FORTINET®

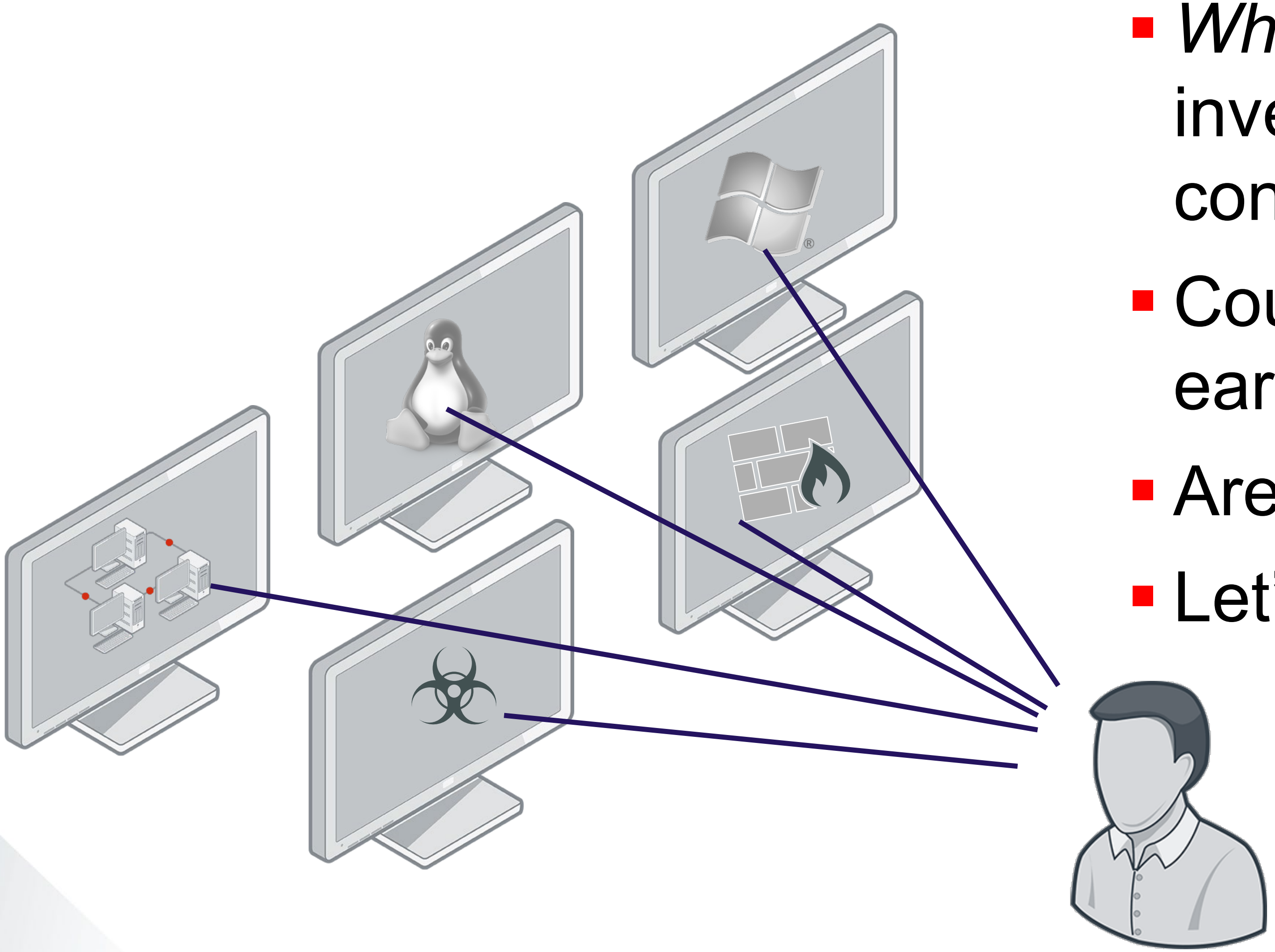
FortiSIEM

Visibility, Correlation, Automated Response and Remediation in a single, scalable solution

Silviu Pufan

Channel Systems Engineer – SEE

IT&C Monitoring – “No Time for Downtime”



- Many systems to monitor
- *When* an incident occurs, investigations can be very time consuming.
- Could we have detected the incident earlier?
- Are we still compromised or at Risk?
- Let’s *hope* not…..

Current monitoring is not scalable.. Silo’d tools

NOC

PRTG NETWORK MONITOR

Nagios

Kaseya

ScienceLogic

WIRESHARK

TICKETING SYSTEMS

servicenow

ConnectWise

Remedy Corporation

SOC

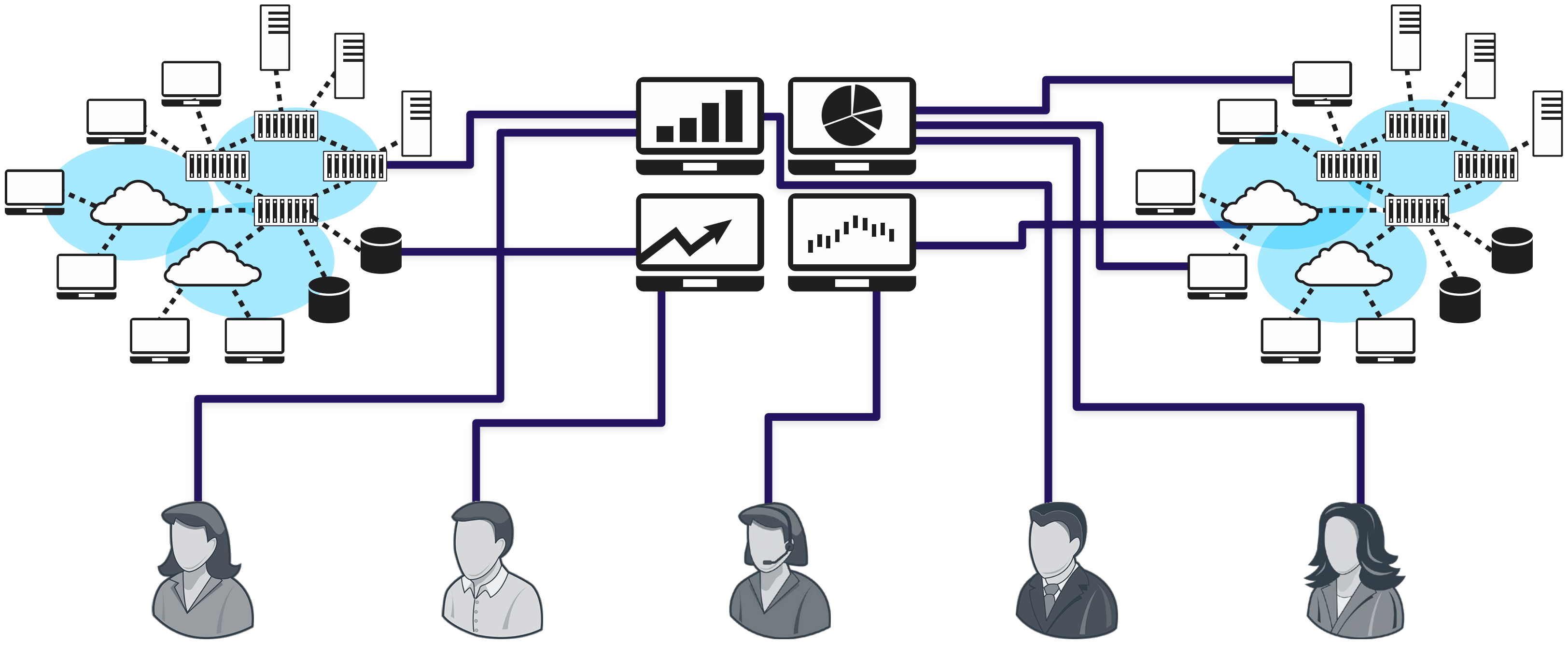
NetIQ

loggly

TIBCO

tripwire

sumologic



NOC Team

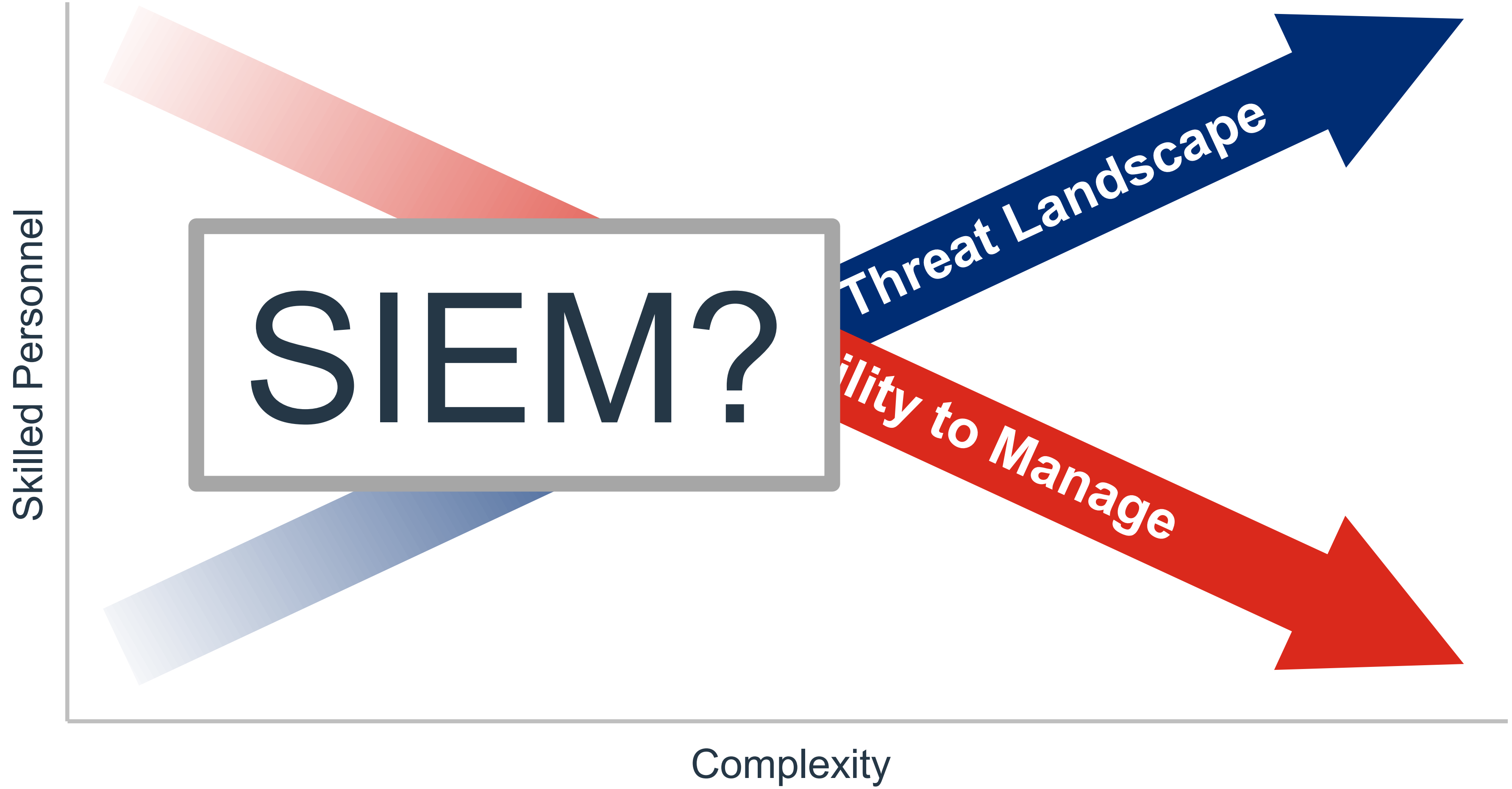
SOC Team

Help Desk

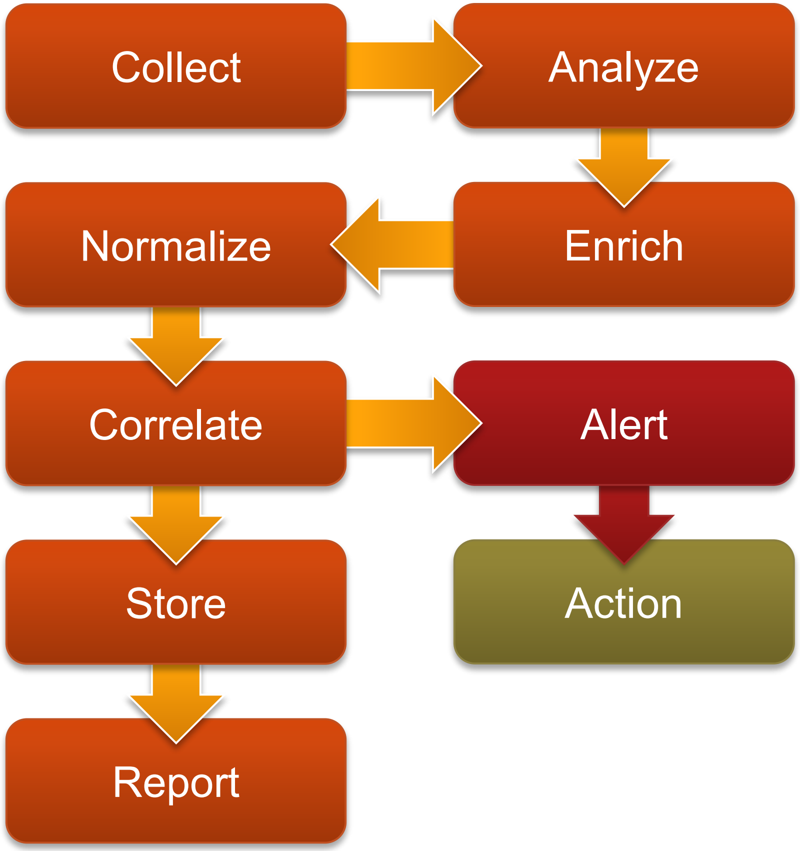
Datacenter Director

Systems, Admin

Dynamics of Current Conditions



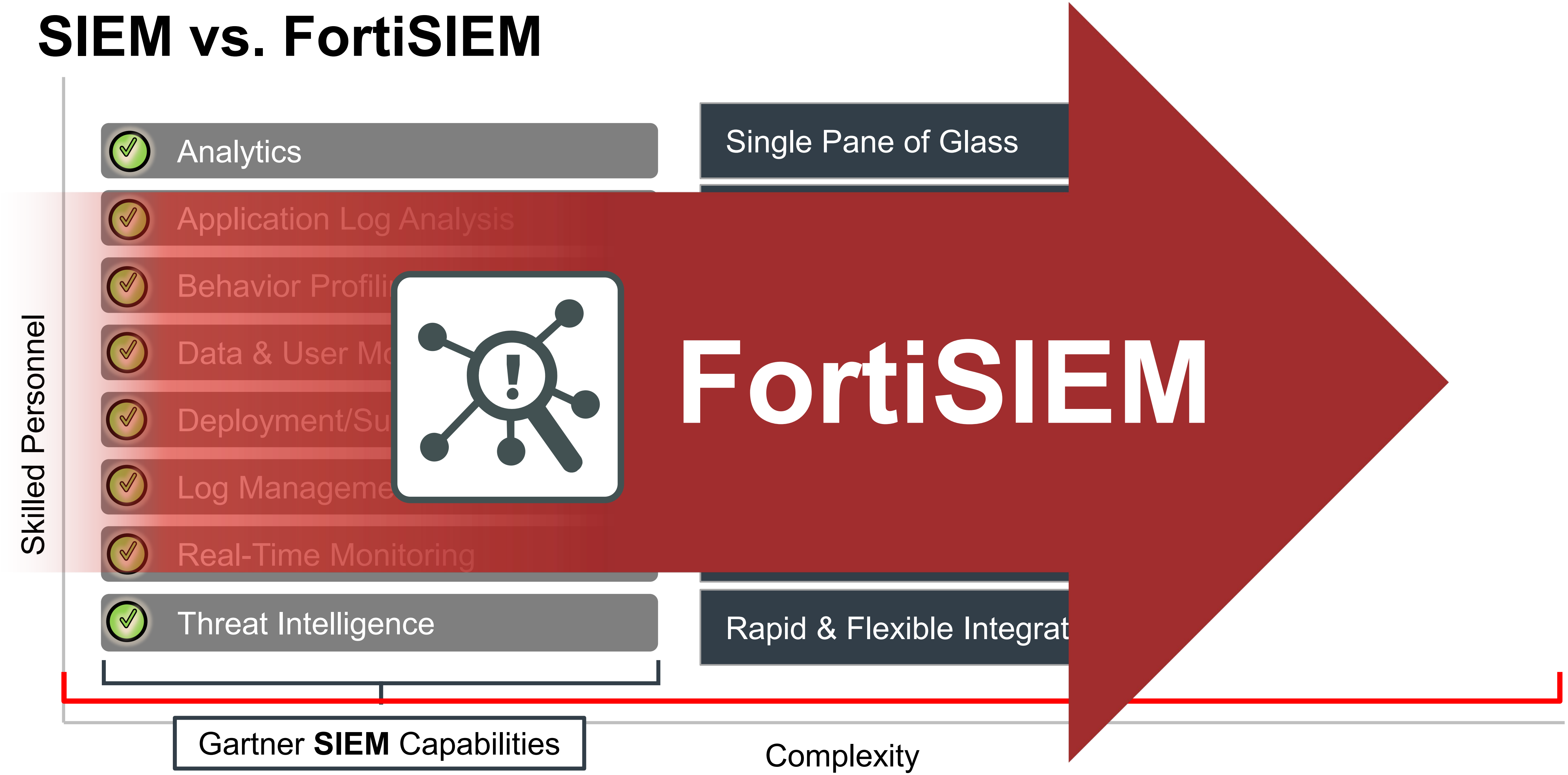
So what is SIEM



- Security Information & Event Management
- Input – Collects logs
- Transformation - Analysis/Correlation
- Output – Alerts/Reports/Dashboards

```
May 6 17:55:48 squid[1773]: [ID 702911 local4.info] 192.168.20.39 1715 2.2.2.2 172.16.10.6
3128 674 - - - - - [06/May/2008:17:55:48 -0700] GET "http://mail.abc.com/mail/?" HTTP/1.1 302
1061 568 "http://www.abc.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.14)
Gecko/20080404 Firefox/2.0.0.14" TCP_MISS:DIRECT
```

