities
Vulnerability Age: Managing SLAs
Statistics
17k
1.3k Critical
8.4k High
545
0 Last 7 Days
12 Last 30 Days
2.5k
99% Successful
1% Failed
Scan Coverage
431
Assets
I'm interested in the visibility of assets

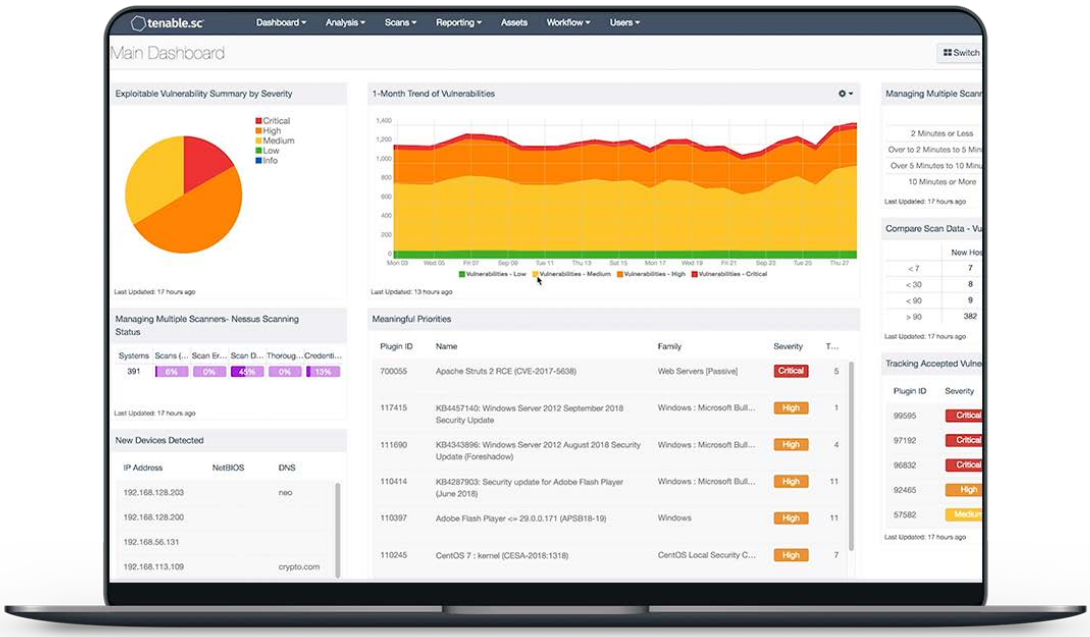

Vulnerabilities
By Plugin
By Asset
Last 30 Days
1210 Aged > 90 days
13 Aged 61-90 days
22 Aged 31-60 days
25 Aged 15-30 days
6 Aged 0-14 days
Filters
Match All
Severity
is equal to
Critical
In The News
is equal to
true
Target Group
is equal to
Business Critical Systems
Add
Reset Filters
Cancel
Apply
NAME
FAMILY
VULNERABILITIES
Security Updates for Microsoft .NET Framework (July 2018)
Windows : Microsoft Bulletins
24
KB4022715: Windows 10 Version 1607 and Windows Server 2016 June 2017 Cumulative Update
Windows : Microsoft Bulletins
23
Bash Remote Code Execution (Shellshock)
Gain a shell remotely
19
Adobe Flash Player <= 29.0.0.113 (APSB18-08)
Windows
19
Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)
Gain a shell remotely
17
KB4093110: Security update for Adobe Flash Player (April 2018)
Windows : Microsoft Bulletins
17
MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
Windows
14
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERN...
Windows
14
Security Update for Microsoft Office Excel Products (September 2017)
Windows : Microsoft Bulletins
14
Security Updates for Microsoft Excel Products (November 2017)
Windows : Microsoft Bulletins
14
Security Updates for Microsoft Word Products (November 2017)
Windows : Microsoft Bulletins
14

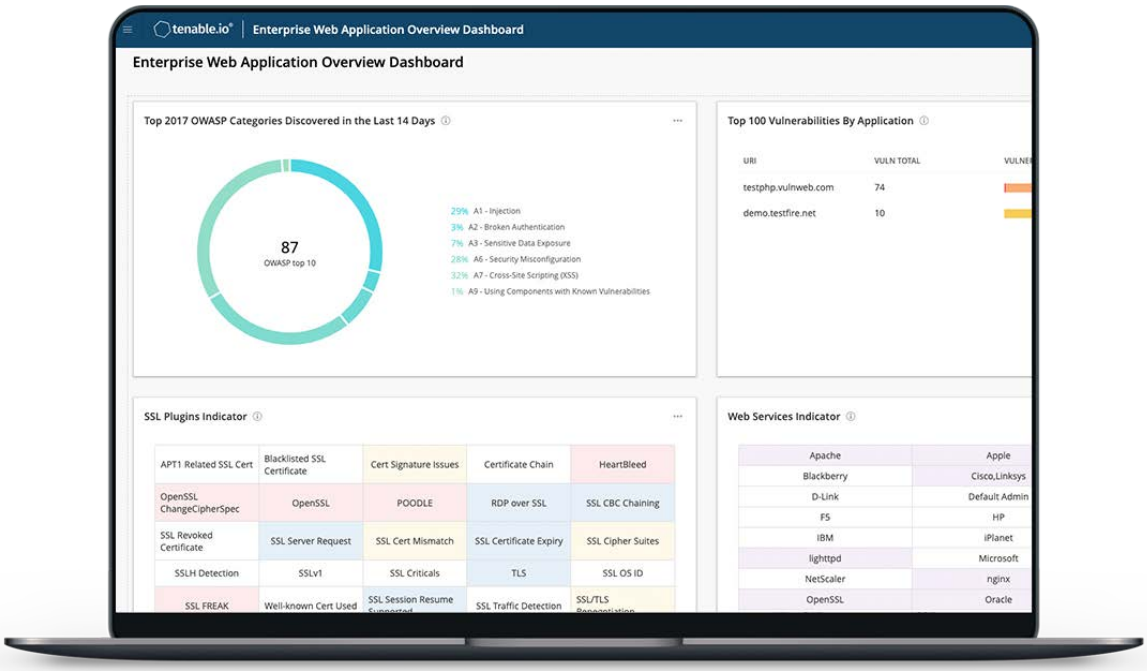

tenable.io
Vulnerability Management Overview
Statistics
9.2k
341 Critical
2.6k High
3.4k
26 Last 7 Days
70 Last 30 Days
1.1k
85% Successful
15% Failed
Scan Coverage
1691
Assets
Vulnerability Priority Rating (VPR)
88
623
3.7k
1.7k
Vulnerability Trending
15k
10k
5k
-90D
-72D
-54D
-36D
-18D
TODAY
Critical
High
Medium
Low
Critical and High Exploitable Vulnerabilities
98
Exploited by Malware
113
Remotely Exploitable and Low Complexity
37
Locally Exploitable and Low Complexity
110
Exploited by Framework
69
Remotely Exploitable and High Complexity
Future Threats: Not Yet Exploitable Vulnerabilities
PUBLISHED 0-30 DAYS AGO
PUBLISHED 31-90 DAYS AGO
PUBLISHED 91-180 DAYS AGO
PUBLISHED 180+ DAYS AGO
Proof of Concept
5
1
24
324
Unproven Exploit
0
0
0
413
Explore key features
90+ DAYS
61-90 DAYS
31-60 DAYS
15-30 DAYS
8-14 DAYS
0-7 DAYS
Critical
277
6
44
2
1
11
High
1810
75
375
229
17
75
Medium
3759
163
801
87
12
423
Low
860
47
130
21
2
13


