



Simplify Security Operations

FMG / FAZ / FSM What's New

Q3 2020

Kevin Yang

Technical Consultant Taiwan

BMW i Motorsport
Official Partner



Cybersecurity Market Trends

A Cybersecurity Platform that Enables Digital Innovation

Zero-Trust Network Access



Accelerated OT/IoT

- Operation Technology
- Millions of IoT Devices
- Mobility

Security-Driven Networking



Accelerated Converged Approach

- SD-WAN (ASIC)
- NGFW (ASIC)
- SASE (Cloud)
- ZTNA (Cloud)

Dynamic Cloud Security



Accelerated Cloud Adoption

- Security **FOR** the Cloud
- Security **FROM** the Cloud
- Work From Home (WFH)

AI-Driven Security Operations

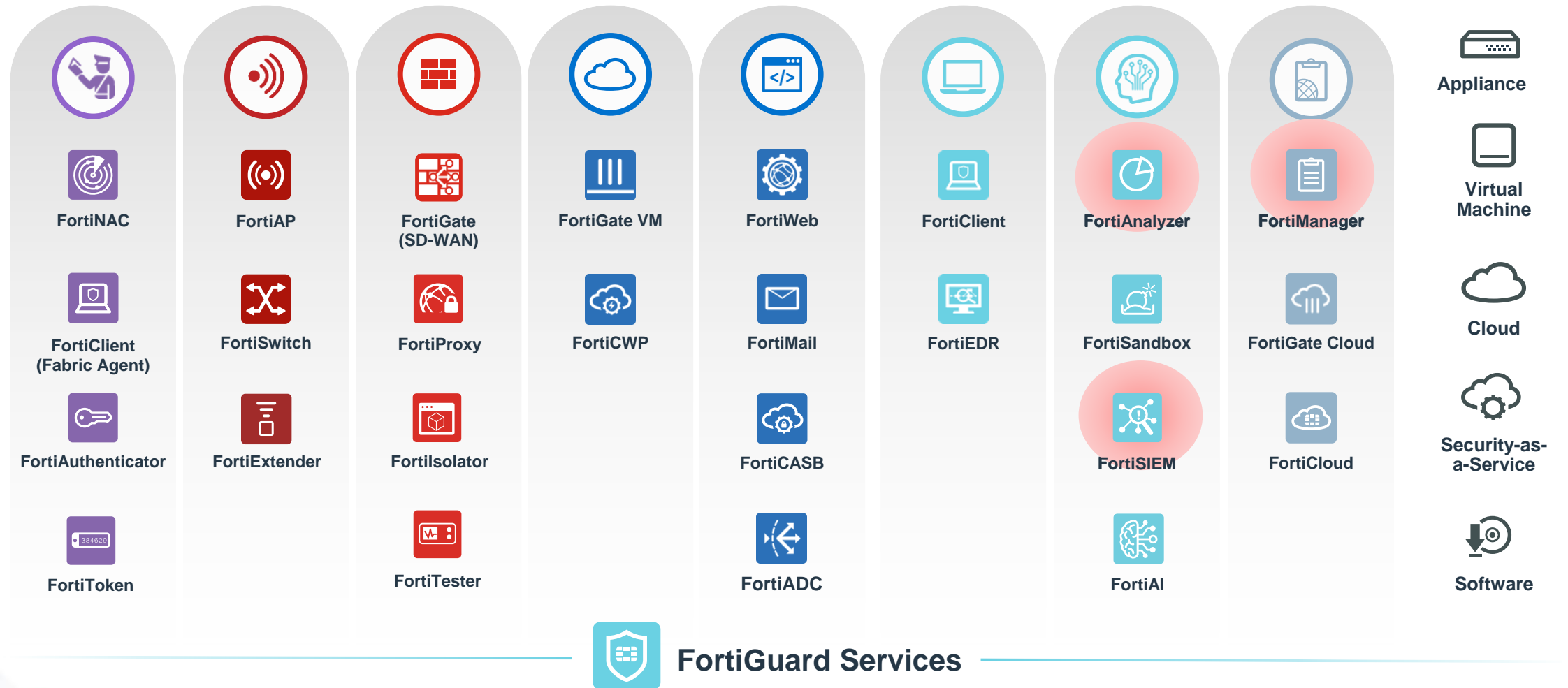


Accelerated Detection / Response

- Too Many Point Products
- Not Enough Skilled people
- Hard to implement Automation