SIEM vs. FortiSIEM



Skilled Personnel

✓ Analytics

✓ Application Log Analysis

✓ Behavior Profili

✓ Data & User Mo

✓ Deployment/Su

✓ Log Manageme

✓ Real-Time Monitoring

✓ Threat Intelligence

Single Pane of Glass

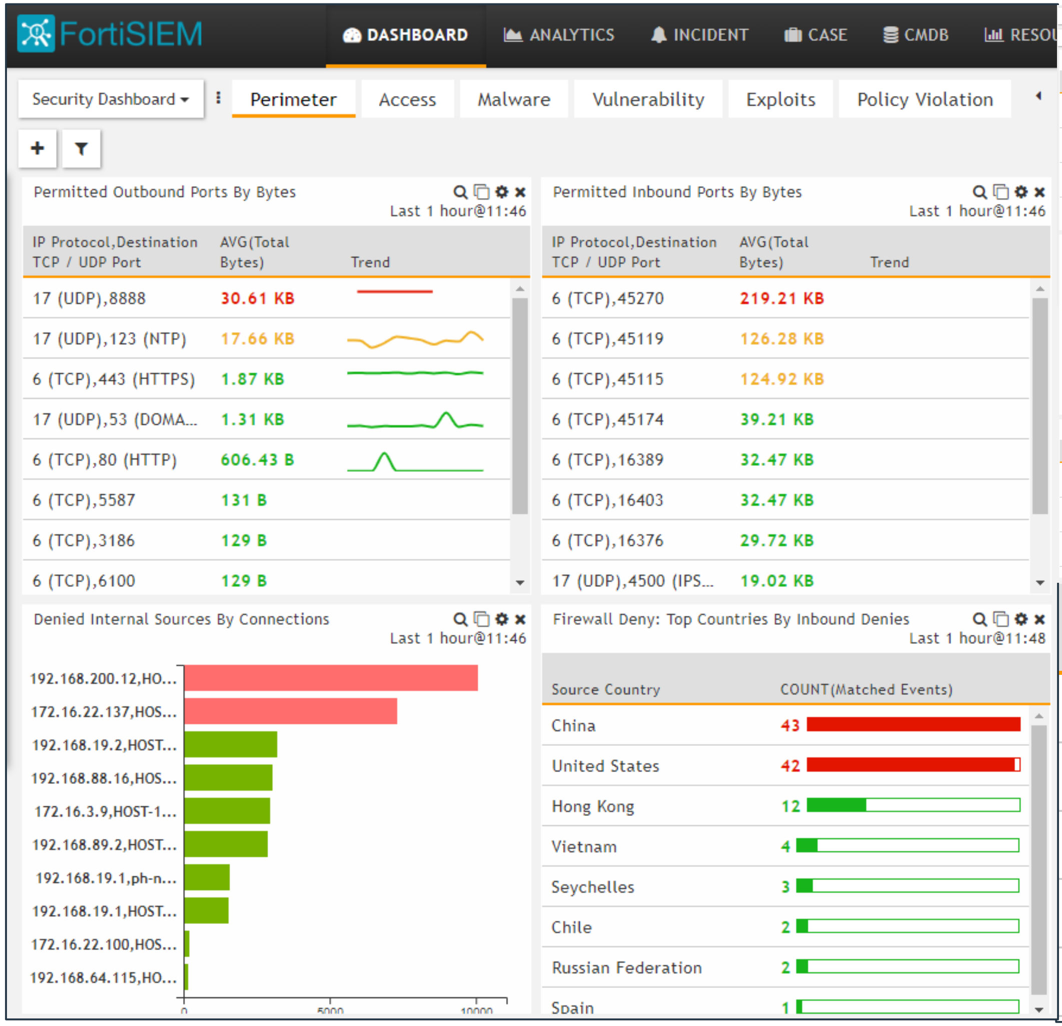
Rapid & Flexible Integrat

FortiSIEM

Gartner **SIEM** Capabilities

Complexity

Unified NOC & SOC



Permitted Outbound Ports By Bytes
Last 1 hour@11:46

IP Protocol,Destination TCP / UDP Port	AVG(Total Bytes)	Trend
17 (UDP),8888	30.61 KB	
17 (UDP),123 (NTP)	17.66 KB	
6 (TCP),443 (HTTPS)	1.87 KB	
17 (UDP),53 (DOMA...	1.31 KB	
6 (TCP),80 (HTTP)	606.43 B	
6 (TCP),5587	131 B	
6 (TCP),3186	129 B	
6 (TCP),6100	129 B	

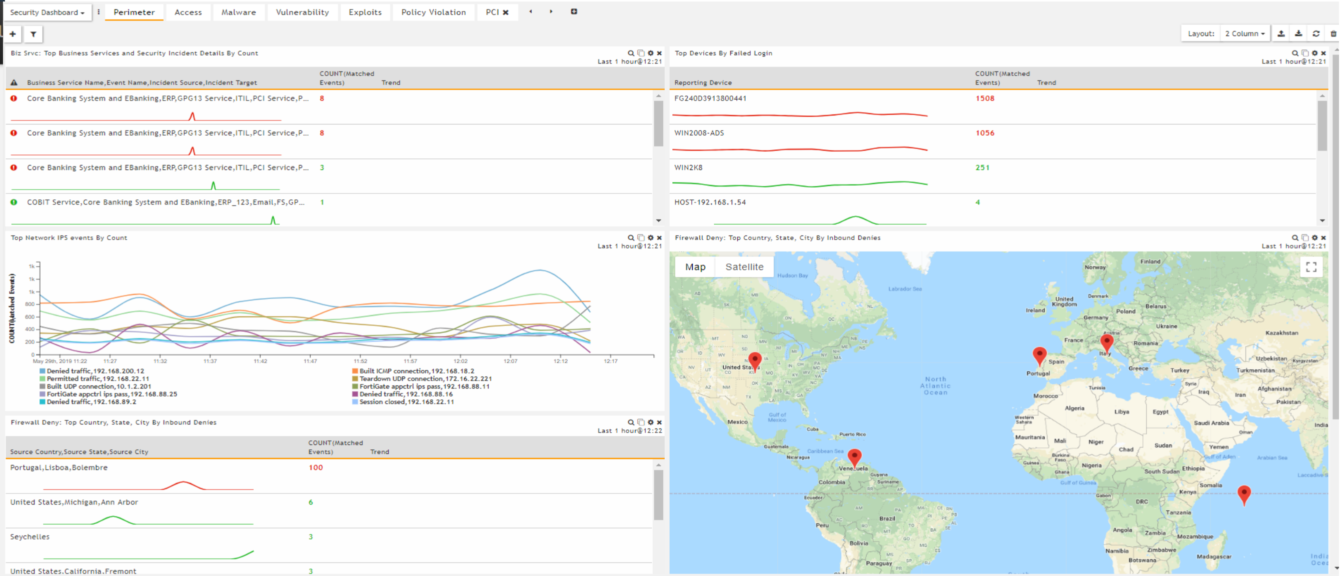
Permitted Inbound Ports By Bytes
Last 1 hour@11:46

IP Protocol,Destination TCP / UDP Port	AVG(Total Bytes)	Trend
6 (TCP),45270	219.21 KB	
6 (TCP),45119	126.28 KB	
6 (TCP),45115	124.92 KB	
6 (TCP),45174	39.21 KB	
6 (TCP),16389	32.47 KB	
6 (TCP),16403	32.47 KB	
6 (TCP),16376	29.72 KB	
17 (UDP),4500 (IPS...	19.02 KB	

Denied Internal Sources By Connections
Last 1 hour@11:46

Firewall Deny: Top Countries By Inbound Denies
Last 1 hour@11:48

Source Country	COUNT(Matched Events)
China	43
United States	42
Hong Kong	12
Vietnam	4
Seychelles	3
Chile	2
Russian Federation	2
Spain	1



Biz Srvc: Top Business Services and Security Incident Details By Count
Last 1 hour@12:21

Business Service Name,Event Name,Incident Source,Incident Target	COUNT(Matched Events)	Trend
Core Banking System and EBanking,ERP,GPG13 Service,ITIL,PCI Service,P...	8	
Core Banking System and EBanking,ERP,GPG13 Service,ITIL,PCI Service,P...	8	
Core Banking System and EBanking,ERP,GPG13 Service,ITIL,PCI Service,P...	3	
COBIT Service,Core Banking System and EBanking,ERP_123,Email,FS,GP...	1	

Top Devices By Failed Login
Last 1 hour@12:21

Reporting Device	COUNT(Matched Events)	Trend
FG240D3913800441	1508	
WIN2008-ADS	1056	
WIN2K8	251	
HOST-192.168.1.54	4	

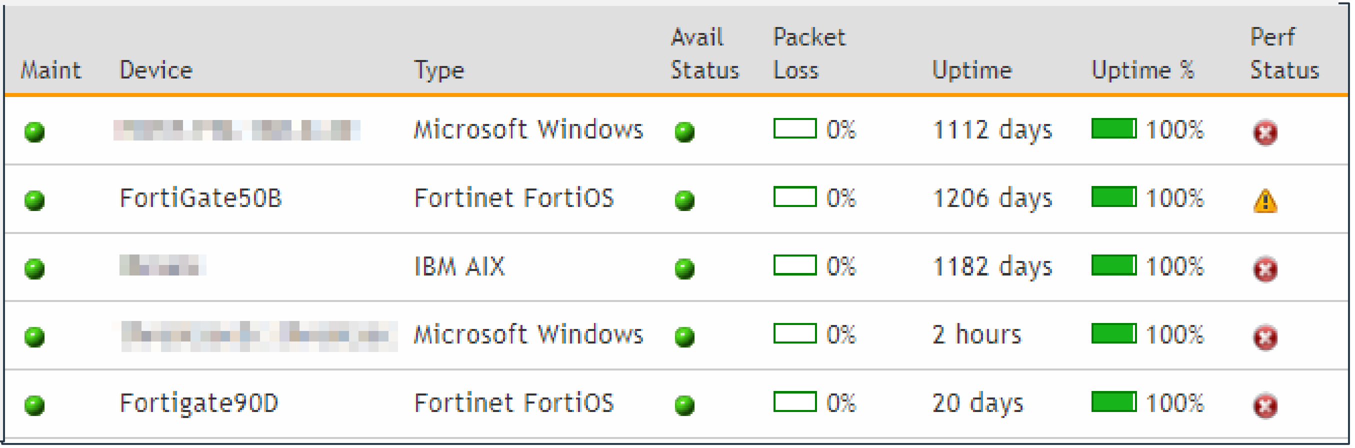
Top Network IPS events By Count
Last 1 hour@12:21

COUNT(Matched Events)
1k
1k
1k
800
600
400
200
0
May 29th, 2019 11:22
11:27
11:32
11:37
11:42
11:47
11:52
11:57
12:02
12:07
12:12
12:17
Denied traffic,192.168.200.12
Permitted traffic,192.168.22.11
Built UDP connection,10.1.2.201
FortiGate appctrl ips pass,192.168.88.25
Denied traffic,192.168.89.2
Built ICMP connection,192.168.18.2
Teardown UDP connection,172.16.22.221
FortiGate appctrl ips pass,192.168.88.11
Denied traffic,192.168.88.16
Session closed,192.168.22.11

Firewall Deny: Top Country, State, City By Inbound Denies
Last 1 hour@12:22

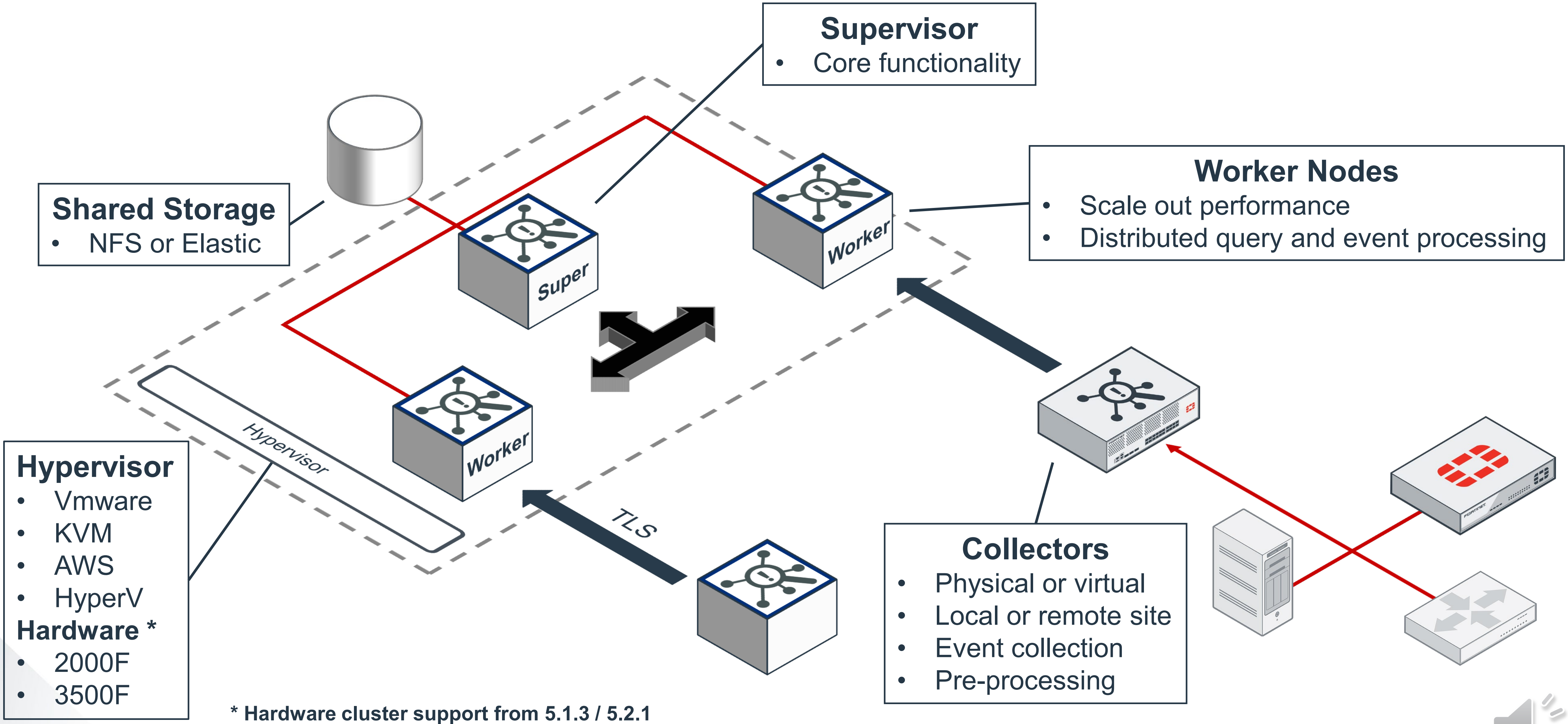
Source Country,Source State,Source City	COUNT(Matched Events)	Trend
Portugal,Lisboa,Bolembre	100	
United States,Michigan,Ann Arbor	6	
Seychelles	3	
United States,California,Fremont	3	