tenable.io | Lumin
Lumin
Cyber Exposure Score
Based on Licensed Assets
591
Medium Risk (350-649)
↓ 31 in 14 days
UPDATED DAILY
591 You
642 Public Services
622 Population
Cyber Exposure Score Trend
Based on Licensed Assets
1000
750
500
250
0
Mar 23
Apr 20
May 18
Jun 15
Jul 13
You
Public Services
Population
Assessment Maturity
Based on Licensed Assets
YOUR GRADE
C 54
↓ 1 in 14 days
PUBLIC SERVICES
C 44
POPULATION
C 41
See Details
Asset Criticality Rating Breakdown
Based on Licensed Assets
865
Assets
0% Critical
14% High
73% Medium
10% Low
3% Unclassified
See Details
Reduce Cyber Ex
Based on Licensed Ass
REDUCE SCORE BY
↓ 38
Exposure Score
SEPTEMBER 21, 2020
Displays the Cyber Exposure Score (CES) for your entire organization.
Cyber Exposure Score (CES) quantifies overall Risk. CES aggregates Asset Exposure Score (AES) which is the exposure score calculated for an asset based on the Asset Criticality Rating (ACR) and all vulnerabilities currently associated with the asset (VPR). CES values range from 0 - 1000, where higher values indicate higher exposure and higher risk: 0 - 349 indicates low risk, 350 - 649 indicates medium risk, and 650 - 1000 indicates high risk.
SCORE
591 ↓ 31
0-349 Low
350-649 Med
650-1000 High
642 Public Services
622 Population
Assets (865)
CRITICAL ASSETS
0%
HIGH ASSETS
14% (↑ 3%)
MEDIUM ASSETS
73% (↑ 4%)
LOW ASSETS
10% (↓ 6%)
Vulnerabilities (35k)
CRITICAL VULNERABILITIES
7% (↓ 4%)
HIGH VULNERABILITIES
18% (↑ 4%)
MEDIUM VULNERABILITIES
48% (↑ 3%)
LOW VULNERABILITIES
17%


tenable.ot
Europe Central - HQ > Mill > All Events
10:41 AM · Monday, Jan 6, 2020
All Events
Filters
Search
Actions
Export
766 Items
1 to 50 of 278
LOG ID
TIME
EVENT TYPE
SEVERITY
POLICY NAME
SRC. ASSET
SRC. ADDRESS
DEST. ASSET
766 9:32:17 AM - Wednesday, Oct 24 Snapshot Mismatch High Snapshot Mistach Production Units Line B #1
765 6:56:38 AM - Wednesday, Oct 24 Rockwell/Code Download Medium After Hours Code Download Control_Room #1 192.168.4.70 Production Units Line D #18
764 4:05:26 AM - Wednesday, Oct 24 Intrusion Detection High Suricata Rules - Intrusion detection FactoryTalk #2 192.168.6.21 Server #49
763 2:12:41 AM - Wednesday, Oct 24 Snapshot Mismatch Medium Snapshot Mistach Assembly Line _B #7
762 10:05:52 PM - Tuesday, Oct 23 Rockwell/Code Download High Code download - Rockwell Controllers Shop_Floor #3 192.168.10.56 Assembly Line _A #19
761 8:47:04 PM - Tuesday, Oct 23 Intrusion Detection High Suricata Rules - Intrusion detection SCADA #2 192.168.9.67
760 3:17:39 PM - Tuesday, Oct 23 IP Conflict Low IP Conflict WINCC #1
759 11:00:21 AM - Tuesday, Oct 23 Unauthorized CIP writing Medium Monitored Tags SCADA #1 192.168.3.71 Assembly Line _B #7
758 5:14:47 AM - Tuesday, Oct 23 Rockwell/Rung Delete Low Rockwell Rung Delete Control_Room #3 192.168.9.124 Production Units Line A #12
757 5:12:11 AM - Tuesday, Oct 23 Unauthorized CIP write Medium Monitored Tags FactoryTalk #2 192.168.6.21 Assembly Line _A #19
756 7:46:27 PM - Monday, Oct 22 Open port Medium Rockwell Unauthorized Ports Production Units Line B #1
755 4:02:11 PM - Monday, Oct 22 Unauthorized Conversations Medium Rockwell Unauthorized Protocols Server #126 192.168.8.136 Production Units Line A #12
754 6:00:10 PM - Sunday, Oct 21 Snapshot Mismatch Medium Snapshot Mismatch on Rockwell Eng. Station #7 10.100.30.55 Assembly#5
EVENT 762
10:05:52 PM - TUESDAY, OCT 23
ROCKWELL/CODE DOWNLOAD
HIGH
NOT RESOLVED
DETAILS
ROUTE
SOURCE
DESTINATION
POLICY
STATUS
Shop_Floor #3 (192.168.10.56)
Code Download
Payload Size: 345K
Protocol: CIP (TCP/44818)
Backplane #16
Power Supply Unit
Power Supply Unit
Assembly Line_A#19
Assembly line_B#7
1756-ENBT
1756-ENBT
192.168.5.95
Event Summary
Events Over Time
80
60
40
20
0
Tue
Thr
Sat
Mon
Wed
Fri
Sat
Most Frequent Events Types
INACTIVE ASSETS
1542
CONVERSATION
416
TAG WRITE
295
CODE UPLOAD
104
GO ONLINE
94
RUNG DELETE
53
Events By Category %
55% Config. Events
15% SCADA Events
10% Network Events
20% Network Threats


tenable.ot
Europe Central - HQ > Mill > Inventory
10:41 AM
MILL
DASHBOARD
EVENTS
POLICIES
INVENTORY
CONTROLLERS
NETWORK ASSETS
RISK
NETWORK
GROUPS
REPORTS
LOCAL SETTINGS
Version 3.0 | Expires: Nov 17, 2020
Controllers
Filters
Search
126 Items
NAME
RISK SCORE
IP/MAC
FAMILY
FIRMWARE
LOCATION
LAST SEEN
BACKPLANE
ASSET
Rockwell (8)
Assembly Line _A #12 98 192.168.9.137 | 192.168.5.95 CompactLogix 28.011 Production Floor A 2 minutes ago Backplane #7
Assembly Line _B #7 93 192.168.1.202 MicroLogix 1400 2.015 Assembly line 1 Now Backplane#2
Assembly Line _A #6 68 192.168.10.6 CompactLogix 5370 30.011 Assembly line 1 4 minutes ago Backplane #3
Production Units Line A #12 61 192.168.10.89 | 192.168.9.137 CompactLogix 28.011 Production Floor A Now Backplane #7
Assembly Line _A #19 32 192.168.5.95 SLC5 3.013 3 days ago Backplane #1
Production Units Line A #9 18 192.168.9.27 ControlLogix 5560 20.055 Produciton Floor B 4 minutes ago Backplane #4
Production Units Line B #1 17 192.168.2.231 ControlLogix 5560 20.013 Now Backplane #5
Production Units Line D #18 12 192.168.10.36 CompactLogix 5370 28.011 Assembly line 2 Now Backplane #6
Schneider (12)
Assembly Line_B#19 85 192.168.6.48 SE Momentum Unity 1.21 Production Floor B Now Backplane #8
Production Units Line B #5 81 192.168.7.46 SE Modicon M340 2.70 Assembly line 2 2 minutes ago Backplane #9
Shop floor_#7 54 192.168.4.70 SE Quantorm Unity 3.20 Production Floor A Now Backplane #11
Shop floor_#8 52 192.168.3.65 SE Modicon M340 2.70 Assembly line 1 Now Backplane #12
Shop floor_#1 48 192.168.7.150 SE Modicon M340 2.70 4 days ago Backplane#10
Production Units Line A #7 46 192.168.10.56 SE Modicon M340 2.70 Assembly line 1 Now Backplane#19
Assembly Line_B#25 18 192.168.9.124 SE Modicon M580 2.10 Assembly line 1 Now Backplane#21