Broadest End-to-End Cybersecurity Platform

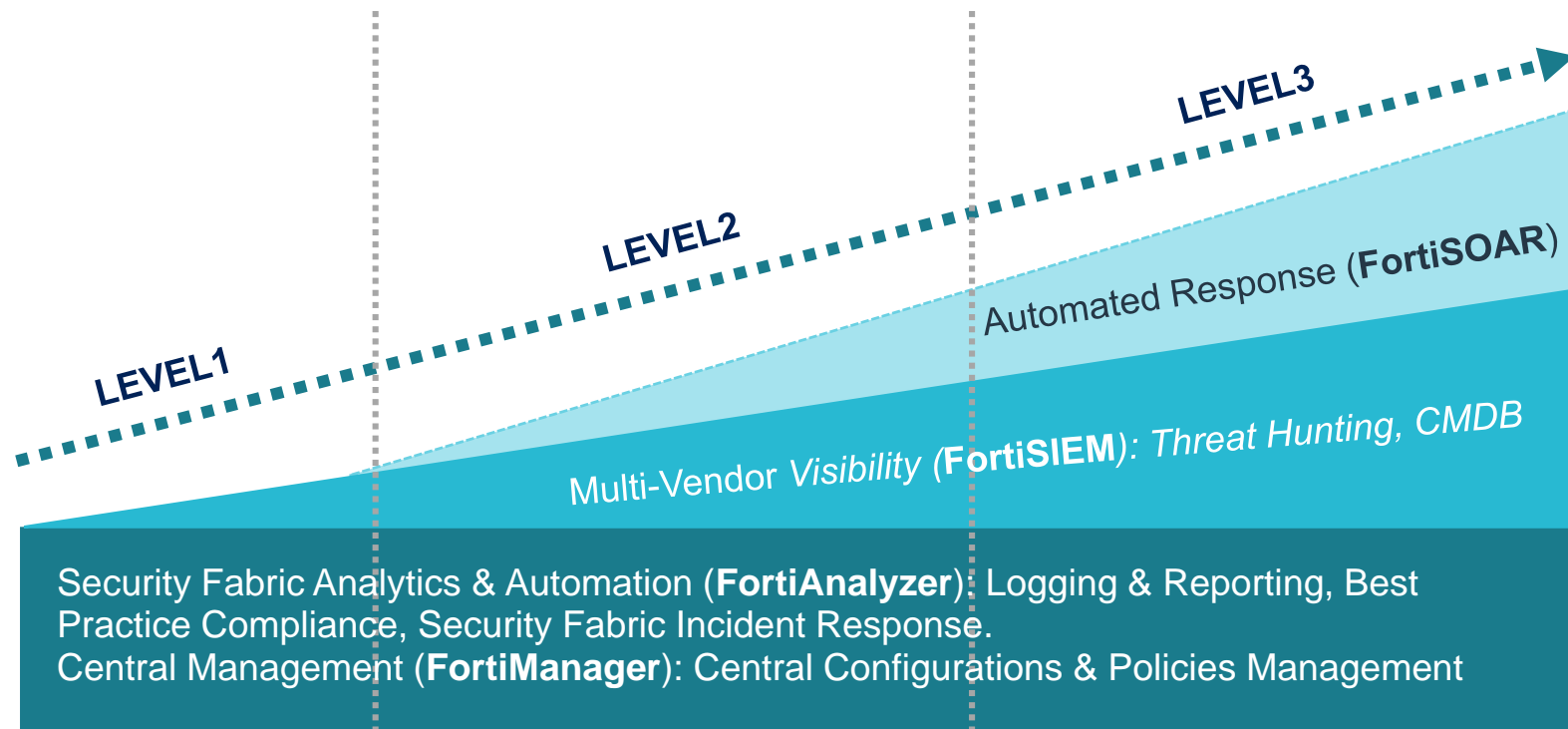
Different consumption models available



FortiGuard Services

Simplify Security Operations

Choose an offering aligned to your SOC maturity



The **SOC Maturity Framework** identifies which SOC capabilities are aligned to an organization based on their SOC maturity. FortiManager, FortiAnalyzer, FortiSIEM & FortiSOAR can be mapped to these capabilities.