Firewall Deny: Top Country, State, City By Inbound Denies
Last 1 hour@12:21



Maint	Device	Type	Avail Status	Packet Loss	Uptime	Uptime %	Perf Status
●	[redacted]	Microsoft Windows	●	0%	1112 days	100%	☒
●	FortiGate50B	Fortinet FortiOS	●	0%	1206 days	100%	⚠
●	[redacted]	IBM AIX	●	0%	1182 days	100%	☒
●	[redacted]	Microsoft Windows	●	0%	2 hours	100%	☒
●	Fortigate90D	Fortinet FortiOS	●	0%	20 days	100%	☒

Scalable Architecture



Supervisor
- Core functionality

Worker Nodes
- Scale out performance
- Distributed query and event processing

Shared Storage
- NFS or Elastic

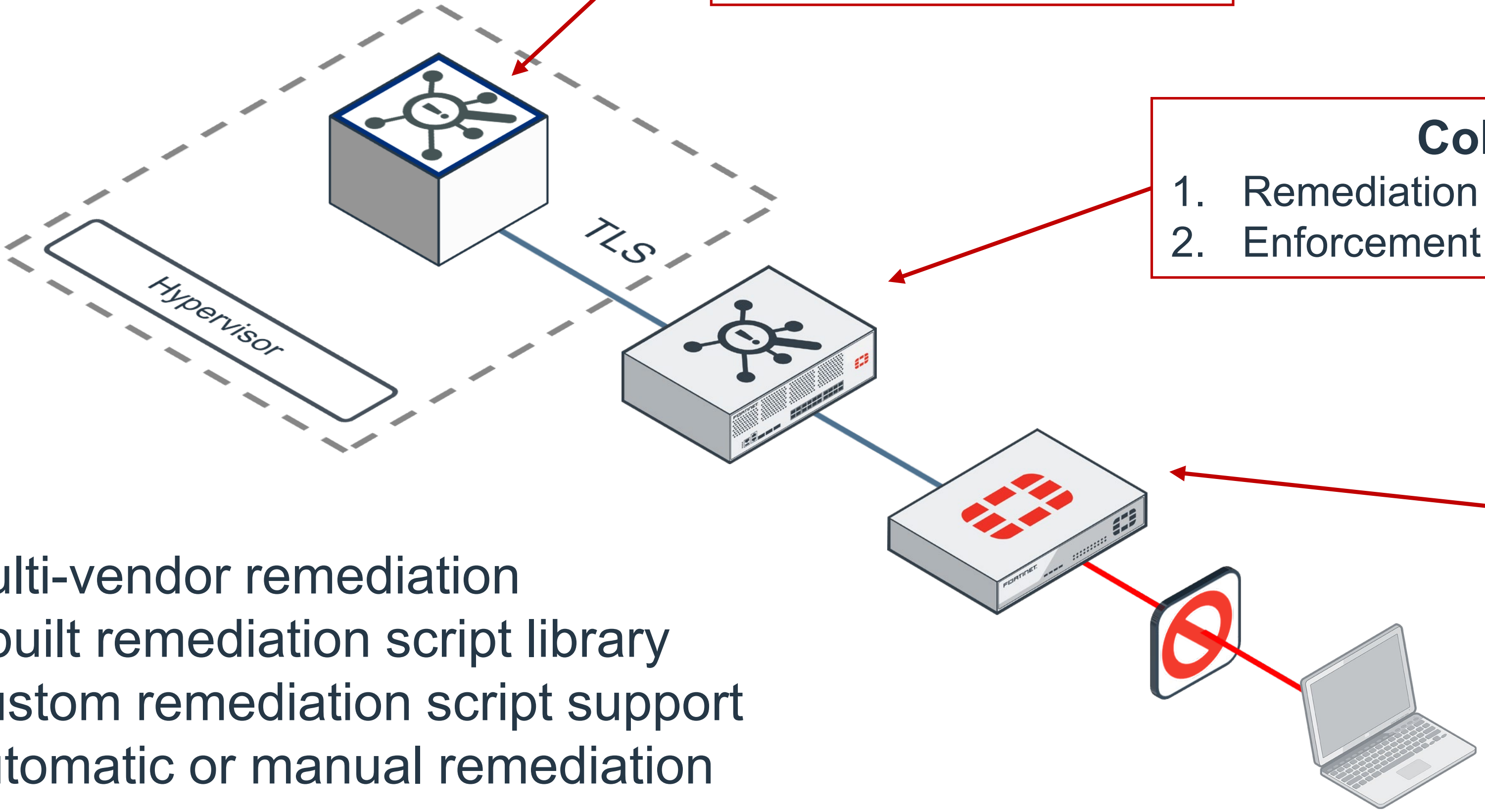
Hypervisor
- Vmware
- KVM
- AWS
- HyperV

Hardware *
- 2000F
- 3500F

Collectors
- Physical or virtual
- Local or remote site
- Event collection
- Pre-processing

*** Hardware cluster support from 5.1.3 / 5.2.1**

FortiSIEM Incident Remediation



Supervisor

1. Rule triggered
2. Incident generated
3. Remediation actioned

Collector

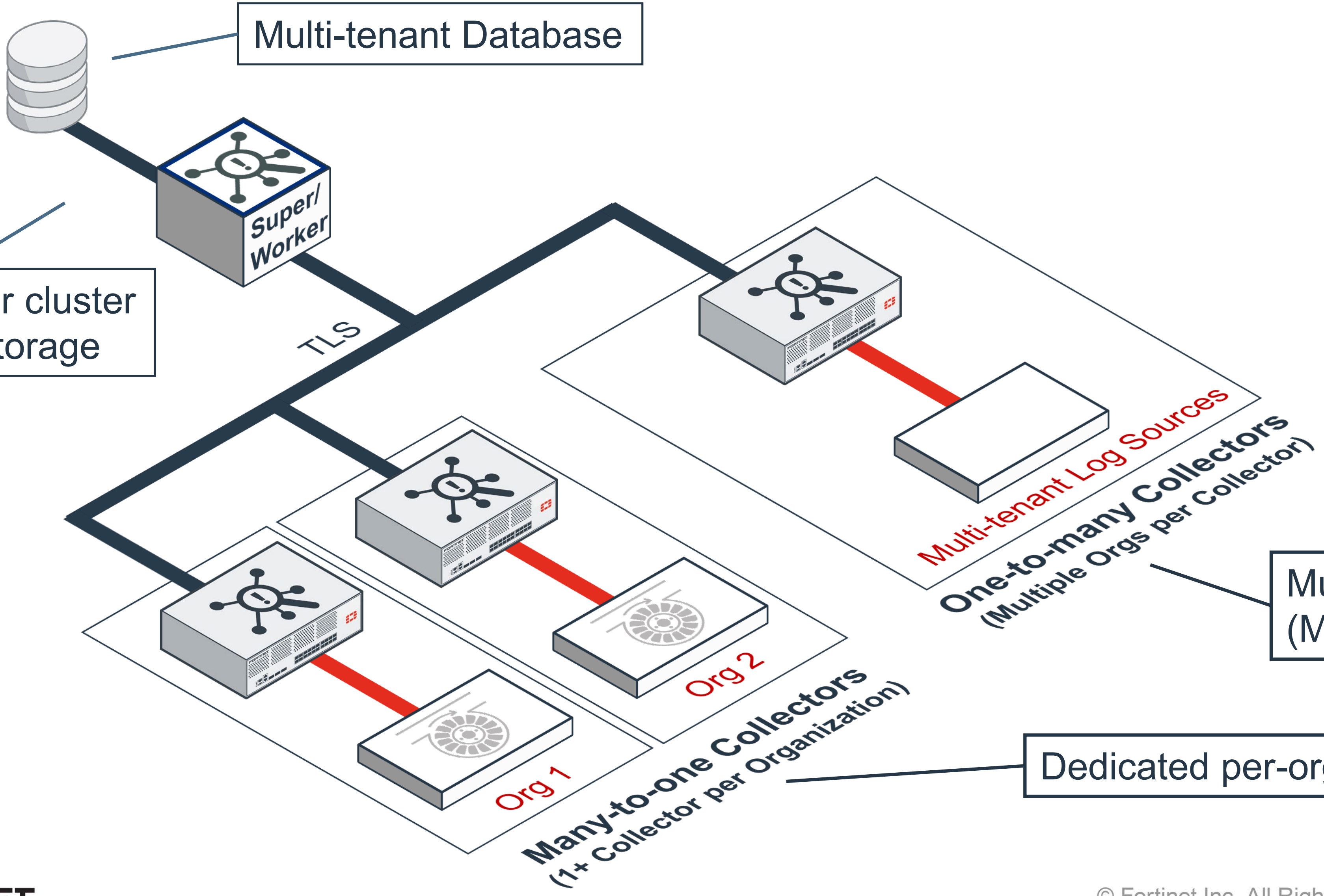
1. Remediation script executed
2. Enforcement device reconfigured

Enforcement Device

1. Enforces remediation action
   1. Block/ quarantine device
   2. De-authenticate user
   3. Etc…

- Multi-vendor remediation
- Inbuilt remediation script library
- Custom remediation script support
- Automatic or manual remediation

Multi-tenant Architecture



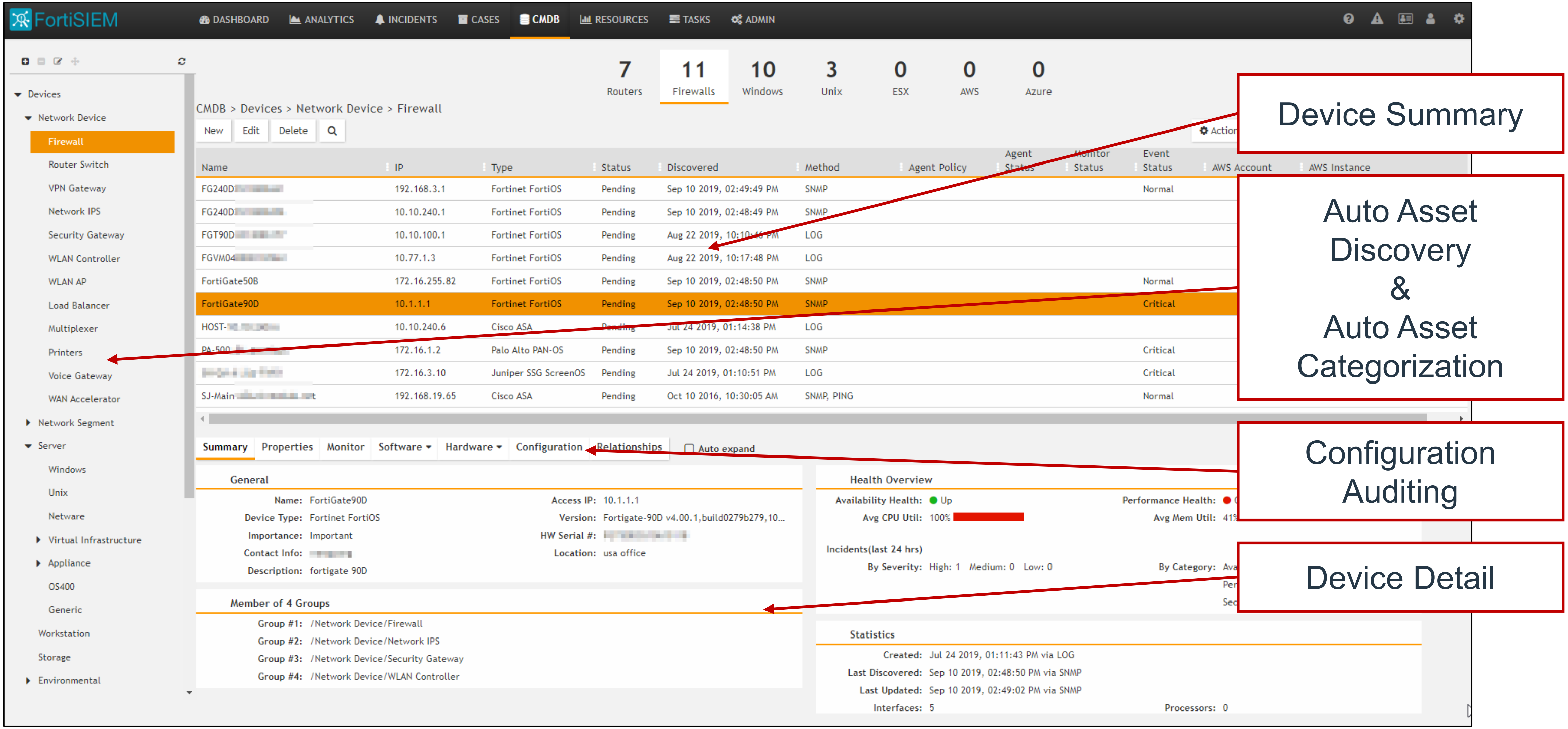
Multi-tenant Database

Super/ Worker cluster
with shared storage

Multi-tenant collector
(More on this later…)

Dedicated per-organization collector

FortiSIEM CMDB Summary



- Devices
  - Network Device
    - Firewall
    - Router Switch
    - VPN Gateway
    - Network IPS
    - Security Gateway
    - WLAN Controller
    - WLAN AP
    - Load Balancer
    - Multiplexer
    - Printers
    - Voice Gateway
    - WAN Accelerator
  - Network Segment
  - Server
    - Windows
    - Unix
    - Netware
    - Virtual Infrastructure
    - Appliance
    - OS400
    - Generic
  - Workstation
  - Storage
  - Environmental

7	11	10	3	0	0	0
Routers	Firewalls	Windows	Unix	ESX	AWS	Azure

CMDB > Devices > Network Device > Firewall

Name	IP	Type	Status	Discovered	Method	Agent Policy	Agent Status	Monitor Status	Event Status	AWS Account	AWS Instance
FG240D[redacted]	192.168.3.1	Fortinet FortiOS	Pending	Sep 10 2019, 02:49:49 PM	SNMP				Normal		
FG240D[redacted]	10.10.240.1	Fortinet FortiOS	Pending	Sep 10 2019, 02:48:49 PM	SNMP						
FGT90D[redacted]	10.10.100.1	Fortinet FortiOS	Pending	Aug 22 2019, 10:10:46 PM	LOG						
FGVM04[redacted]	10.77.1.3	Fortinet FortiOS	Pending	Aug 22 2019, 10:17:48 PM	LOG						
FortiGate50B	172.16.255.82	Fortinet FortiOS	Pending	Sep 10 2019, 02:48:50 PM	SNMP				Normal		
FortiGate90D	10.1.1.1	Fortinet FortiOS	Pending	Sep 10 2019, 02:48:50 PM	SNMP				Critical		
HOST-[redacted]	10.10.240.6	Cisco ASA	Pending	Jul 24 2019, 01:14:38 PM	LOG						
PA-500[redacted]	172.16.1.2	Palo Alto PAN-OS	Pending	Sep 10 2019, 02:48:50 PM	SNMP				Critical		
[redacted]	172.16.3.10	Juniper SSG ScreenOS	Pending	Jul 24 2019, 01:10:51 PM	LOG				Critical		
SJ-Main[redacted]t	192.168.19.65	Cisco ASA	Pending	Oct 10 2016, 10:30:05 AM	SNMP, PING				Normal		

General

Name: FortiGate90D
Device Type: Fortinet FortiOS
Importance: Important
Contact Info: [redacted]
Description: fortigate 90D
Access IP: 10.1.1.1
Version: Fortigate-90D v4.00.1,build0279b279,10...
HW Serial #: [redacted]
Location: usa office

Member of 4 Groups

Group #1: /Network Device/Firewall
Group #2: /Network Device/Network IPS
Group #3: /Network Device/Security Gateway
Group #4: /Network Device/WLAN Controller

Health Overview

Availability Health: ● Up
Performance Health: ●
Avg CPU Util: 100%
Avg Mem Util: 41

Incidents(last 24 hrs)
By Severity: High: 1 Medium: 0 Low: 0
By Category: Ava
Per
Sec

Statistics

Created: Jul 24 2019, 01:11:43 PM via LOG
Last Discovered: Sep 10 2019, 02:48:50 PM via SNMP
Last Updated: Sep 10 2019, 02:49:02 PM via SNMP
Interfaces: 5
Processors: 0