tenable.sc
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Users
Main Dashboard
Switch
Exploitable Vulnerability Summary by Severity
Critical
High
Medium
Low
Info
Last Updated: 17 hours ago
1-Month Trend of Vulnerabilities
Vulnerabilities - Low
Vulnerabilities - Medium
Vulnerabilities - High
Vulnerabilities - Critical
Last Updated: 13 hours ago
Managing Multiple Scanners
2 Minutes or Less
Last Updated: 17 hours ago
Compare Scan Data
Last Updated: 17 hours ago
Managing Multiple Scanners- Nessus Scanning Status
Systems
391
Last Updated: 17 hours ago
Meaningful Priorities
Plugin ID
Name
Family
Severity
700055
Apache Struts 2 RCE (CVE-2017-5638)
Web Servers [Passive]
Critical
117415
KB4457140: Windows Server 2012 September 2018 Security Update
Windows : Microsoft Bull...
High
111690
KB4343896: Windows Server 2012 August 2018 Security Update (Foreshadow)
Windows : Microsoft Bull...
High
110414
KB4287903: Security update for Adobe Flash Player (June 2018)
Windows : Microsoft Bull...
High
110397
Adobe Flash Player <= 29.0.0.171 (APSB18-19)
Windows
High
110245
CentOS 7 : kernel (CESA-2018:1318)
CentOS Local Security C...
High
New Devices Detected
IP Address
NetBIOS
DNS
192.168.128.203
neo
192.168.128.200
192.168.56.131
192.168.113.109
crypto.com
Tracking Accepted Vulne
Plugin ID
Severity
99595
97192
96832
92465
57582


tenable.io
Enterprise Web Application Overview Dashboard
Enterprise Web Application Overview Dashboard
Top 2017 OWASP Categories Discovered in the Last 14 Days
87
OWASP top 10
29% A1 - Injection
3% A2 - Broken Authentication
7% A3 - Sensitive Data Exposure
28% A6 - Security Misconfiguration
32% A7 - Cross-Site Scripting (XSS)
1% A9 - Using Components with Known Vulnerabilities
Top 100 Vulnerabilities By Application
URI
VULN TOTAL
testphp.vulnweb.com
74
demo.testfire.net
10
SSL Plugins Indicator
APT1 Related SSL Cert
Blacklisted SSL Certificate
Cert Signature Issues
Certificate Chain
HeartBleed
OpenSSL ChangeCipherSpec
OpenSSL
POODLE
RDP over SSL
SSL CBC Chaining
SSL Revoked Certificate
SSL Server Request
SSL Cert Mismatch
SSL Certificate Expiry
SSL Cipher Suites
SSLH Detection
SSLv1
SSL Criticals
TLS
SSL OS ID
SSL FREAK
Well-known Cert Used
SSL Session Resume Supported
SSL Traffic Detection
SSL/TLS Renegotiation
Web Services Indicator
Apache
Apple
Blackberry
Cisco,Linksys
D-Link
Default Admin
F5
HP
IBM
iPlanet
lighttpd
Microsoft
NetScaler
nginx
OpenSSL
Oracle

Trend Micro Cloud One

Trend Micro is a well positioned leader in the hybrid cloud security, helping organizations unify policies across both on-prem and public cloud deployments.

- **Key Values and Differentiators**:
    - Robust offering that integrates workload, storage, and network security as well as compliance capabilities
    - Workload security feature; extends the same policy and protection to multiple deployment modalities, including on-prem, private, and public cloud workloads
    - Provides virtual patching for vulnerabilities to help limit risks as rapidly as possible
    - Security can be codified, with templates that align with leading security standards and can be deployed with simple AWS CloudFormation templates
- **Features include:**
    -

Screenshots of UI:

VMware Cloud

VMware has multiple capabilities for cloud security, includings its secure state and Cloudhealth products.

- **Key Values and Differentiators**:
    - CloudHealth provides deeper integration with VMware workloads, alongside public cloud
    - Provides cloud governance features to help organizations align security and regulatory compliance
    - Delivers multi-cloud security posture management that focuses on configuration security
    - Secure State is particularly good at providing insights into security risks due to connections between cloud objects and services
- **Features include:**
    -

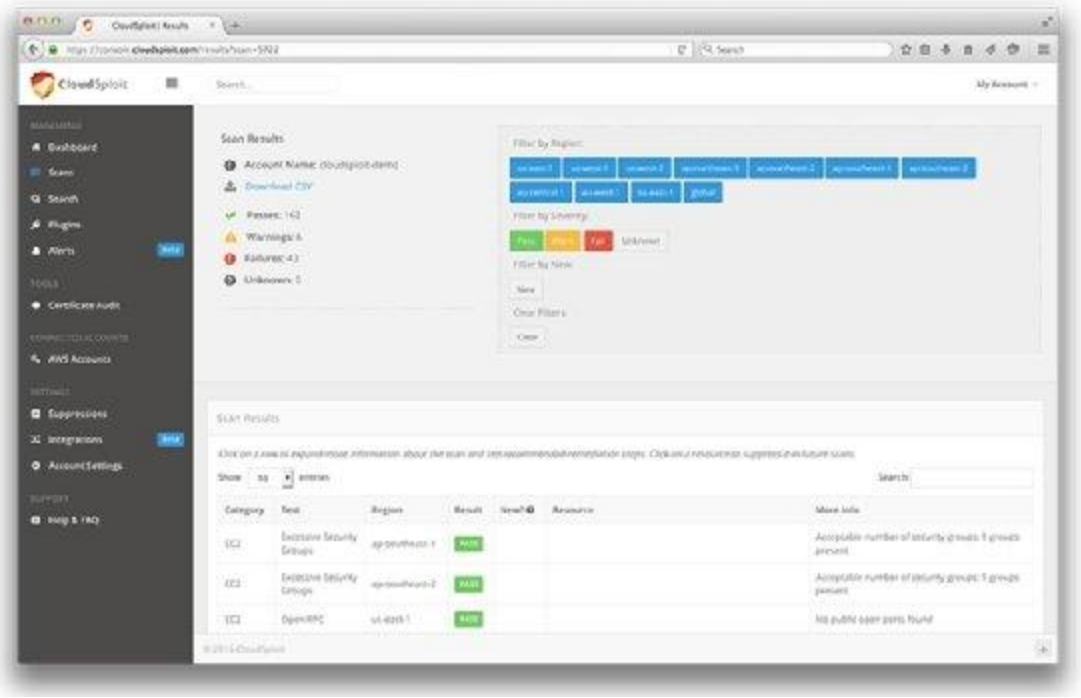
Screenshots of UI:

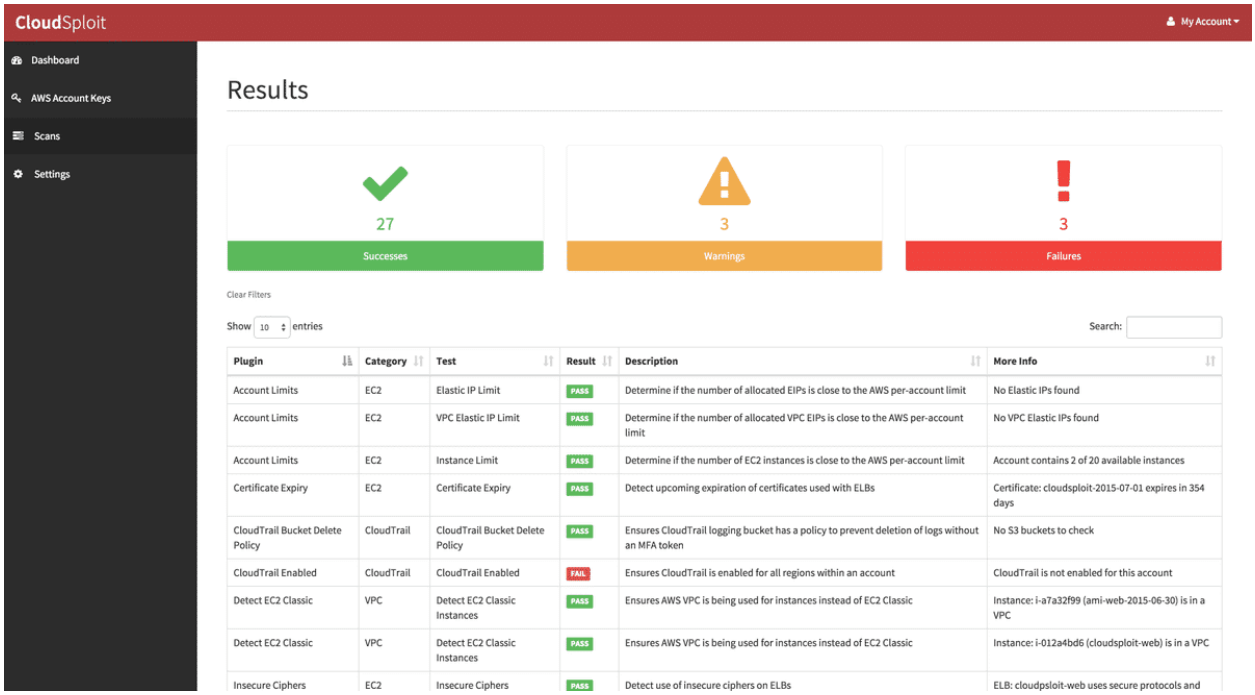
CloudSploit

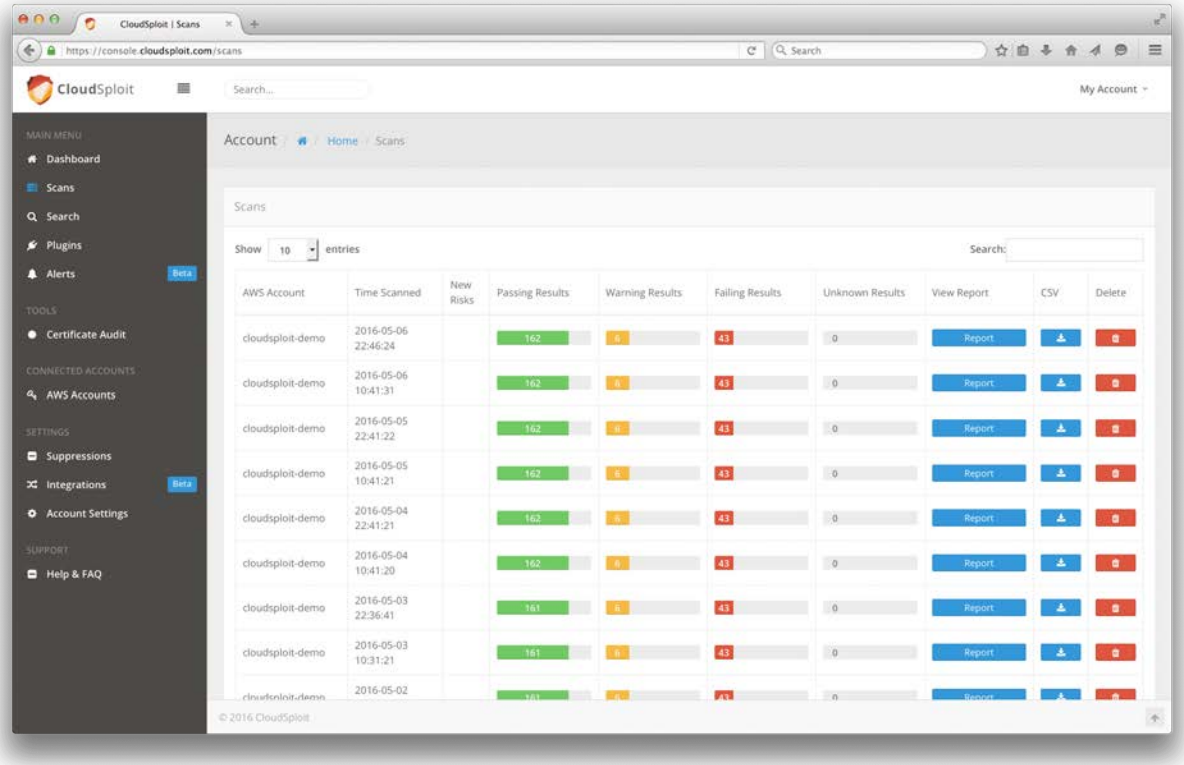
CloudSploit is a security and configuration scanner that can detect thousands of threats in your cloud accounts.

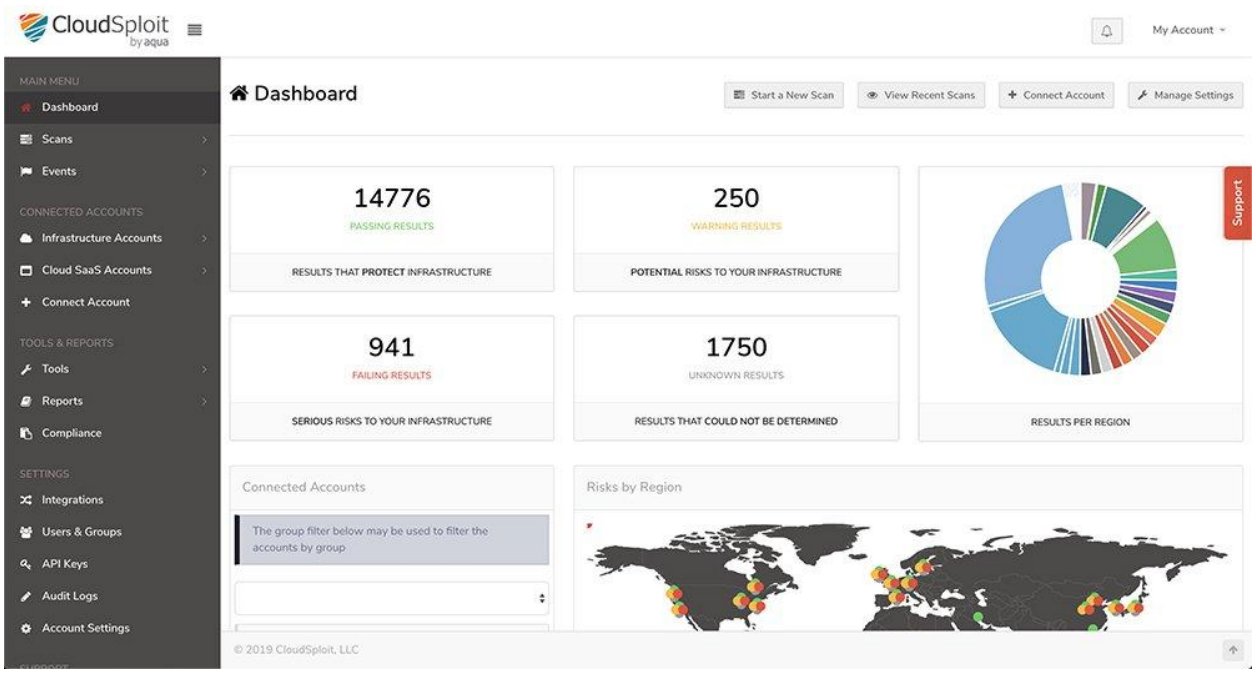
4. **Key Values and Differentiators**:
    - Automates the detection of risks on a continuous basis
    - Scan reports can be used to quickly assess risk, plan for remediation, and audit changes over time
    - Reports include in-depth remediation steps
    - Detects misconfigurations before they are exploited and ensures environments stay secure
5. **Features include:**
    - Fully-Managed
    - Simple, 2-Minute setup
    - Multi cloud and region
    - Users and groups
    - Downloadable reports
    - API driven
    - Archived results
    - Alerts and integrations