FortiSOAR enables full orchestration and automation across the Security Fabric and multivendor environments.

FortiSIEM brings multi-vendor visibility across your network. Higher levels of correlation and customization can be integrated with the Security Fabric.

FortiAnalyzer provides logging, reporting, analytics and automation for all "on fabric" devices and endpoints.
FortiManager provides central configurations and policies management

Security Operations Center (SOC) Maturity Framework

People, Process, Capabilities

	SOC Maturity LEVEL1	SOC Maturity LEVEL2	SOC Maturity LEVEL3
People	Medium business with one Team - IT & Security (<5 IT-security staff)	Med-Large business with dedicate security team (3-5 dedicated <u>security</u> staff)	Large enterprise with experienced SOC analysts / SOC Team (5+ Dedicated SOC Staff)
Process	Best effort incident response	Basic incident response plan	Advanced SOC processes and playbooks
Capabilities	<ul style="list-style-type: none">• Logging & Reporting• Automated Detection & Response• Configuration Management	Level 1 plus: <ul style="list-style-type: none">•Multi-Vendor Incident Detection & Response	Level 2 plus: <ul style="list-style-type: none">•Alert Management•Unified Orchestration Automation & Response

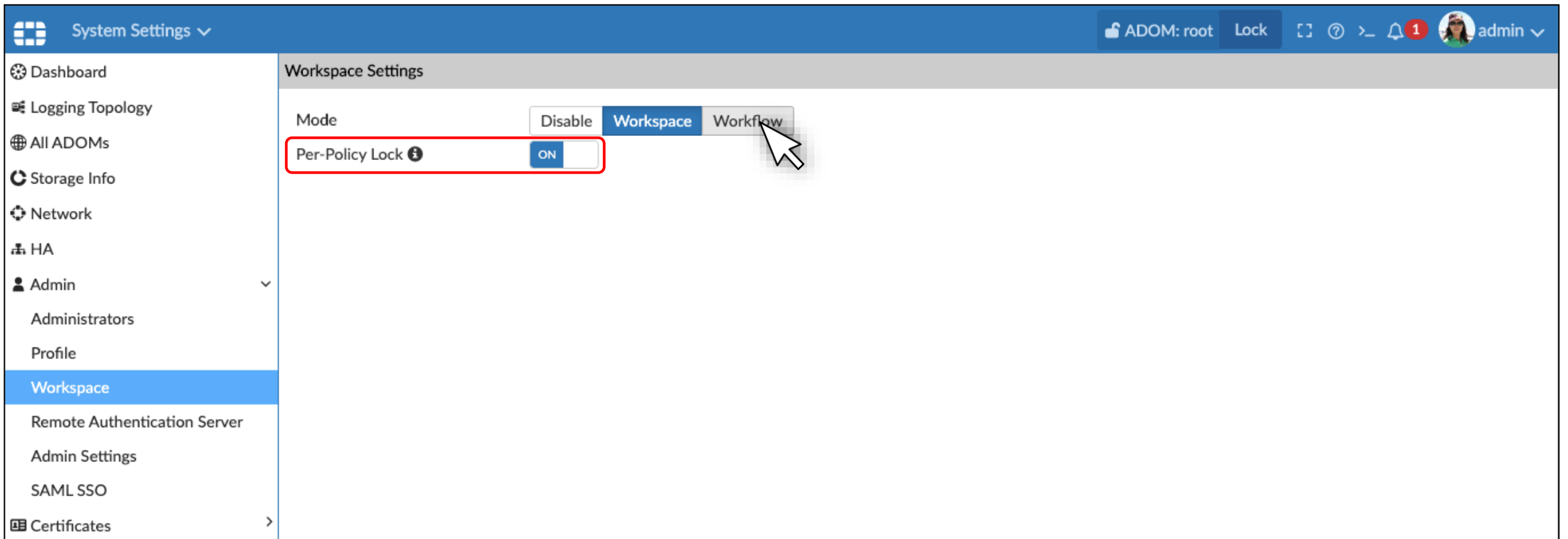
FortiManager 6.4 What's New

FortiManager 6.4 What's New

- Workspace Enhancement (per-policy lock / policy package lock)
- ADOM Selection & Revision Enhancement
- Normalized Interfaces
- Zero Touch Provisioning (ZTP) Enhancement
- Management Extensions - SD-WAN Orchestrator