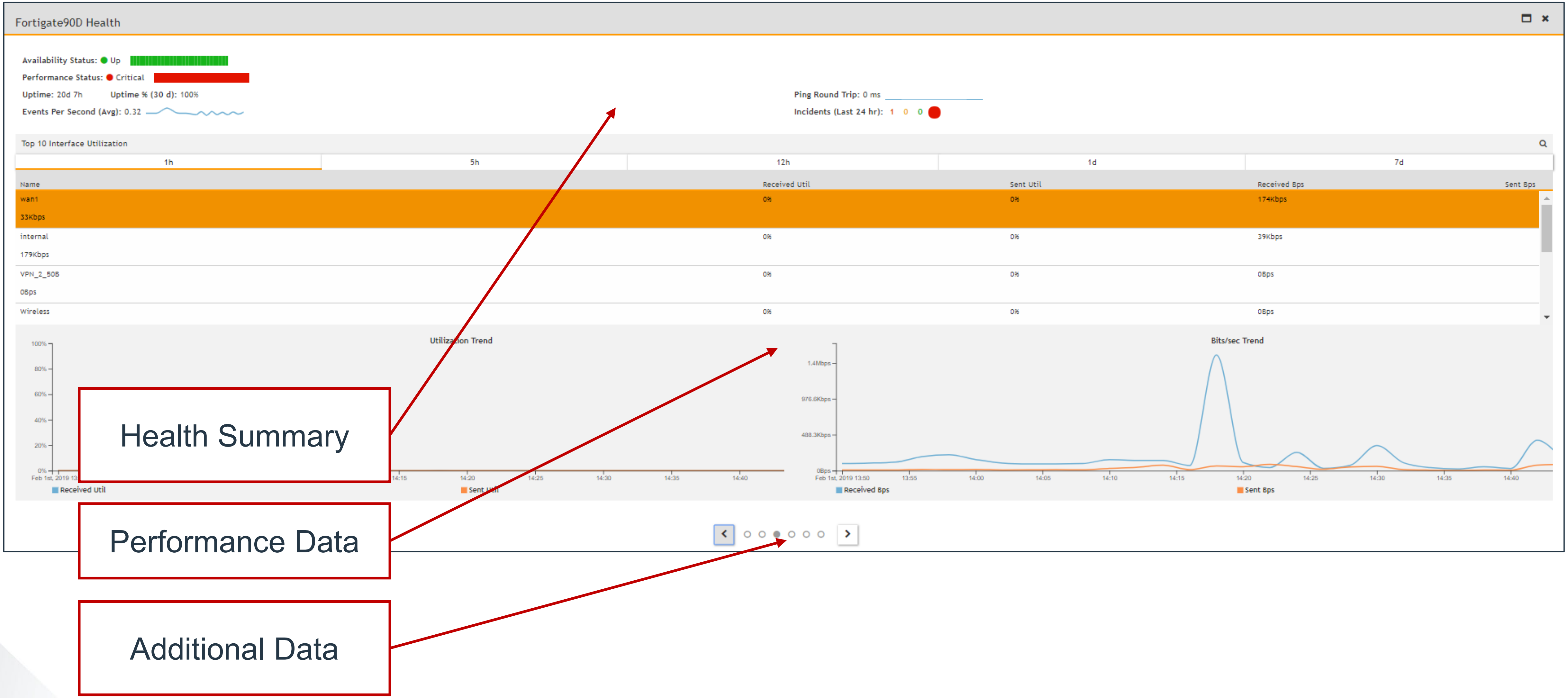
Device Summary

Auto Asset Discovery & Auto Asset Categorization

Configuration Auditing

Device Detail

CMDB Performance and Availability Monitoring



Fortigate90D Health

Availability Status: ● Up

Performance Status: ● Critical

Uptime: 20d 7h Uptime % (30 d): 100%

Events Per Second (Avg): 0.32

Ping Round Trip: 0 ms

Incidents (Last 24 hr): 1 0 0 ●

Top 10 Interface Utilization

1h | 5h | 12h | 1d | 7d

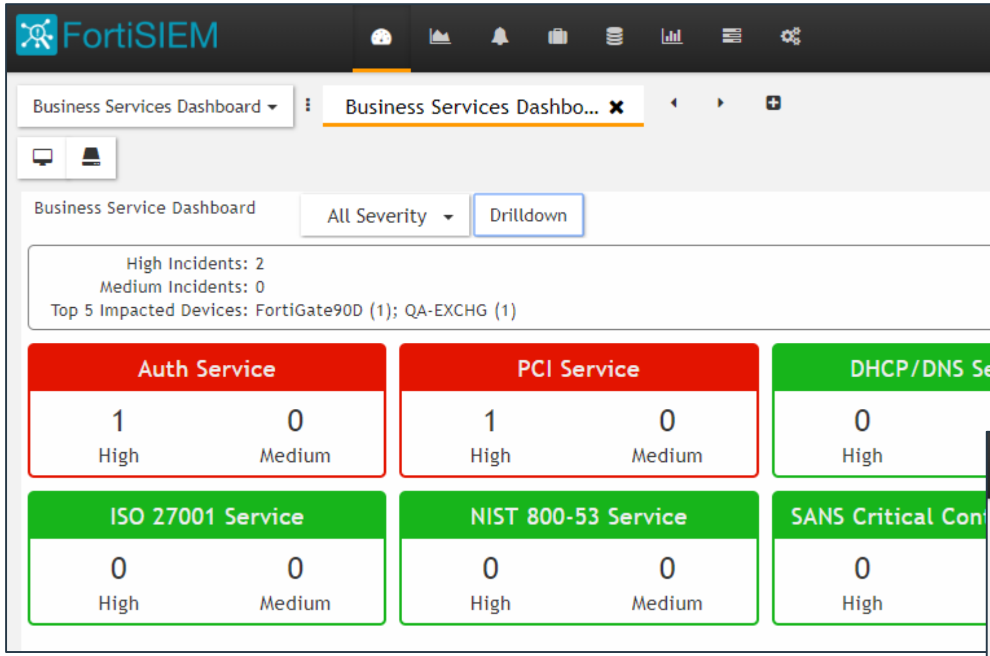
Name	Received Util	Sent Util	Received Bps	Sent Bps
wan1	0%	0%	174Kbps	33Kbps
internal	0%	0%	39Kbps	179Kbps
VPN_2_50B	0%	0%	0Bps	0Bps
Wireless	0%	0%	0Bps	

Health Summary

Performance Data

Additional Data

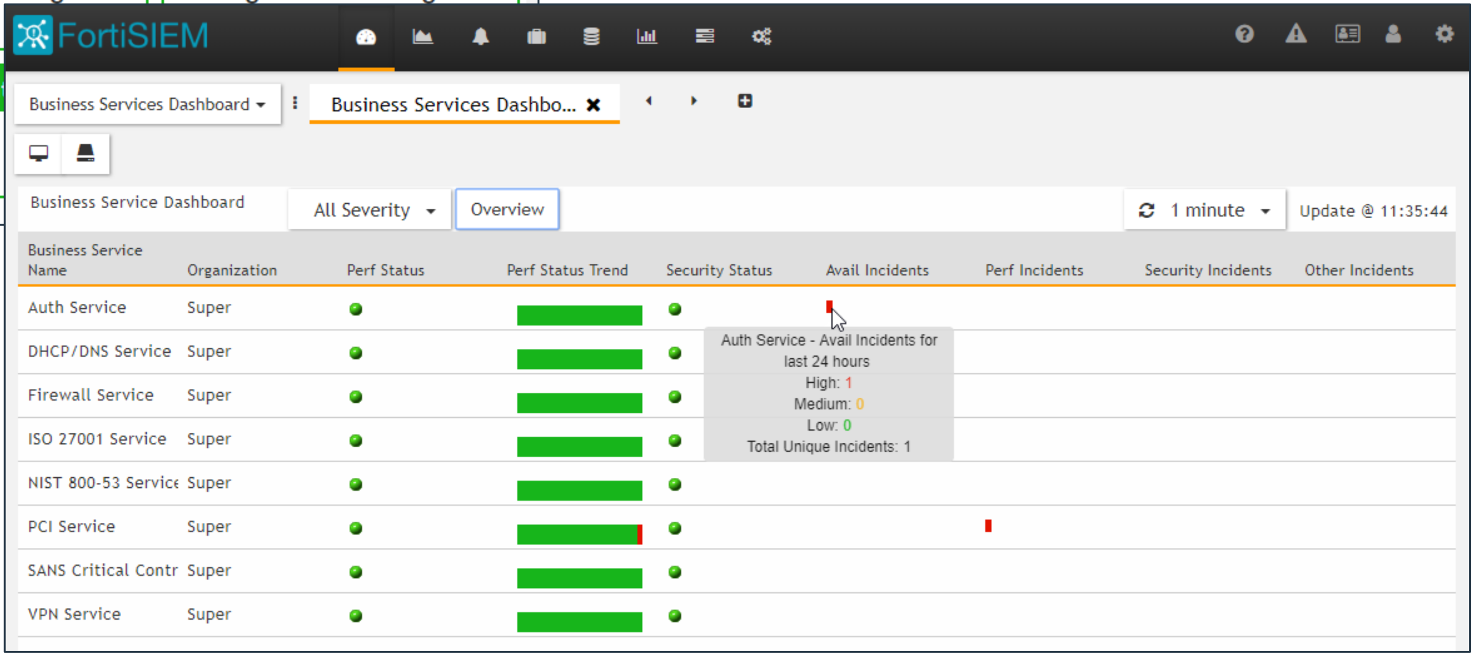
CMDB Business Services



Business Service Dashboard All Severity Drilldown 1 minute Update @ 11:35:08

High Incidents: 2
Medium Incidents: 0
Top 5 Impacted Devices: FortiGate90D (1); QA-EXCHG (1)

Auth Service: 1 High, 0 Medium
PCI Service: 1 High, 0 Medium
DHCP/DNS Service: 0 High, 0
Firewall Service: 0, 0
ISO 27001 Service: 0 High, 0 Medium
NIST 800-53 Service: 0 High, 0 Medium
SANS Critical Con: 0 High



Business Service Dashboard All Severity Overview 1 minute Update @ 11:35:44

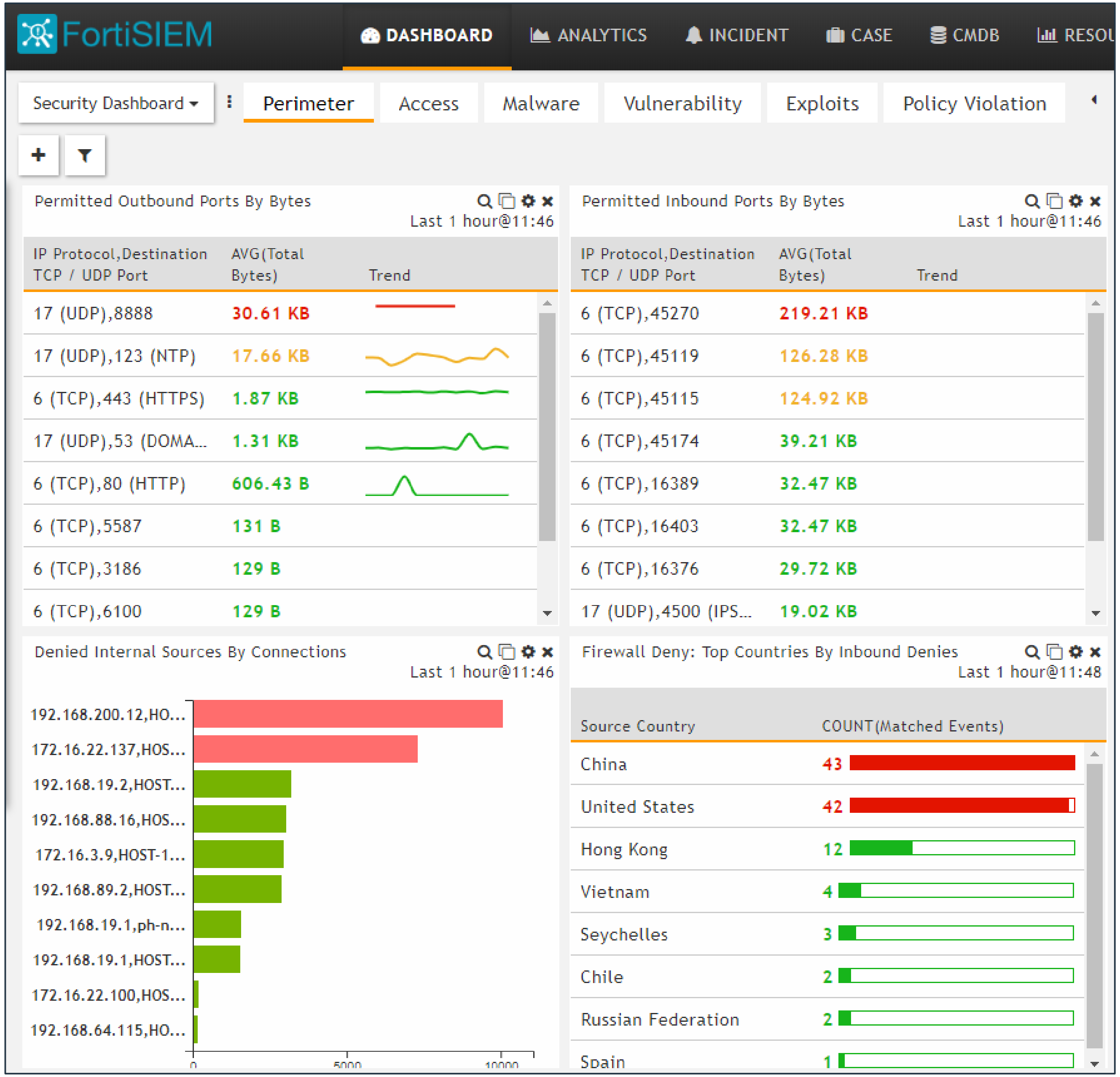
Business Service Name	Organization	Perf Status	Perf Status Trend	Security Status	Avail Incidents	Perf Incidents	Security Incidents	Other Incidents
Auth Service	Super	●	🟩	●	🟥			
DHCP/DNS Service	Super	●	🟩	●				
Firewall Service	Super	●	🟩	●				
ISO 27001 Service	Super	●	🟩	●				
NIST 800-53 Service	Super	●	🟩	●				
PCI Service	Super	●	🟩	●		🟥		
SANS Critical Contr	Super	●	🟩	●				
VPN Service	Super	●	🟩	●				

Auth Service - Avail Incidents for last 24 hours
High: 1
Medium: 0
Low: 0
Total Unique Incidents: 1

- Group disparate devices
- Monitor via dedicated dashboards
- Report, alert and monitor critical services

Dashboards

- Multiple dashboard types
  - Widget
  - Device Summary
  - Business Service
  - Identity & Location
  - Interface Usage
  - PCI
- Dashboard slideshow
- Customizable data visualization
- Multi dashboard support
- RBAC
- Shared dashboards



Permitted Outbound Ports By Bytes
Last 1 hour@11:46

IP Protocol,Destination TCP / UDP Port	AVG(Total Bytes)	Trend
17 (UDP),8888	30.61 KB	
17 (UDP),123 (NTP)	17.66 KB	
6 (TCP),443 (HTTPS)	1.87 KB	
17 (UDP),53 (DOMA...	1.31 KB	
6 (TCP),80 (HTTP)	606.43 B	
6 (TCP),5587	131 B	
6 (TCP),3186	129 B	
6 (TCP),6100	129 B	