Screenshots of UI:




CloudSploit
My Account
Dashboard
AWS Account Keys
Scans
Settings
Results
27
Successes
3
Warnings
3
Failures
Clear Filters
Show 10 entries
Search:
Plugin
Category
Test
Result
Description
More Info
Account Limits
EC2
Elastic IP Limit
PASS
Determine if the number of allocated EIPs is close to the AWS per-account limit
No Elastic IPs found
Account Limits
EC2
VPC Elastic IP Limit
PASS
Determine if the number of allocated VPC EIPs is close to the AWS per-account limit
No VPC Elastic IPs found
Account Limits
EC2
Instance Limit
PASS
Determine if the number of EC2 instances is close to the AWS per-account limit
Account contains 2 of 20 available instances
Certificate Expiry
EC2
Certificate Expiry
PASS
Detect upcoming expiration of certificates used with ELBs
Certificate: cloudsploit-2015-07-01 expires in 354 days
CloudTrail Bucket Delete Policy
CloudTrail
CloudTrail Bucket Delete Policy
PASS
Ensures CloudTrail logging bucket has a policy to prevent deletion of logs without an MFA token
No S3 buckets to check
CloudTrail Enabled
CloudTrail
CloudTrail Enabled
FAIL
Ensures CloudTrail is enabled for all regions within an account
CloudTrail is not enabled for this account
Detect EC2 Classic
VPC
Detect EC2 Classic Instances
PASS
Ensures AWS VPC is being used for instances instead of EC2 Classic
Instance: i-a7a32f99 (ami-web-2015-06-30) is in a VPC
Detect EC2 Classic
VPC
Detect EC2 Classic Instances
PASS
Ensures AWS VPC is being used for instances instead of EC2 Classic
Instance: i-012a4bd6 (cloudsploit-web) is in a VPC
Insecure Ciphers
EC2
Insecure Ciphers
PASS
Detect use of insecure ciphers on ELBs
ELB: cloudpsloit-web uses secure protocols and


CloudSploit | Scans
https://console.cloudsploit.com/scans
CloudSploit
Search...
My Account
MAIN MENU
Dashboard
Scans
Search
Plugins
Alerts
Beta
TOOLS
Certificate Audit
CONNECTED ACCOUNTS
AWS Accounts
SETTINGS
Suppressions
Integrations
Beta
Account Settings
SUPPORT
Help & FAQ
Account
Home
Scans
Scans
Show 10 entries
Search:
AWS Account
Time Scanned
New Risks
Passing Results
Warning Results
Failing Results
Unknown Results
View Report
CSV
Delete
cloudsploit-demo
2016-05-06 22:46:24
162
6
43
0
Report
cloudsploit-demo
2016-05-06 10:41:31
162
6
43
0
Report
cloudsploit-demo
2016-05-05 22:41:22
162
6
43
0
Report
cloudsploit-demo
2016-05-05 10:41:21
162
6
43
0
Report
cloudsploit-demo
2016-05-04 22:41:21
162
6
43
0
Report
cloudsploit-demo
2016-05-04 10:41:20
162
6
43
0
Report
cloudsploit-demo
2016-05-03 22:36:41
161
6
43
0
Report
cloudsploit-demo
2016-05-03 10:31:21
161
6
43
0
Report
© 2016 CloudSploit