Workspace Enhancement – Per-Policy Lock Support

From ADOM Lock To Per-Policy Lock Support



The screenshot displays the Fortinet System Settings interface. The top navigation bar includes "System Settings" with a dropdown arrow, and user information for "ADOM: root" with a "Lock" button. The left sidebar lists various system settings categories, with "Workspace" currently selected. The main content area is titled "Workspace Settings" and features three tabs: "Disable", "Workspace" (which is active), and "Workflow". Below the tabs, the "Per-Policy Lock" setting is shown with an information icon and a toggle switch set to "ON". A red rectangular box highlights the "Per-Policy Lock" label and its toggle switch. A mouse cursor is positioned over the "Workflow" tab.

Workspace Enhancement – Per-Policy Lock Support

Implicit Lock

The screenshot shows the Fortinet GUI interface for Policy Packages. The 'Save' button is circled in red. A table lists policies under 'Project #1 (1-9 / Total: 9)'. Policy_001 is highlighted with a red lock icon in the first column. A red circle also highlights the source hosts: host_001, host_002, host_003, and host_004. A red arrow points from a female user icon to the lock icon on Policy_001.

#	Name	From	To	Source	Destination	Security Profiles	Schedule	Service	Users	Action
1	Policy_001	LAN	WAN	host_001, host_002, host_003, host_004	host_051	no-inspection	always	ALL		Accept
2	Policy_002	LAN	WAN	host_002	host_052	no-inspection	always	ALL		Accept
3	Policy_003	LAN	WAN	host_003	host_053	no-inspection	always	ALL		Accept



The screenshot shows the Fortinet GUI interface for Policy Packages. A red circle highlights Policy_001, which has a lock icon. A tooltip is displayed over Policy_001, stating: "The Policy was locked by admin at 2020-02-13 13:44:47". A red arrow points from a male user icon to the lock icon on Policy_001.

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile
1	Policy_001	LAN	WAN	host_001	host_051	always	ALL		Accept	no-inspection
2	Policy_002	LAN	WAN	host_002	host_052	always	ALL		Accept	no-inspection
3	Policy_003	LAN	WAN	host_003	host_053	always	ALL		Accept	no-inspection
4	Policy_004	LAN	WAN	host_004	host_054	always	ALL		Accept	no-inspection
5	Policy_005	LAN	WAN	host_005	host_055	always	ALL		Accept	no-inspection
6	Policy_006	LAN	WAN	host_006	host_056	always	ALL		Accept	no-inspection

Workspace Enhancement – Per-Policy Lock Support

New Save All Option To Save All Touched Policy Packages

The screenshot shows the Fortinet Policy Packages management interface. The top navigation bar includes 'Policy & Objects', 'Policy Packages', and 'Object Configurations'. The user is logged in as 'admin'. The main area displays a table of policy packages with columns for #, Name, From, To, Source, Destination, Schedule, and Service. The first row, 'test_001', has a lock icon in the # column, indicating it is locked. Below it is an 'Implicit Deny' row.

#	Name	From	To	Source	Destination	Schedule	Service
1	test_001	1-A11 net_lan	dmz	all	all	always	ALL
▼ Implicit (2-2 / Total: 1)							
2	Implicit Deny	any	any	all	all	always	ALL

View Locked Policy Packages Option

Quick Check Locked Policy Packages

The screenshot shows the Fortinet Policy Packages interface. A context menu is open over the 'Implicit Deny' policy package. The menu items are: Install Wizard, New, Clone, New Folder, Lock, Unlock, View Locked Packages (highlighted), Move, Edit, Delete, Policy Check, Run Script, Export to Excel, and Export to CSV. A red arrow points from a text box to the 'View Locked Packages' option.