Permitted Inbound Ports By Bytes
Last 1 hour@11:46

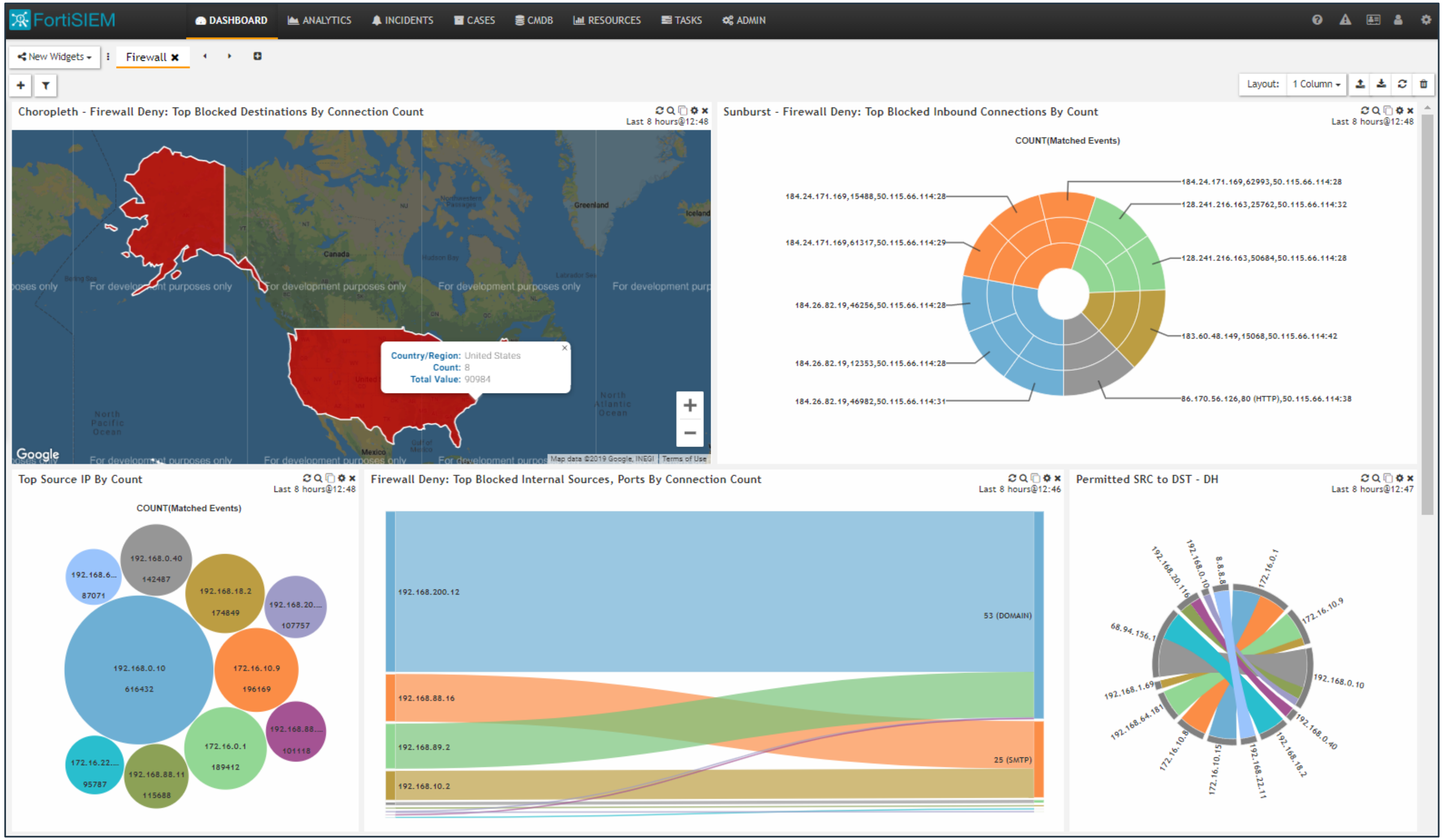
IP Protocol,Destination TCP / UDP Port	AVG(Total Bytes)	Trend
6 (TCP),45270	219.21 KB	
6 (TCP),45119	126.28 KB	
6 (TCP),45115	124.92 KB	
6 (TCP),45174	39.21 KB	
6 (TCP),16389	32.47 KB	
6 (TCP),16403	32.47 KB	
6 (TCP),16376	29.72 KB	
17 (UDP),4500 (IPS...	19.02 KB	

Denied Internal Sources By Connections
Last 1 hour@11:46

Firewall Deny: Top Countries By Inbound Denies
Last 1 hour@11:48

Source Country	COUNT(Matched Events)
China	43
United States	42
Hong Kong	12
Vietnam	4
Seychelles	3
Chile	2
Russian Federation	2
Spain	1

Dashboard Visualizations

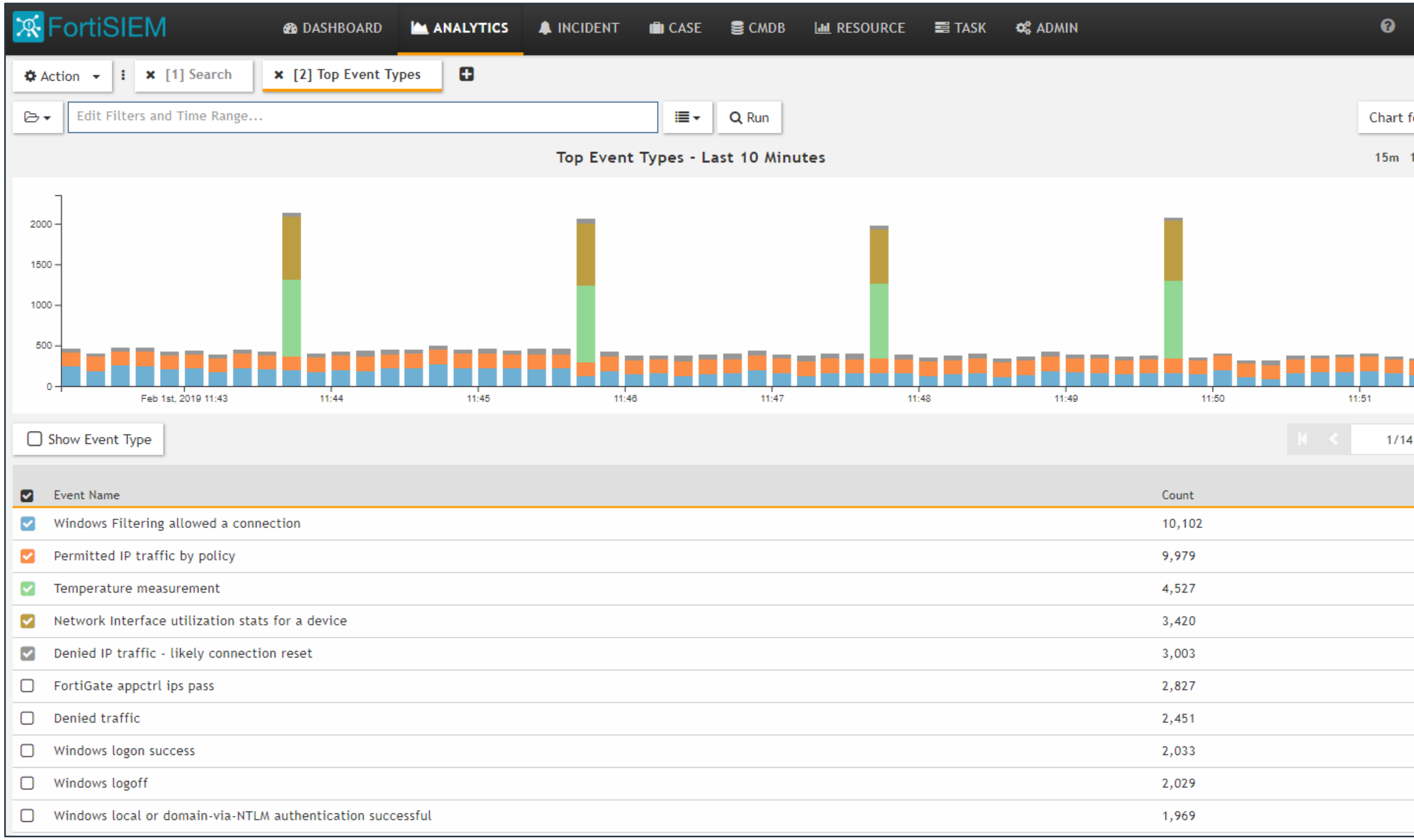


Wide range of data visualizations, including:

- Bar and line chart
- Table
- Sankey and chord
- Choropleth
- Starburst
- Bubble
- Donut
- Heat map
- Pivot table
- … and more!

FortiSIEM Analytics

- Analytics
  - Real time
  - Historical
- 2000+ prebuilt reports
- 600+ inbuilt rules
- Custom rules and reports
- Easy to use GUI
  - Multi tab
  - Easy to use query builder



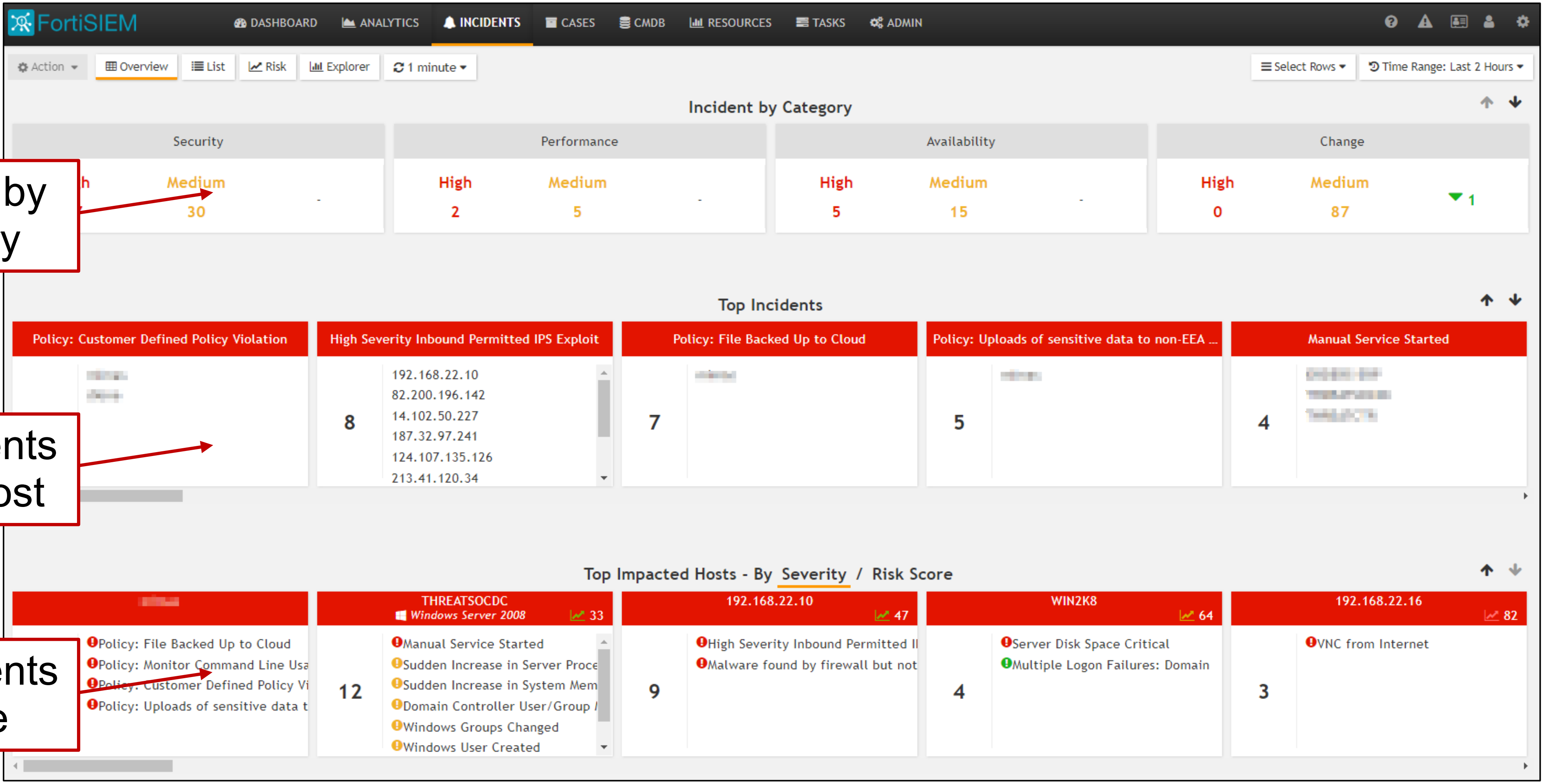
Top Event Types - Last 10 Minutes

□ Show Event Type

☑	Event Name	Count
☑	Windows Filtering allowed a connection	10,102
☑	Permitted IP traffic by policy	9,979
☑	Temperature measurement	4,527
☑	Network Interface utilization stats for a device	3,420
☑	Denied IP traffic - likely connection reset	3,003
□	FortiGate appctrl ips pass	2,827
□	Denied traffic	2,451
□	Windows logon success	2,033
□	Windows logoff	2,029
□	Windows local or domain-via-NTLM authentication successful	1,969

Incident Summary Dashboard

At-a-Glance View of Triggered Incidents



Incident by Category

Security			Performance			Availability			Change		
h	Medium		High	Medium		High	Medium		High	Medium	
	30	-	2	5	-	5	15	-	0	87	▼ 1

Top Incidents

Policy: Customer Defined Policy Violation		High Severity Inbound Permitted IPS Exploit		Policy: File Backed Up to Cloud		Policy: Uploads of sensitive data to non-EEA ...		Manual Service Started	
	[redacted] [redacted]	8	192.168.22.10 82.200.196.142 14.102.50.227 187.32.97.241 124.107.135.126 213.41.120.34	7	[redacted]	5	[redacted]	4	[redacted] [redacted] [redacted]

Top Impacted Hosts - By Severity / Risk Score

[redacted]		THREATSOCDC Windows Server 2008 33		192.168.22.10 47		WIN2K8 64		192.168.22.16 82	
	Policy: File Backed Up to Cloud Policy: Monitor Command Line Usa Policy: Customer Defined Policy Vi Policy: Uploads of sensitive data t	12	Manual Service Started Sudden Increase in Server Proce Sudden Increase in System Mem Domain Controller User/Group / Windows Groups Changed Windows User Created	9	High Severity Inbound Permitted II Malware found by firewall but not	4	Server Disk Space Critical Multiple Logon Failures: Domain	3	VNC from Internet

Incidents by Category

Incidents by Host

Top Incidents by Type

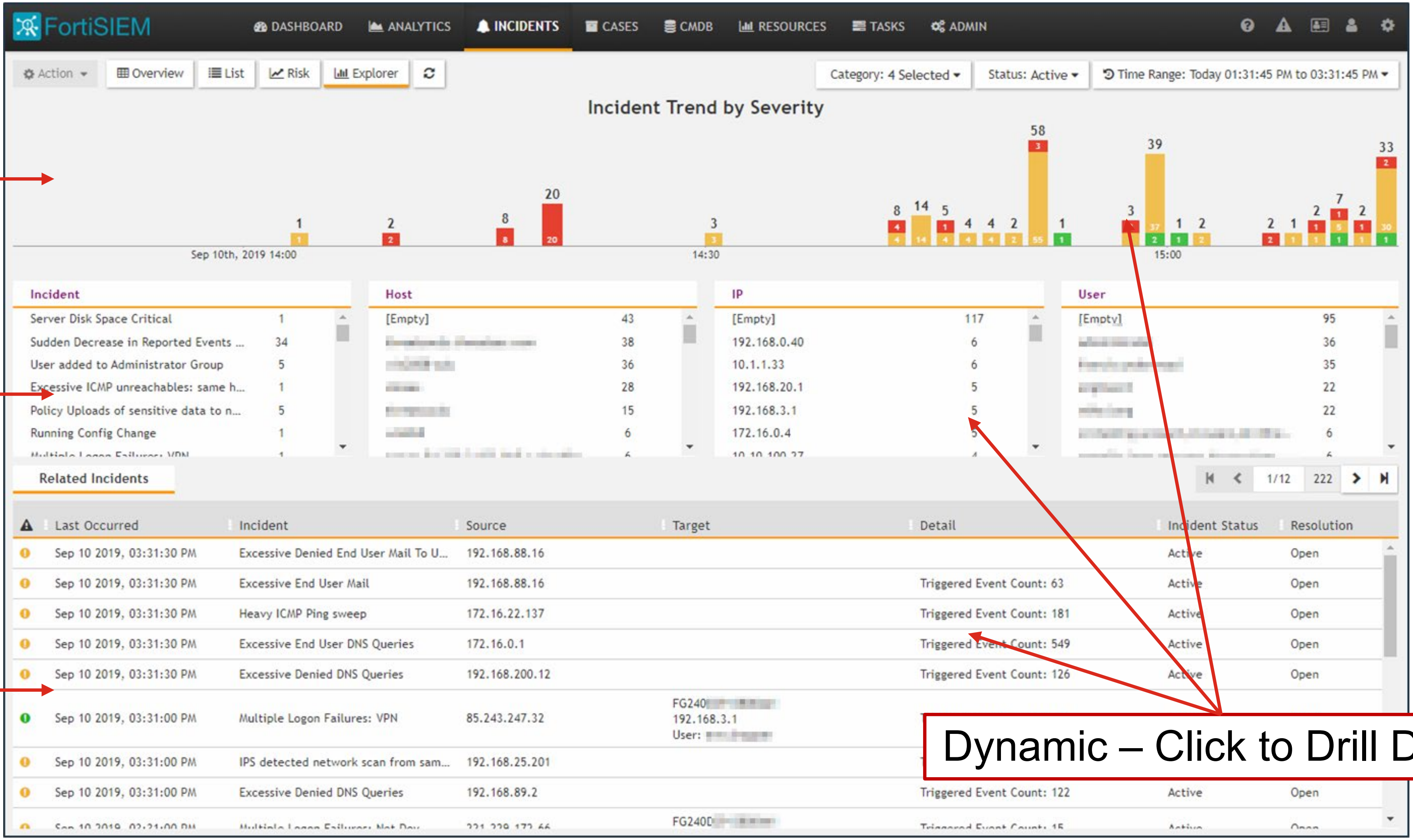
Incident Explorer

Dynamically Explore FortiSIEM Incidents

Incident Trend Graph

Incident, Host, IP and User Panels

Incident Table



Category: 4 Selected · Status: Active · Time Range: Today 01:31:45 PM to 03:31:45 PM