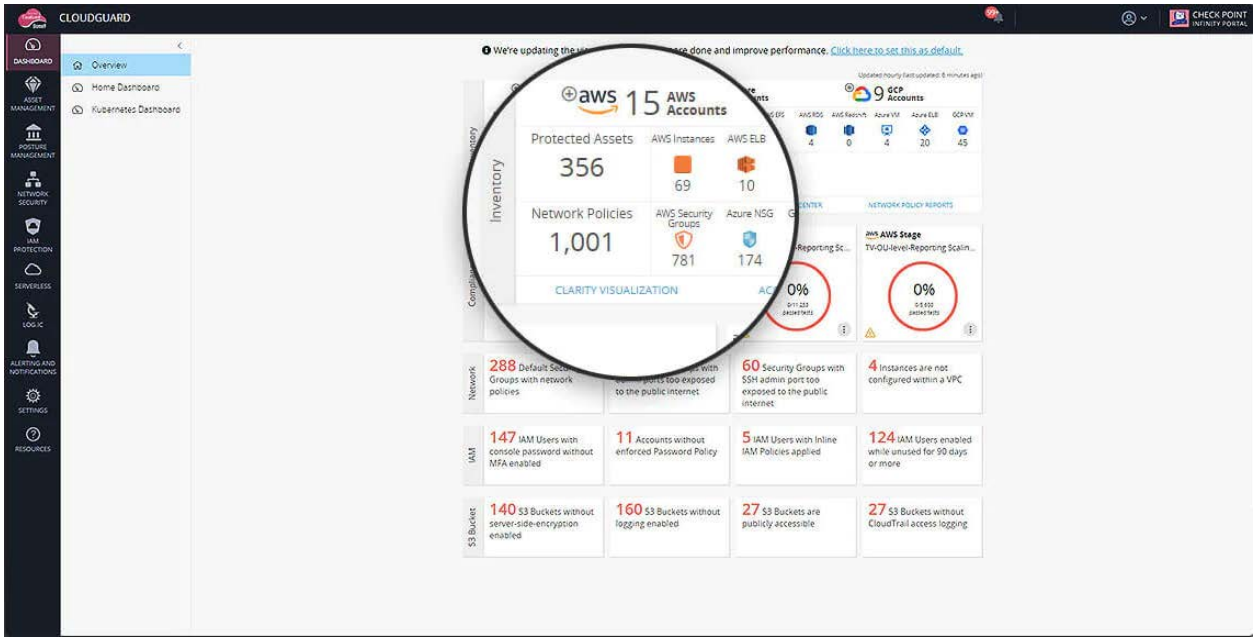
CheckPoint CloudGuard

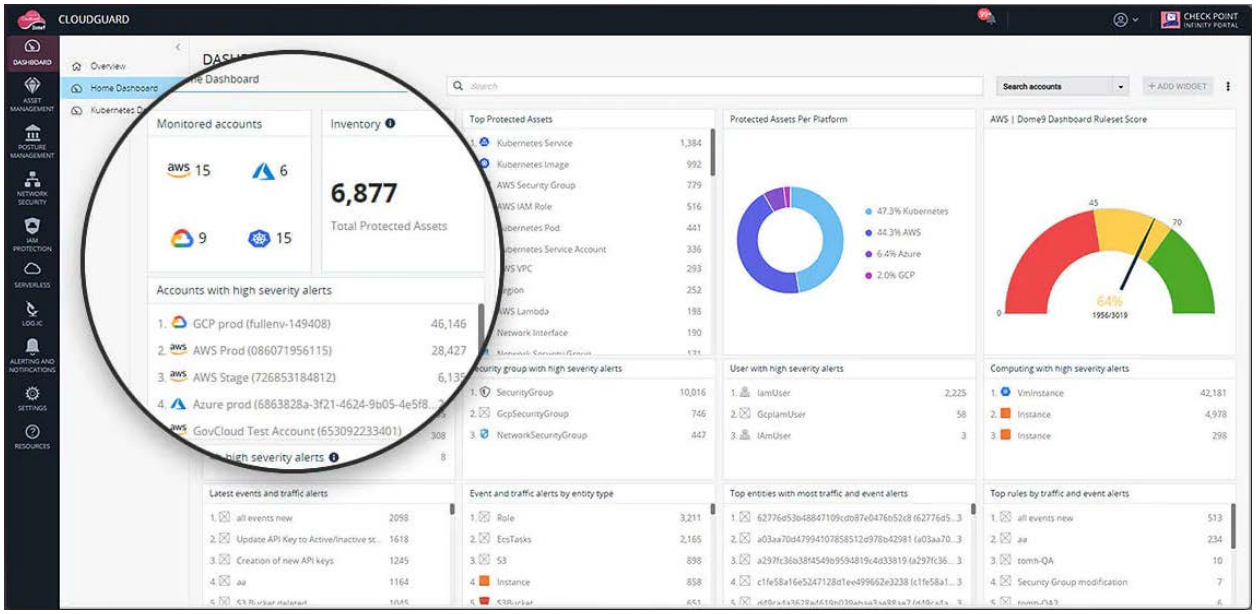
CloudGuard Cloud Security Posture Management automates governance across multi-cloud assets and services including visualization and assessment of security posture, misconfiguration detection, and enforcement of security best practices and compliance frameworks.

[Product Demo]

6. **Key Values and Differentiators**:
    - Granular, intuitive visibility into all cloud assets, networks, and security groups
    - Conform to regulatory requirements and security best practices automatically
    - Enforce access based on IAM users and roles to most sensitive operations
7. **Features include:**
    - Visualization of cloud assets, including network topology, firewalls, etc.
    - Auto-remediation solutions for AWS
    - Cloud security intelligence
    - Continuous monitoring and automation reversion of unauthorized modifications
    - Compliance management

Screenshots of UI:





Vantage

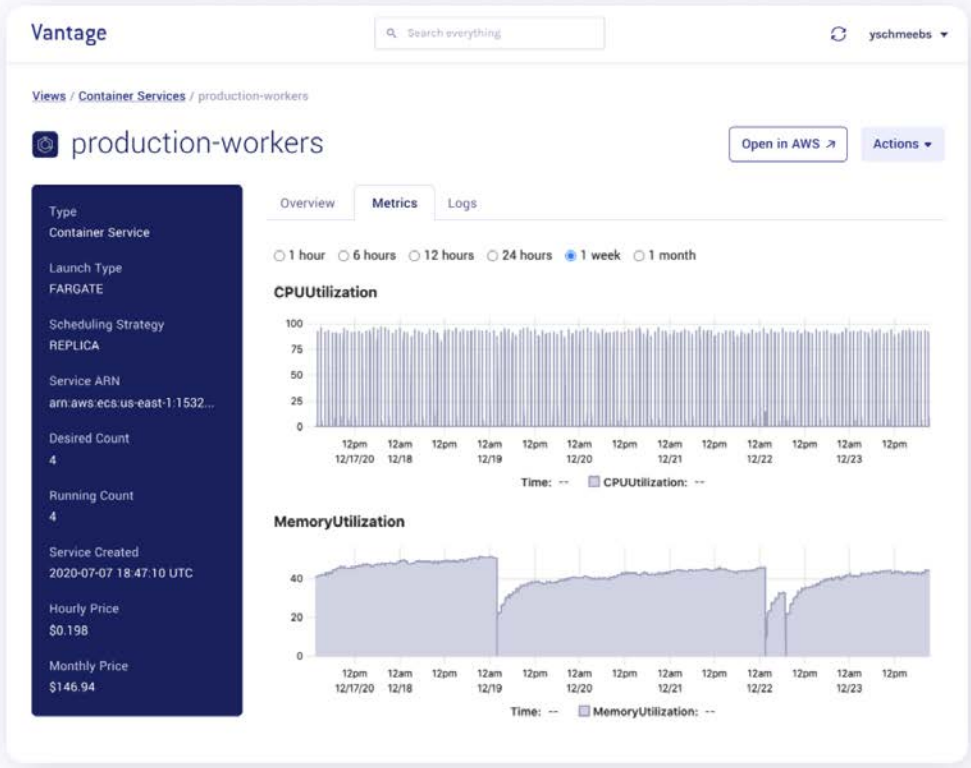
Vantage is your AWS companion, focused on user experience and cost transparency. Vantage is a team of product managers, designers and engineers committed to providing a superior developer experience for public cloud. They are applying what they've learned from combined experience at AWS and DigitalOcean, and reimagining what the experience of the cloud can be.

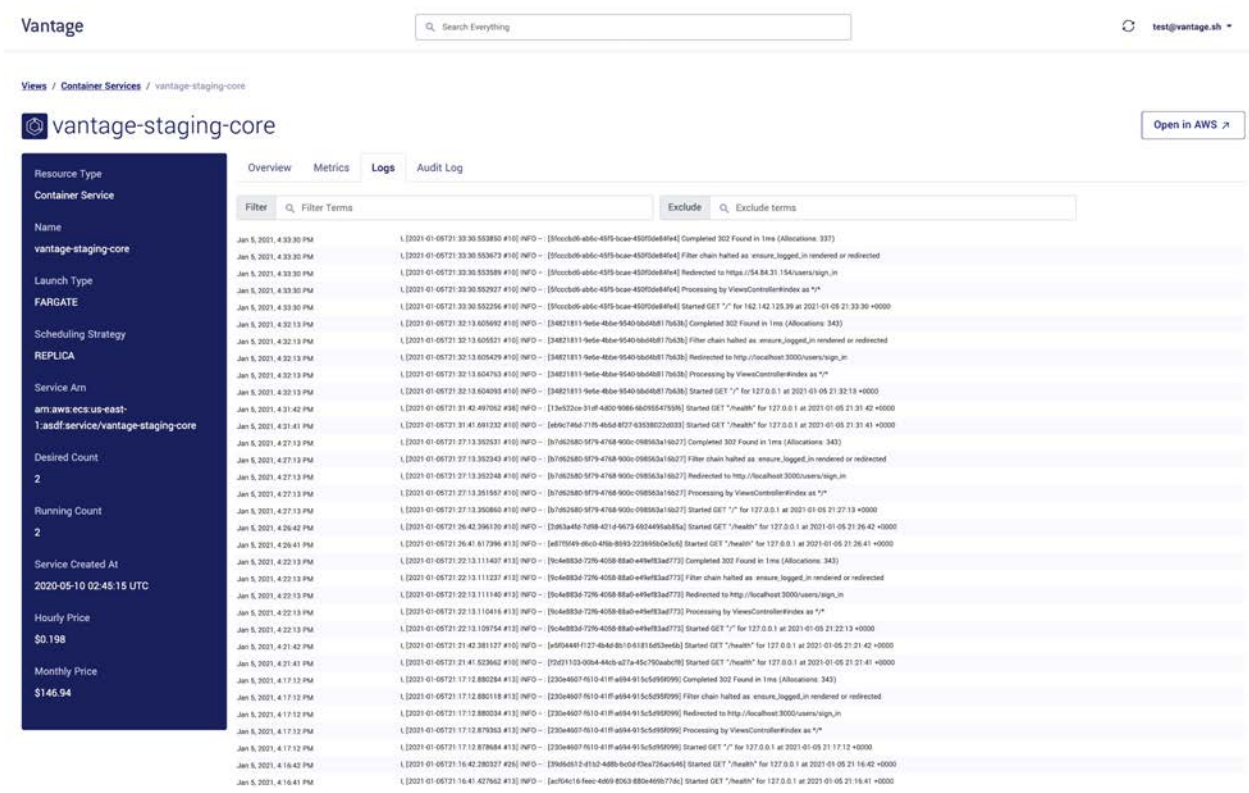
8. **Key Values and Differentiators**:

- Views allow you to group different parts of your infrastructure together through conditions or using tags
- One click to connect
- Read-only by default
- Global search

9. **Features include:**
    - Cost visibility
    - Cross region visibility
    - Merge multiple AWS accounts into a single workspace
    - Leverage AWS best practices for securely syncing and storing data
    - Discover relationships
    - Audit logs, CloudWatch logs and metrics

Screenshots of UI:





Create a new view

Start with one of the basics, then add additional criteria to refine your View.

Custom View

View from Tag

Recommended For You

Below is a list of popular view templates that you can further edit and customize if you'd like:

Unassigned IP Addresses
Clean up any IP addresses you aren't using.

Unattached EBS Volumes
Never lose track of an orphaned block storage volume again.

My IAM Roles
Filter out AWS roles for just the roles I created.

All Paid Resources
A view of everything costing you money.

Vantage Offered Views

Below is a list of views managed by Vantage. These views can not be edited as they have custom functionality:

Unused Security Groups
Find unused security groups.

Empty S3 Buckets
Find and remove empty buckets.

Lumigo

Lumigo lets developers effortlessly find and fix issues in serverless and microservices environments with one-click distributed tracing.

10. **Key Values and Differentiators**:
    - Find and fix issues in seconds with visual debugging; everything is displayed in a visual map that can be searched and filtered
    - Automatic distributed tracking of entire environment including Lambdas, other AWS services, and every API call and external SaaS service
    - Automatically identifies worst latency offenders and remove performance bottlenecks
    - Using machine learning, Lumigo's predictive analytics identifies and alerts on issues before they impact app performance or costs
11. **Features include:**
    - Debugging
    - Correlation engine; see only relevant logs and debugging information related to a transaction
    - Logs, traces, and metrics
    - One-click integration to your AWS account
    - Issues page

Screenshots of UI:

SafeBreach

SafeBreach enables security teams to provide data-driven proof of security, eliminate security blind spots and weaknesses, and validate that controls are working as expected. SafeBreach Insights automatically analyzes thousands of results, and continually provides detailed guidance for the security team to quickly remediate gaps or suboptimal configurations in your security controls.