Name	From	To	Source	Destination	Security Profiles	Schedule	Service	Users	Ac
	any	any	all	all	high_security no-inspection	always	ALL		✓
cit (2-2 / Total: 1)									
Implicit Deny	any	any	all	all		always	ALL		⊗

New option to expose the whole list of *locked* Policy Packages

ADOM Selection Enhancements

New Create New, Edit and Delete Options

New right-click options: *Edit*, *Delete*, *Lock* and *Unlock*

New *Create New* option






Tool-tip showing the ADOM *description*

The screenshot shows a window titled "Select an ADOM" with a search bar at the top right. Below the search bar is a grid of ADOMs. The grid has three columns. The first column contains ADOMs like "root (5)", "ADOM_6_0", "ADOM_TEMPLATE_001", "DEMO_001 (7)", "DEMO_004", "DEMO_010 (2)", "DEMO_013 (4)", "ICRC (1)", and "STAGING". The second column contains "ADOM_001", "ADOM_BACKUP_001 (Backup)", "CUSTOMER_001 (1)", "DEMO_002 (1)", "DEMO_005 (2)", "DEMO_011 (1)", "DEMO_014 (3)", "SCRIPT", and "demo_001". The third column contains "ADOM_5_6 (1)", "ADOM DEMO (25) This is a demo ADOM backup)", "DEMO (25)", "DEMO_003 (2)", "DEMO_006", "DEMO_012 (2)", "DEMO_015", "SDWAN_001 (4)", and "Global Database". A context menu is open over the "DEMO (25)" ADOM, showing options: Edit, Delete, Lock, and Unlock. At the bottom left of the grid is a "+ Create New" button, and at the bottom right is a "Close" button.

ADOM Revision Enhancements

Support Additional Templates

ADOM Revision

<input type="checkbox"/>	ID	Name	Created By	Created Time	Comment
<input type="checkbox"/>	13	staging.pp_2020-5-26-16	 admin	2020-05-26 16:39:49	
<input type="checkbox"/>	12	staging.pp_2020-5-26-15	 admin	2020-05-26 15:57:07	
<input type="checkbox"/>	11	staging.pp_2020-5-26-15	 admin	2020-05-26 15:54:22	
<input type="checkbox"/>	10	staging.pp_2020-5-26-15	 admin	2020-05-26 15:50:44	
<input type="checkbox"/>	9	staging.pp_2020-5-26-15	 admin	2020-05-26 15:45:26	

[Settings](#) [Close](#)