Incident Trend by Severity

Incident	
Server Disk Space Critical	1
Sudden Decrease in Reported Events ...	34
User added to Administrator Group	5
Excessive ICMP unreachables: same h...	1
Policy Uploads of sensitive data to n...	5
Running Config Change	1
Multiple Logon Failures: VPN	1

Host	
[Empty]	43
[redacted]	38
[redacted]	36
[redacted]	28
[redacted]	15
[redacted]	6
[redacted]	6

IP	
[Empty]	117
192.168.0.40	6
10.1.1.33	6
192.168.20.1	5
192.168.3.1	5
172.16.0.4	5
10.10.100.27	4

User	
[Empty]	95
[redacted]	36
[redacted]	35
[redacted]	22
[redacted]	22
[redacted]	6
[redacted]	6

Related Incidents

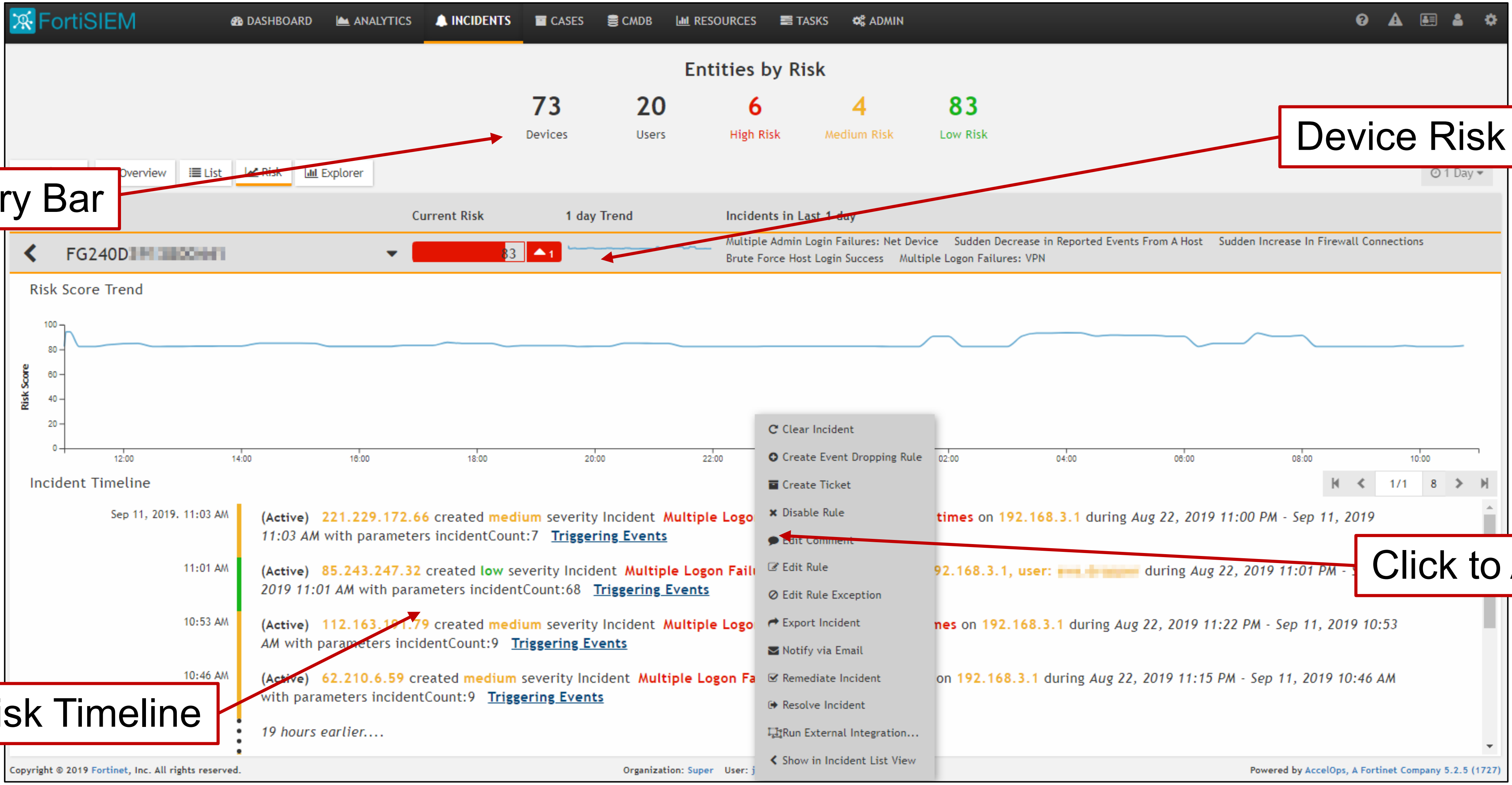
1/12 222

▲	Last Occurred	Incident	Source	Target	Detail	Incident Status	Resolution
●	Sep 10 2019, 03:31:30 PM	Excessive Denied End User Mail To U...	192.168.88.16			Active	Open
●	Sep 10 2019, 03:31:30 PM	Excessive End User Mail	192.168.88.16		Triggered Event Count: 63	Active	Open
●	Sep 10 2019, 03:31:30 PM	Heavy ICMP Ping sweep	172.16.22.137		Triggered Event Count: 181	Active	Open
●	Sep 10 2019, 03:31:30 PM	Excessive End User DNS Queries	172.16.0.1		Triggered Event Count: 549	Active	Open
●	Sep 10 2019, 03:31:30 PM	Excessive Denied DNS Queries	192.168.200.12		Triggered Event Count: 126	Active	Open
●	Sep 10 2019, 03:31:00 PM	Multiple Logon Failures: VPN	85.243.247.32	FG240[redacted] 192.168.3.1 User: [redacted]			
●	Sep 10 2019, 03:31:00 PM	IPS detected network scan from sam...	192.168.25.201				
●	Sep 10 2019, 03:31:00 PM	Excessive Denied DNS Queries	192.168.89.2		Triggered Event Count: 122	Active	Open
●	Sep 10 2019, 03:31:00 PM	Multiple Logon Failures: Net Dev...	221.229.172.66	FG240D[redacted]	Triggered Event Count: 15	Active	Open

Dynamic – Click to Drill Down

Risk Dashboard

User and Entity Risk View



Entities by Risk

73	20	6	4	83
Devices	Users	High Risk	Medium Risk	Low Risk

	Current Risk	1 day Trend	Incidents in Last 1 day
FG240D[redacted]	83 ▲1		Multiple Admin Login Failures: Net Device Sudden Decrease in Reported Events From A Host Sudden Increase In Firewall Connections Brute Force Host Login Success Multiple Logon Failures: VPN

Risk Score Trend

Incident Timeline

Sep 11, 2019. 11:03 AM (Active) 221.229.172.66 created medium severity Incident Multiple Logo … times on 192.168.3.1 during *Aug 22, 2019 11:00 PM - Sep 11, 2019 11:03 AM* with parameters incidentCount:7 Triggering Events

11:01 AM (Active) 85.243.247.32 created low severity Incident Multiple Logon Failu … 92.168.3.1, user: [redacted] during *Aug 22, 2019 11:01 PM - … 2019 11:01 AM* with parameters incidentCount:68 Triggering Events

10:53 AM (Active) 112.163.1?1.79 created medium severity Incident Multiple Logo … nes on 192.168.3.1 during *Aug 22, 2019 11:22 PM - Sep 11, 2019 10:53 AM* with parameters incidentCount:9 Triggering Events

10:46 AM (Active) 62.210.6.59 created medium severity Incident Multiple Logon Fa … on 192.168.3.1 during *Aug 22, 2019 11:15 PM - Sep 11, 2019 10:46 AM* with parameters incidentCount:9 Triggering Events

19 hours earlier....

Copyright © 2019 Fortinet, Inc. All rights reserved.   Organization: Super   User: j   Powered by AccelOps, A Fortinet Company 5.2.5 (1727)

Summary Bar

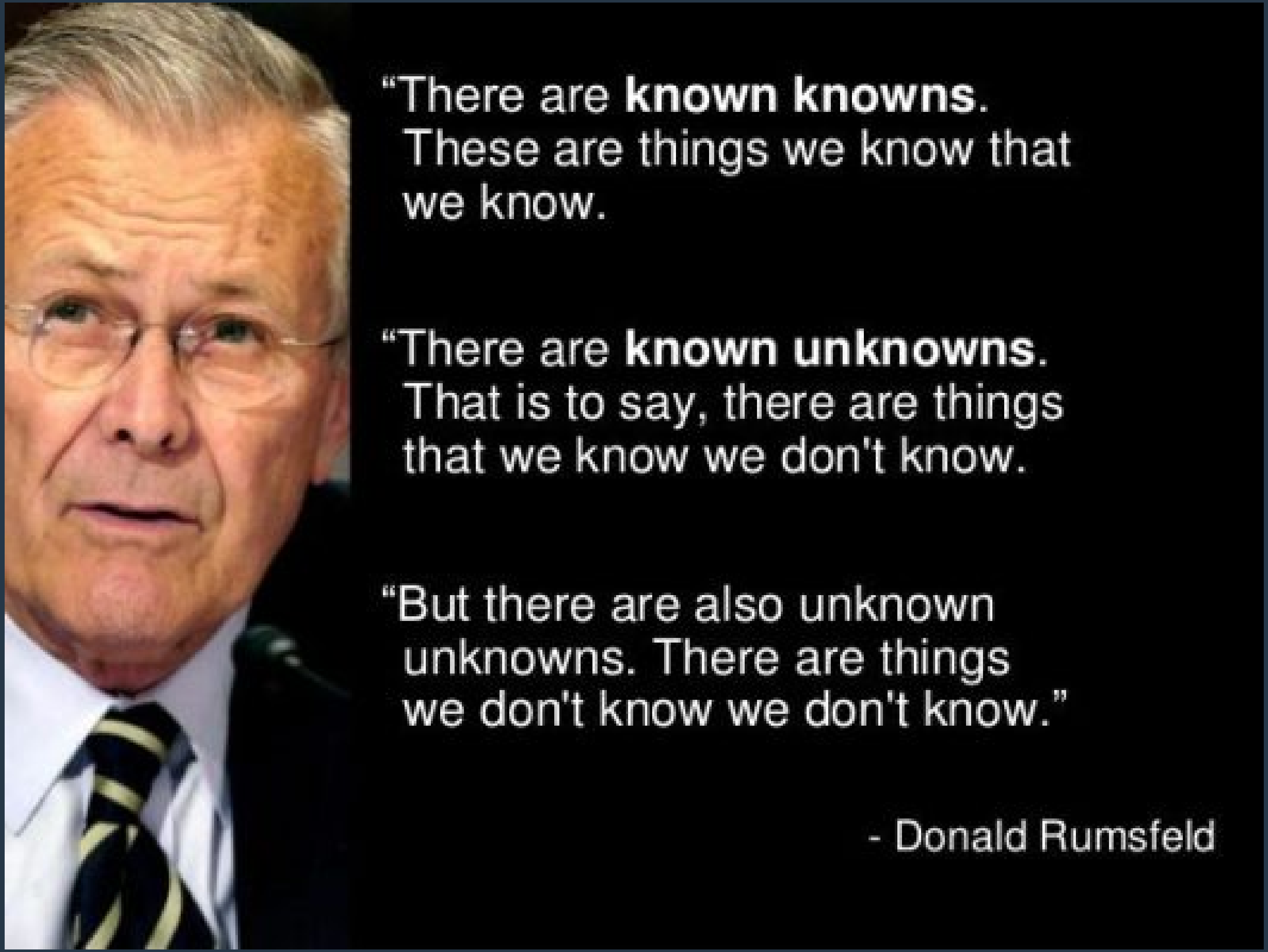
Device Risk Score

Click to Action

Device Risk Timeline

User Entity Behavior Analytics

FortiSIEM & FortiInsight – Machine Learning to detect anomalous threats



"There are **known knowns**.
These are things we know that
we know.

"There are **known unknowns**.
That is to say, there are things
that we know we don't know.

"But there are also unknown
unknowns. There are things
we don't know we don't know."

- Donald Rumsfeld

FortiInsight Machine Learning

For Anomalous Behavior Detection

Machine Learning

- The FortiInsight Machine Learning capability allows users to detect ‘unknown unknowns’
  - For example: Leavers – Bob is about to leave his job, and his behavior has changed. This is hard to detect with rules alone

Profile Building

- Builds profiles of normal behavior so that it can detect abnormal behavior

Easy Setup

- Easy to set up and starts learning user behavior without configuration

User Tracking

- Uses UBA to track users and detect threats, by looking at patterns of human behavior

FortiInsight

Feature Set

Endpoint Agent

Non-intrusive, lightweight endpoint agent

Push-Architecture

Rapid deployment and instant protection

Central Analytics

No need to push policies to endpoints

Alerting

Rules
map policies and compliance into alert

Machine Learning
detect anomalous threats

Network Monitoring

See where your data is going and where it's coming from, even when it's off your corporate network