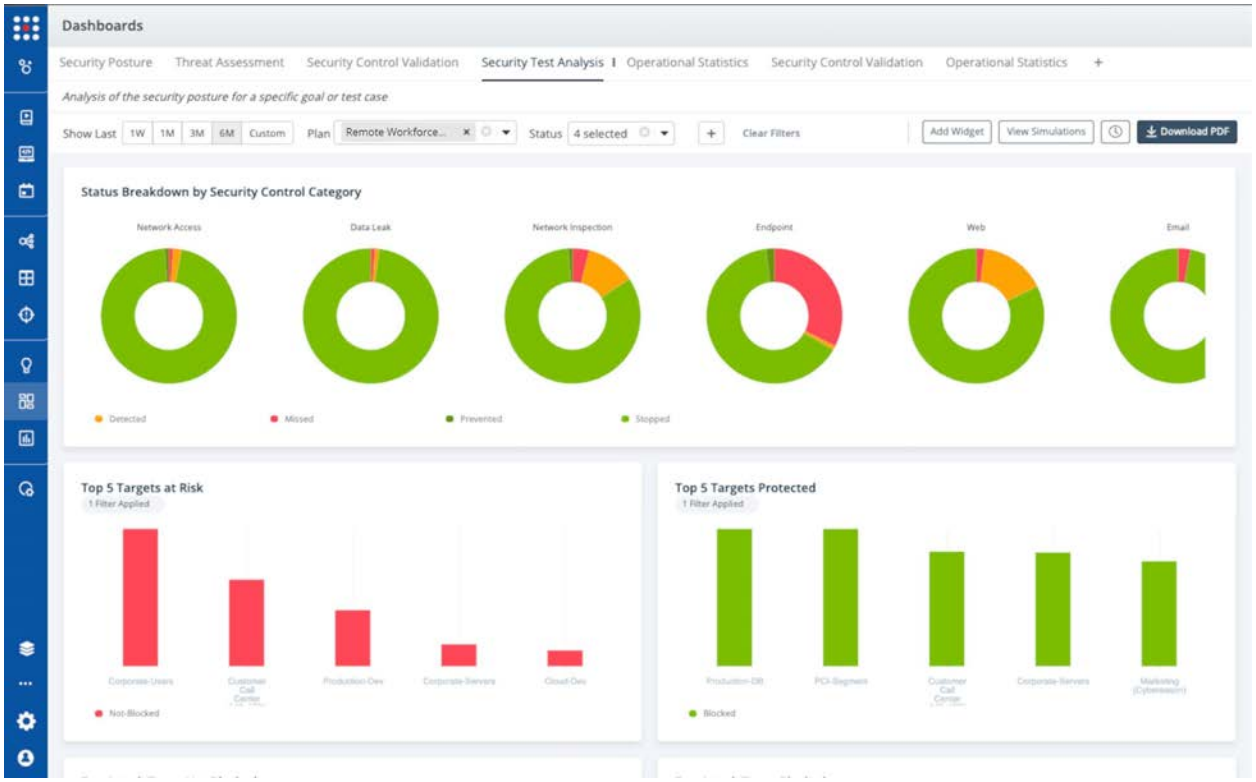
Product Tour

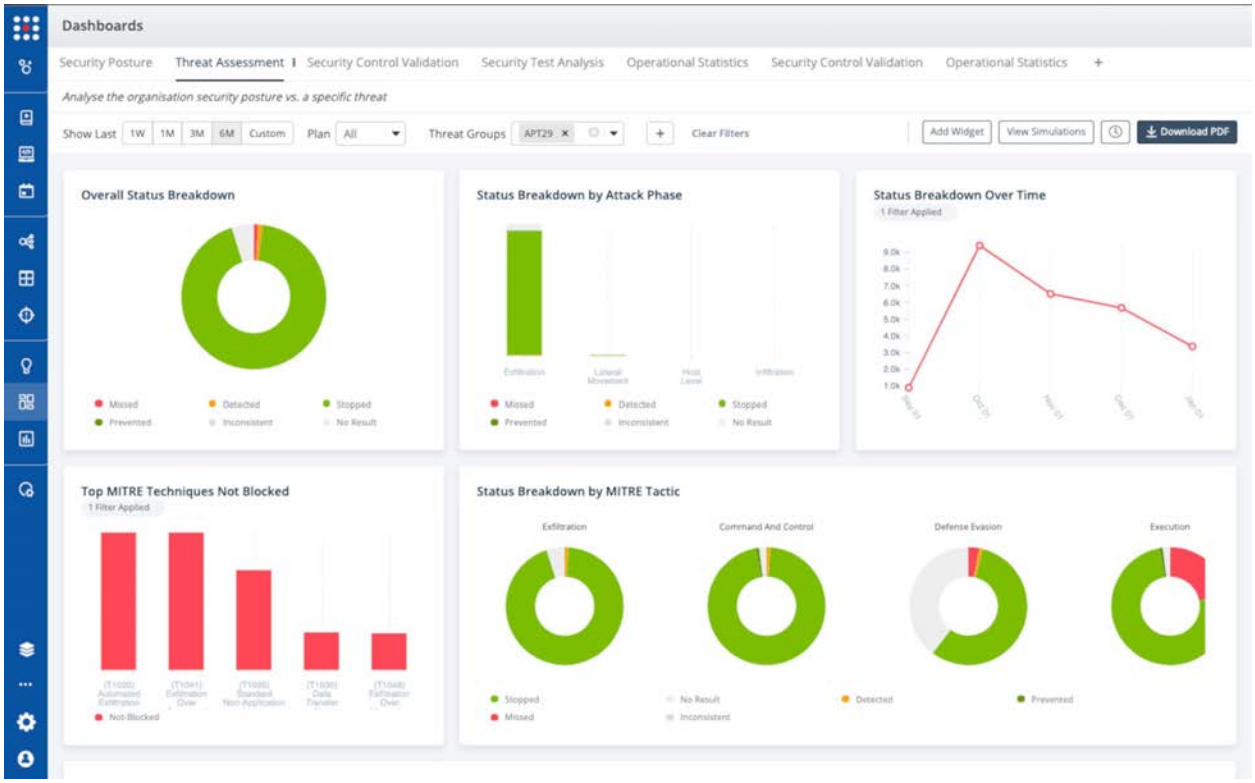
12. **Key Values and Differentiators**:
    - Validate security controls with over 15,000 attack methods to test defenses across your network, endpoint and cloud solutions

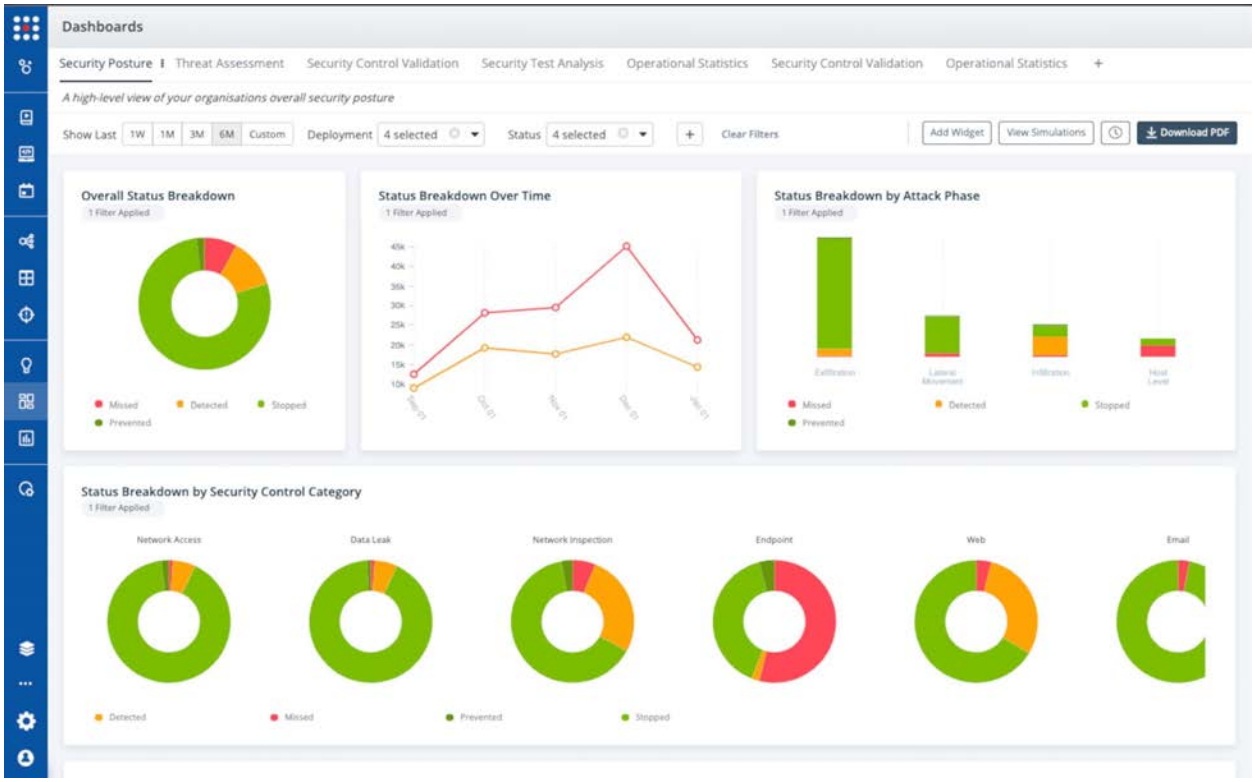
- Detailed network topology view shows all exposures along the cyber attack kill chain
- Data-driven results prioritize remediation of security controls and vulnerability management patching of systems that are actually exploitable
- Collaborate across Security and Infrastructure teams with actionable remediation data and feed mitigation data to your network, endpoint, SIEM and SOAR solutions

13. **Features include:**
    -

Screenshots of UI:




Dashboards
Security Posture
Threat Assessment
Security Control Validation
Security Test Analysis
Operational Statistics
Security Control Validation
Operational Statistics
Analyse the organisation security posture vs. a specific threat
Show Last 1W 1M 3M 6M Custom
Plan All
Threat Groups APT29
Clear Filters
Add Widget
View Simulations
Download PDF
Overall Status Breakdown
Missed
Detected
Stopped
Prevented
Inconsistent
No Result
Status Breakdown by Attack Phase
Status Breakdown Over Time
1 Filter Applied
Top MITRE Techniques Not Blocked
1 Filter Applied
Not-Blocked
Status Breakdown by MITRE Tactic
Exfiltration
Command And Control
Defense Evasion
Execution
Stopped
Missed
No Result
Inconsistent
Detected
Prevented


Dashboards
Security Posture
Threat Assessment
Security Control Validation
Security Test Analysis
Operational Statistics
Security Control Validation
Operational Statistics
A high-level view of your organisations overall security posture
Show Last 1W 1M 3M 6M Custom
Deployment 4 selected
Status 4 selected
Clear Filters
Add Widget
View Simulations
Download PDF
Overall Status Breakdown
1 Filter Applied
Missed
Detected
Stopped
Prevented
Status Breakdown Over Time
1 Filter Applied
Status Breakdown by Attack Phase
1 Filter Applied
Status Breakdown by Security Control Category
1 Filter Applied
Network Access
Data Leak
Network Inspection
Endpoint
Web
Email
Detected
Missed
Prevented
Stopped