Threat Hunting

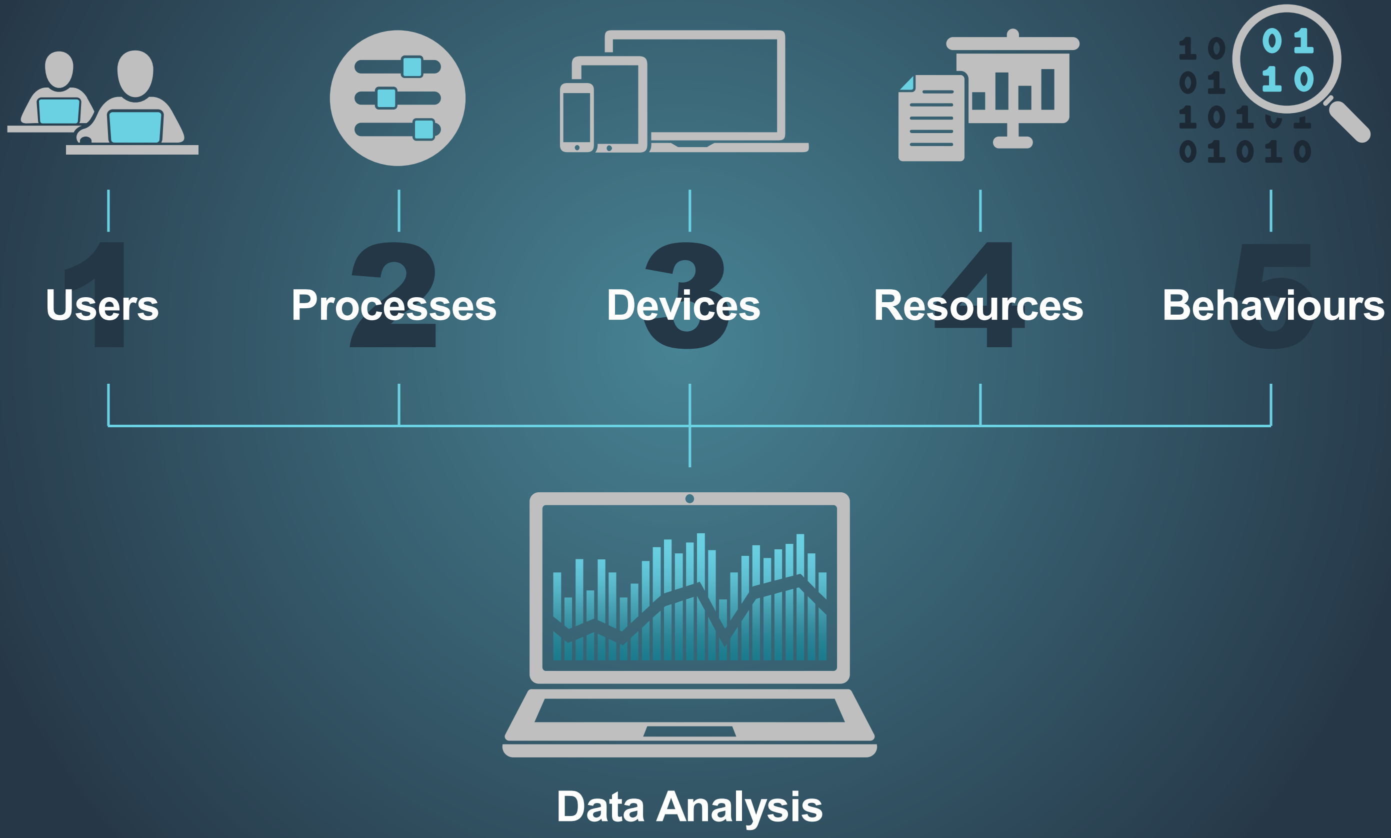
7 day record of all activities

Unique 5-Factor Telemetry Model

Engineered to detect insider threats

FortiInsight

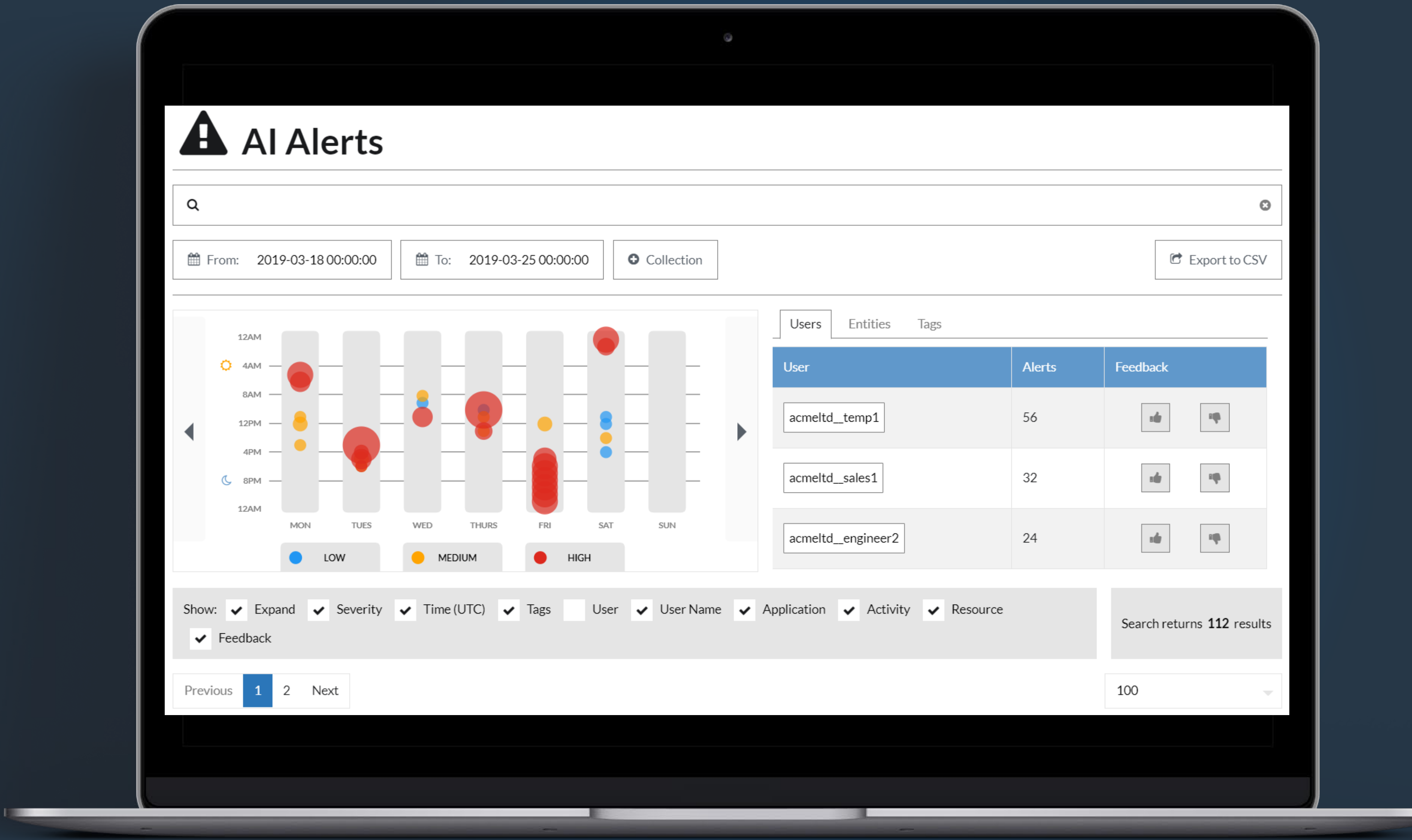
Wherever a machine is located and whatever network the machine is connected to, **FortiInsight** captures the key information from 5 anchors to deliver insights built upon, the key metadata and behavior analysis around:



Machine Learning

Alerts

- Use Visualization and summary table to find what’s important to you
- Users, Entities, Tags for scoping
- Feedback mechanism
- Pivot on Threat Hunting for context



AI Alerts

From: 2019-03-18 00:00:00 | To: 2019-03-25 00:00:00 | Collection | Export to CSV

Users | Entities | Tags

User	Alerts	Feedback
acmeltd__temp1	56	👍 👎
acmeltd__sales1	32	👍 👎
acmeltd__engineer2	24	👍 👎

Show: ☑ Expand ☑ Severity ☑ Time (UTC) ☑ Tags □ User ☑ User Name ☑ Application ☑ Activity ☑ Resource ☑ Feedback

Search returns 112 results

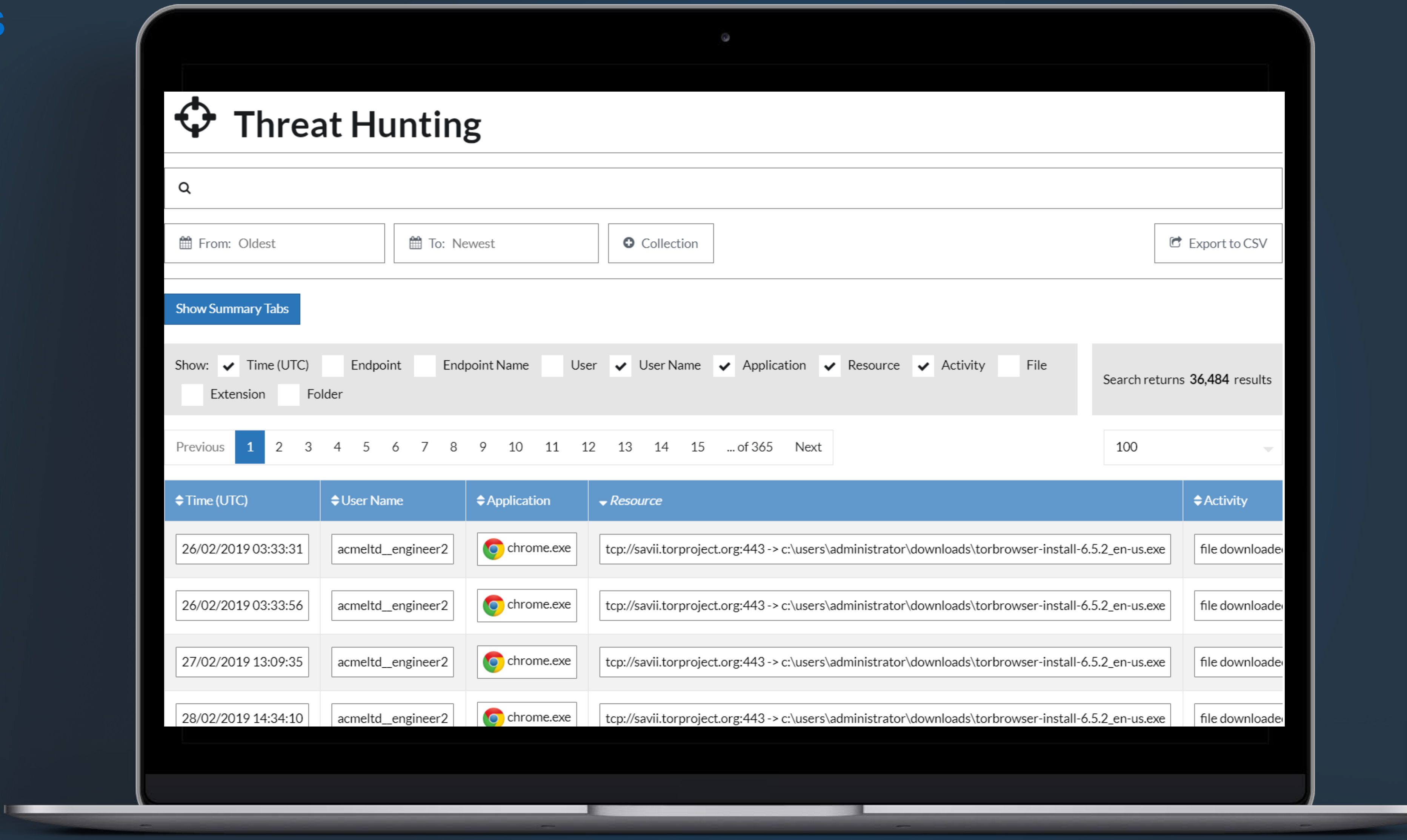
Previous 1 2 Next

100

Threat Hunting

Your view of events

- Interactive search of the event record
- 7 days of full history
- Summary Tabs – use to refine search
- Event List – sortable and selectable columns



Threat Hunting

Show: ☑ Time (UTC) □ Endpoint □ Endpoint Name □ User ☑ User Name ☑ Application ☑ Resource ☑ Activity □ File □ Extension □ Folder

Search returns 36,484 results

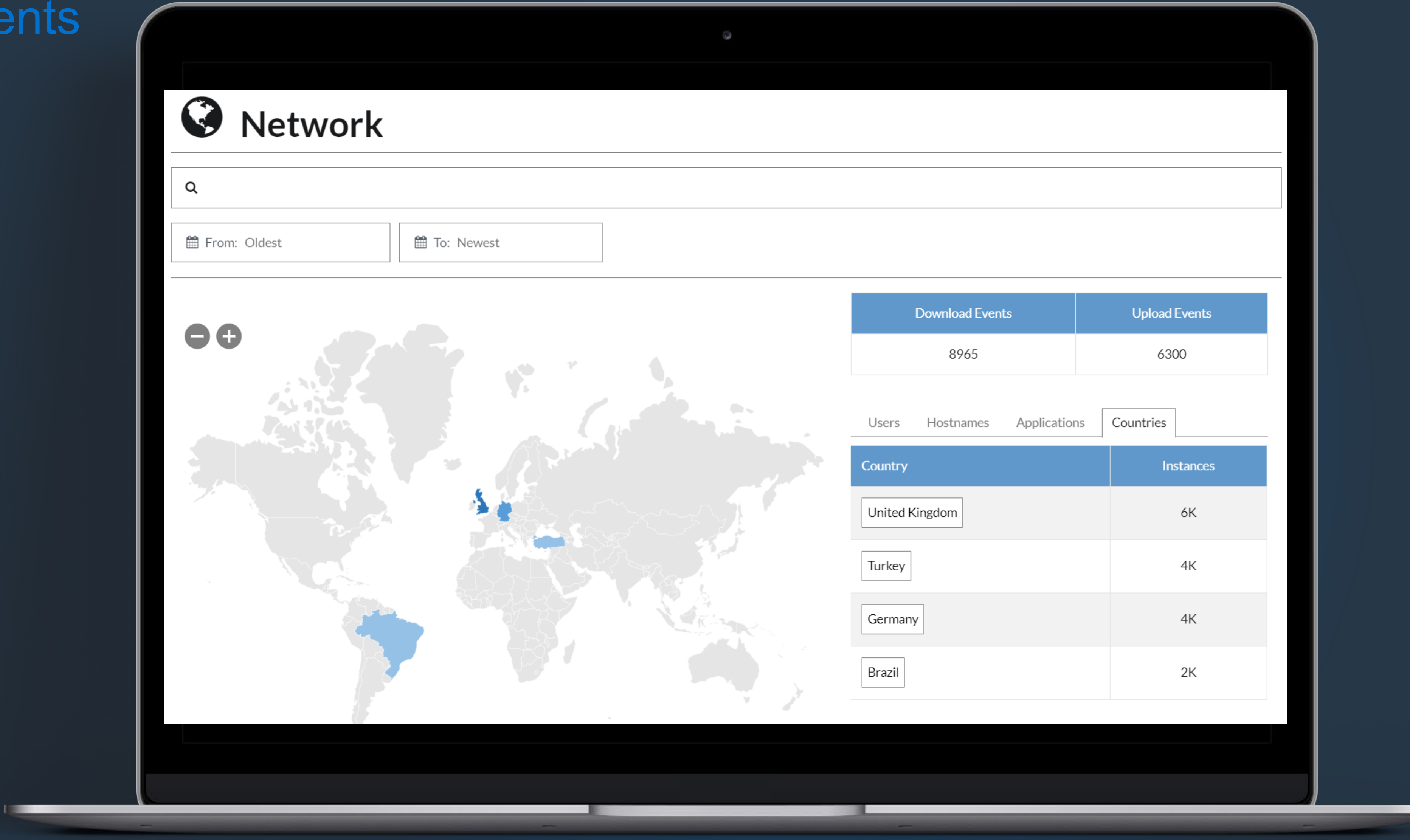
Previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ... of 365 Next
100

Time (UTC)	User Name	Application	Resource	Activity
26/02/2019 03:33:31	acmeltd_engineer2	chrome.exe	tcp://savii.torproject.org:443 -> c:\users\administrator\downloads\torbrowser-install-6.5.2_en-us.exe	file downloade
26/02/2019 03:33:56	acmeltd_engineer2	chrome.exe	tcp://savii.torproject.org:443 -> c:\users\administrator\downloads\torbrowser-install-6.5.2_en-us.exe	file downloade
27/02/2019 13:09:35	acmeltd_engineer2	chrome.exe	tcp://savii.torproject.org:443 -> c:\users\administrator\downloads\torbrowser-install-6.5.2_en-us.exe	file downloade
28/02/2019 14:34:10	acmeltd_engineer2	chrome.exe	tcp://savii.torproject.org:443 -> c:\users\administrator\downloads\torbrowser-install-6.5.2_en-us.exe	file downloade

North/South Data Movement

Search network events

- Map – at a glance data sources\destinations
- View data coming into the organization and leaving it
- Activity search filters on file downloaded\uploaded
- Top users, hostnames, applications, & countries for easy filtering
- Low level event data



Network

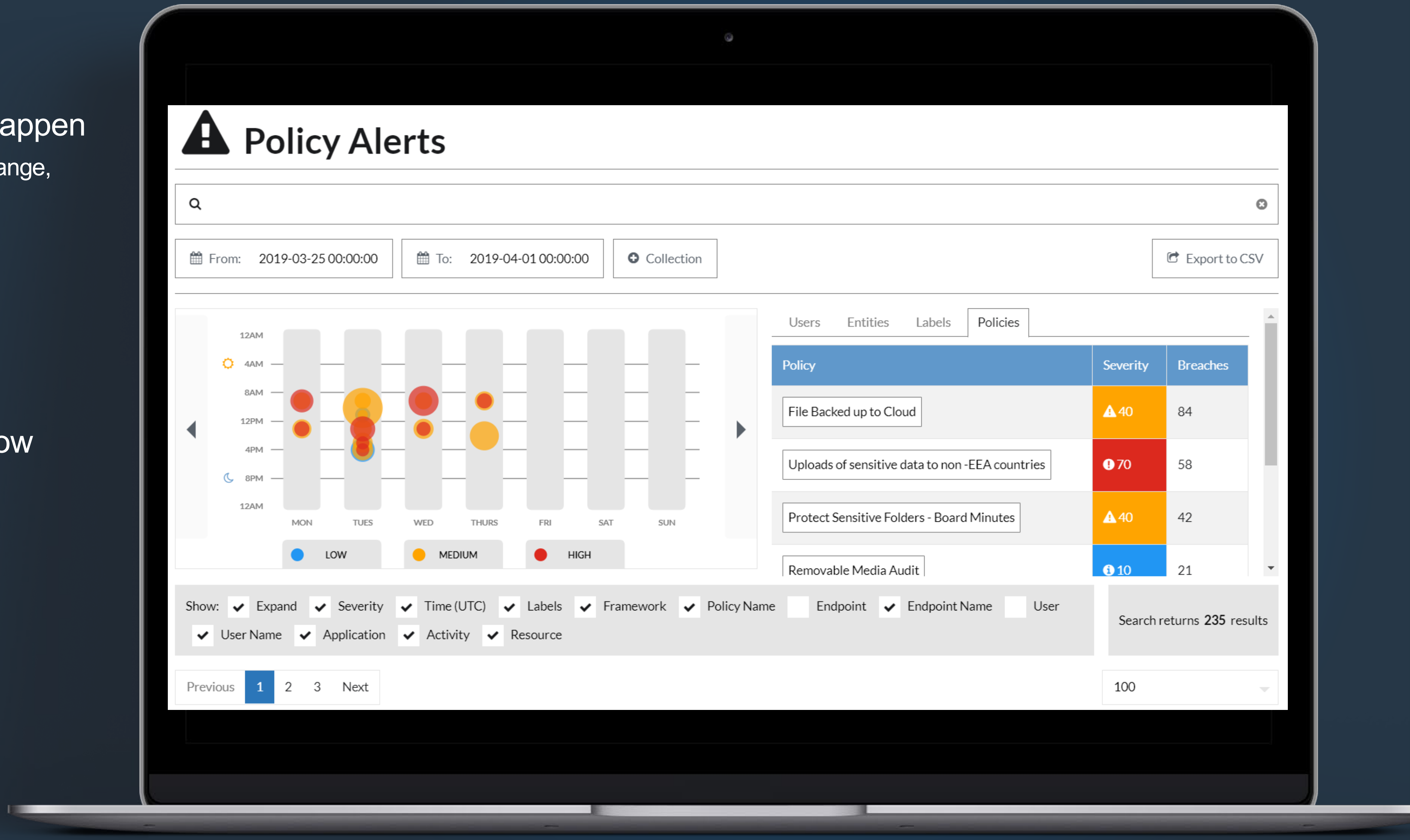
Download Events	Upload Events
8965	6300

Country	Instances
United Kingdom	6K
Turkey	4K
Germany	4K
Brazil	2K

Policies

Policy Alerts

- Live view of alerts, as they happen
  - Selectable timeframe – date & time range, or selectable week view
- Click on alerts to drill down for event details
  - Packed events
- Filter alerts using search
- Use Summary Table to narrow your search
  - User
  - Entities
  - Labels
  - Policies
- Pivot to Threat Hunting
  - Gain context
- Export data as csv



Policy Alerts

From: 2019-03-25 00:00:00 To: 2019-04-01 00:00:00 Collection Export to CSV

Policy	Severity	Breaches
File Backed up to Cloud	40	84
Uploads of sensitive data to non -EEA countries	70	58
Protect Sensitive Folders - Board Minutes	40	42
Removable Media Audit	10	21

Show: ☑ Expand ☑ Severity ☑ Time (UTC) ☑ Labels ☑ Framework ☑ Policy Name □ Endpoint ☑ Endpoint Name □ User ☑ User Name ☑ Application ☑ Activity ☑ Resource

Search returns 235 results

Previous 1 2 3 Next

100

FortiSIEM - ADC integration

Challenges

- Need to add servers as apps grow
- Ensure application availability
- Maximize server utilization
- Need to inspect encrypted traffic

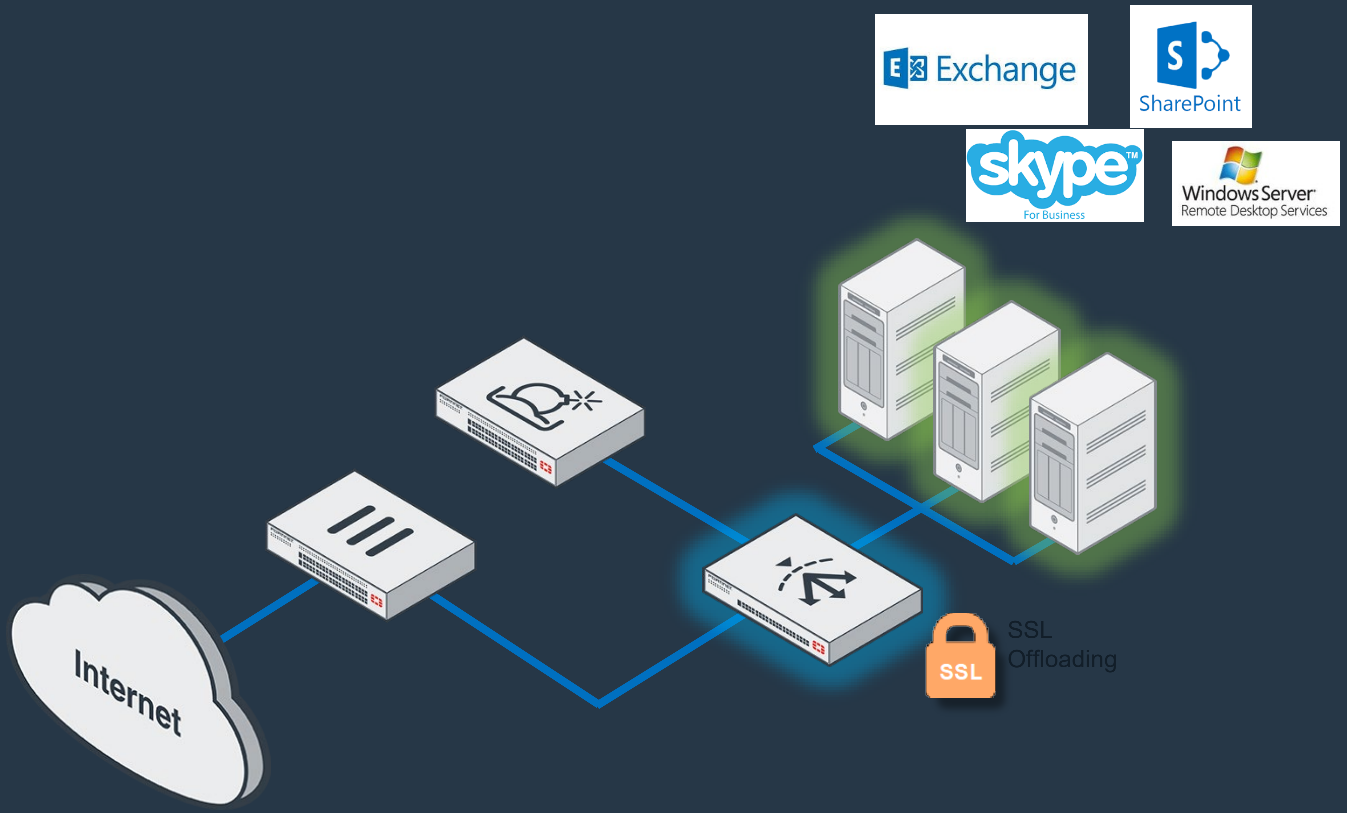
Solution

FortiADC Application Delivery Controller

- Server Load Balancing
- Health checking
- Persistence
  SSL Offloading

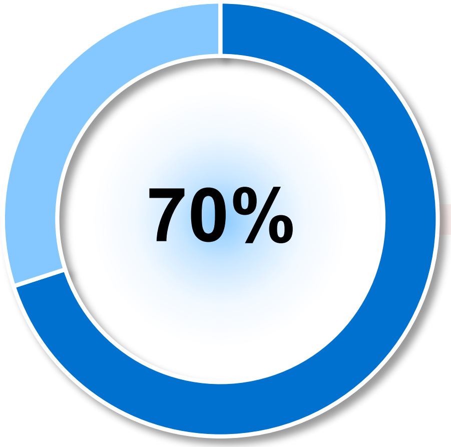
Advantages

- Add multiple servers to meet needs
- Users see increased response and uptime
- Up to 25% increase in per server capacity

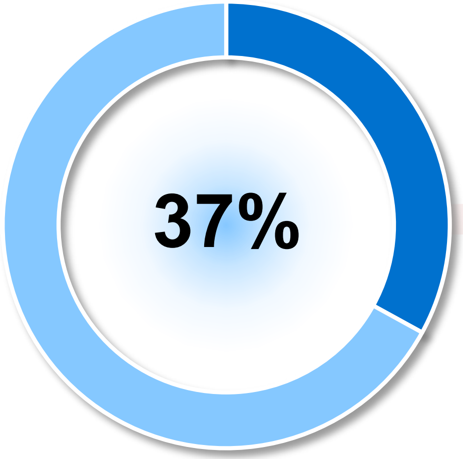


FortiSIEM - SD-WAN monitoring

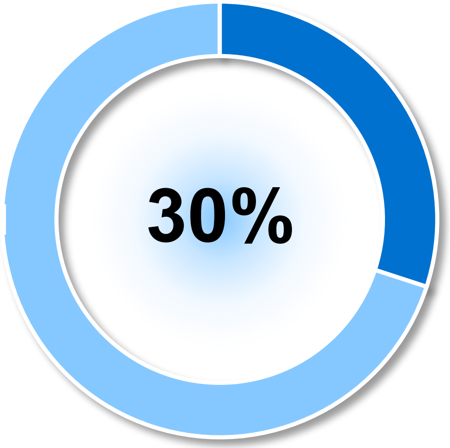
Office 365 salesforce Skype for Business slack



Percentage of application
have already moved to cloud

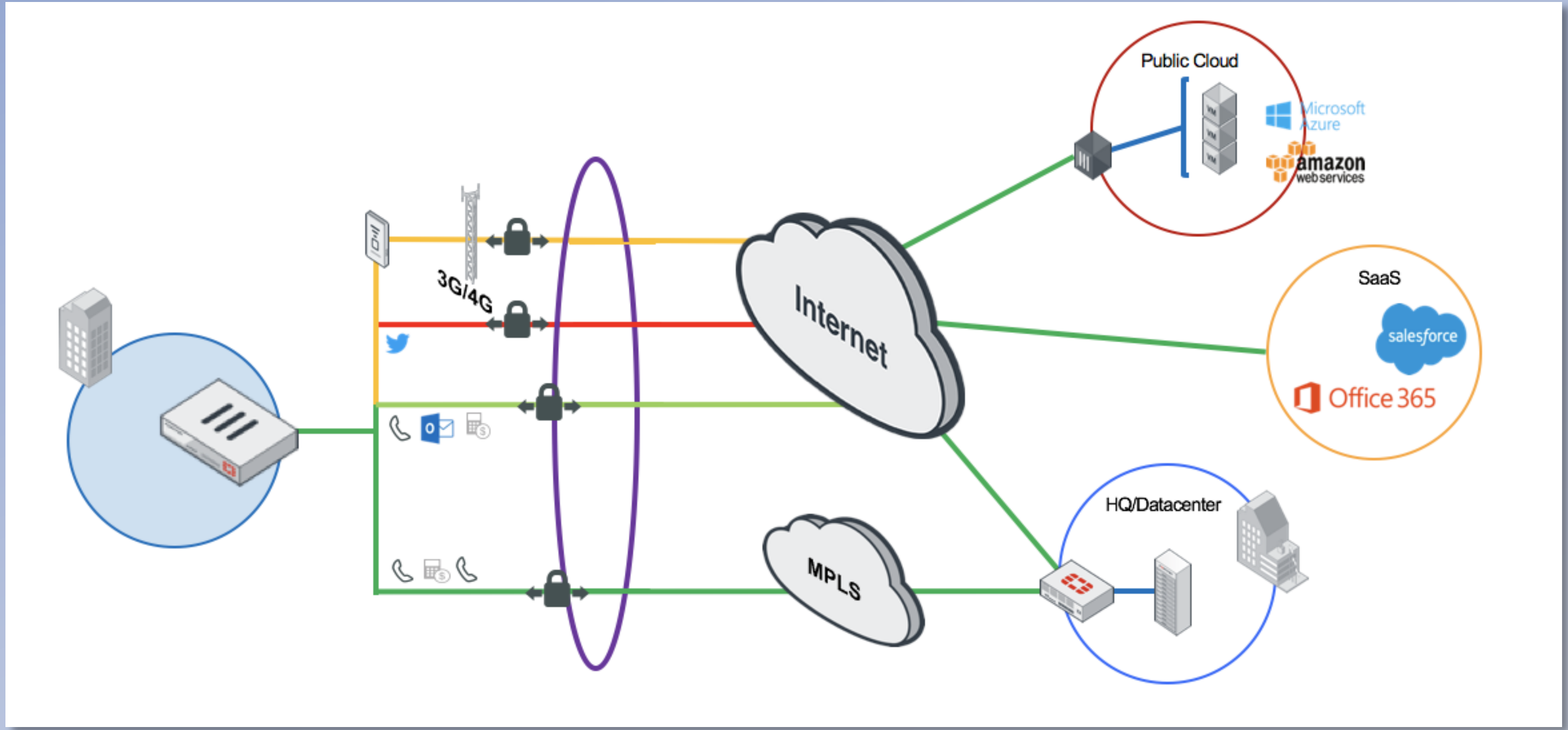


Considered SaaS Easier to Deploy
vs On Premise Applications



Lower user acceptance
for SaaS applications

Dynamic WAN Path Controller and Measurement



Application Steering

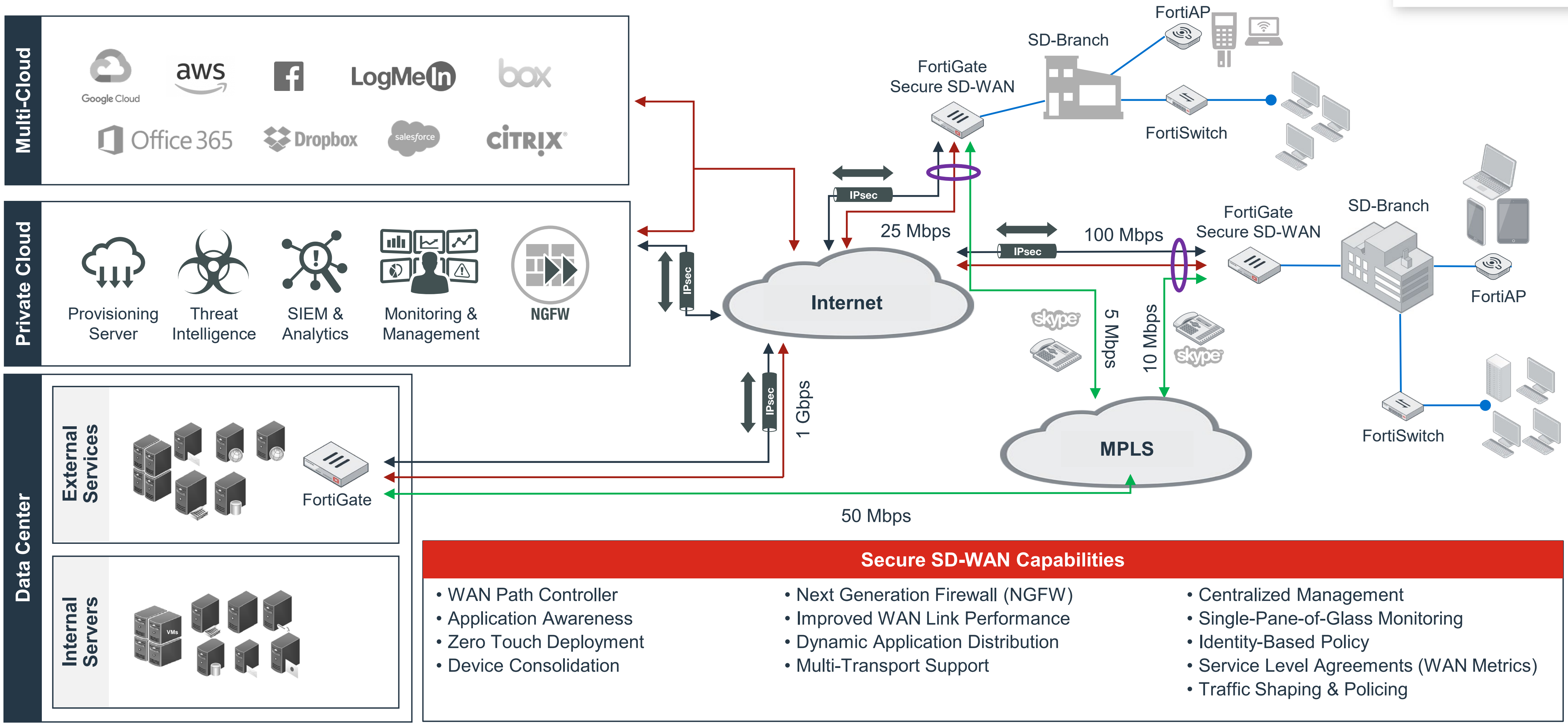
WAN Path Measurements

Dynamic Application Fail-over

Simplify with Secure SD-Branch

FORTINET SECURITY FABRIC

MPLS 🟩
IPSec Tunnel ⬛
Broadband 🟥
LAN 🟦



Secure SD-WAN Capabilities

- WAN Path Controller
- Application Awareness
- Zero Touch Deployment
- Device Consolidation

- Next Generation Firewall (NGFW)
- Improved WAN Link Performance
- Dynamic Application Distribution
- Multi-Transport Support

- Centralized Management
- Single-Pane-of-Glass Monitoring
- Identity-Based Policy
- Service Level Agreements (WAN Metrics)
- Traffic Shaping & Policing

FORTINET®