SD-WAN Templates

FAP Profiles

FSW Templates

CLI Templates

Certificate
Templates

Normalization Interfaces

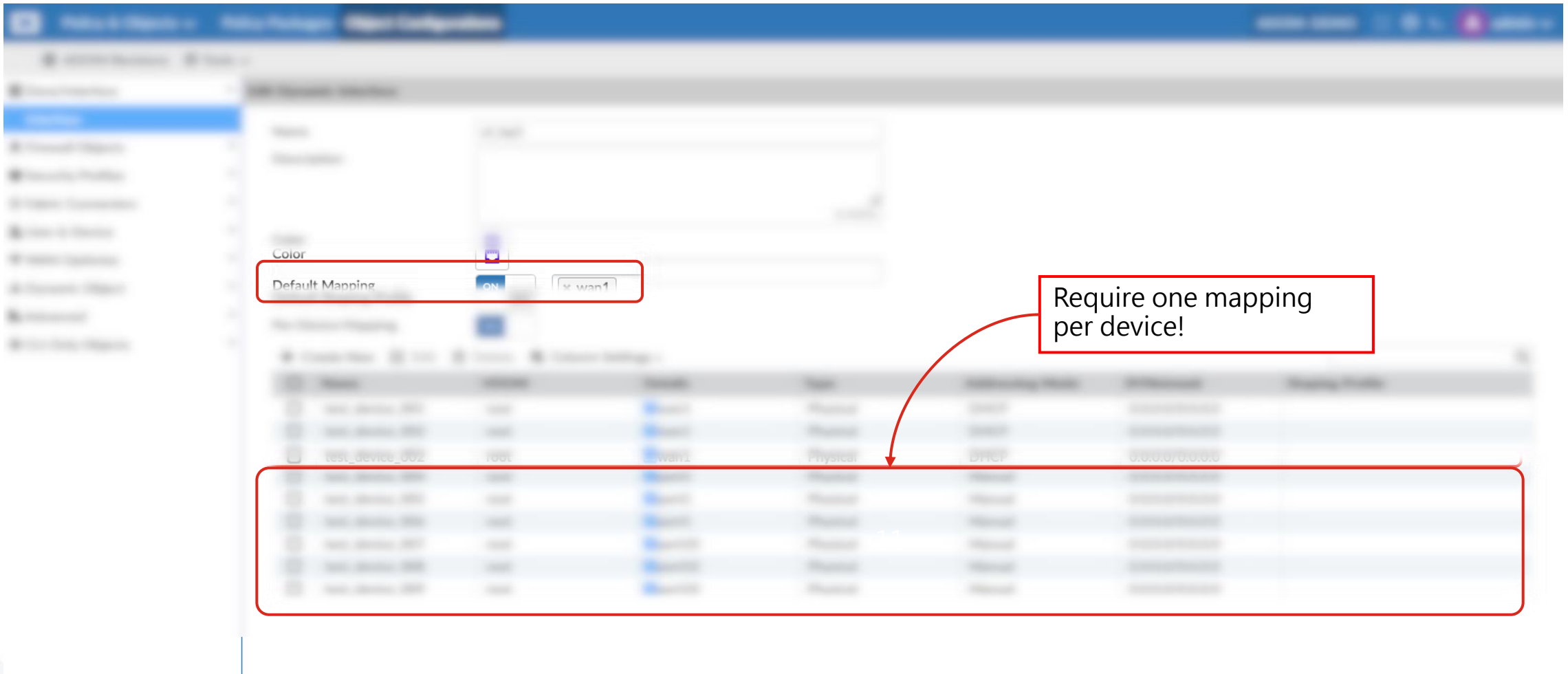
Concern: Lot Of Wordings And Confusion

- Dynamic Interface: Policy Zone vs Policy Interface

Type1	Name	Per-device mapping	FortiGate policies will reference
Interface	u1_isp1	wan1	wan1
Zone	z_dmz	dmz , wan2	z_dmz
Zone	z_dmz	z_dmz (dmz , wan2)	z_dmz (dmz , wan2)

Normalization Interfaces

Concern: Per-Device Mapping Is Not Flexible Enough



Require one mapping per device!

Normalization Interfaces

Using Rules: **Per-Device, Per-Platform, Default Mapping!**

The screenshot shows the 'Create New Normalized Interface' configuration page in the FortiGate GUI. The interface name is 'ul_isp1'. The 'Per-Platform Mapping' toggle is set to 'ON' and is highlighted with a red box. Below it, a table lists mapping rules. The first rule, with 'Name' 'all' and 'Device Interface Name' 'wan1', is highlighted with a red box and labeled 'Default!' with a red arrow. The 'Per-Device Mapping' toggle is also set to 'ON' and highlighted with a red box. Below it, another table lists device-specific mappings for 'branch1' and 'branch2'.

#	Name	Device Interface Name	Egress Shaping Profile	Ingress Shaping Profile
1	all	wan1		
2	FortiGate-1500D	port10		
3	FortiGate-3000D	port22		

Name	VDOM	Details	Type	Addressing Mode	IP/Netmask	Shaping
branch1	root	wan2	Physical	DHCP	0.0.0.0/0.0.0.0	
branch2	root	wan2	Physical	DHCP	0.0.0.0/0.0.0.0	

Takes precedence...

Normalization Interfaces

Update Import Policy

Import Device - foobar_device_001 [root]

Create a new policy package for import.

Policy Package Name: foobar_device_001

Folder: root

Policy Selection: Import All (2) Select Policies to Import

Object Selection: Import only policy dependent objects Import all objects

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Device Interface	Mapping Type	Normalized Interface
lan	<input checked="" type="radio"/> Per-Device <input type="radio"/> Per-Platform	lan
wan1	<input type="radio"/> Per-Device <input checked="" type="radio"/> Per-Platform	wan1

Add mappings for all unused device interfaces

Next > Cancel

ZTP Enhancements

New Cluster Model Device

Add Device

Discover Device Add Model Device Add Model HA Cluster

Name

HA Mode

Cluster Name

Password

Link Device By

Serial Number

Priority

Device Model

Enforce Firmware Version

Assign Policy Package

Assign Device Provision Profile

Monitor Interfaces

Heartbeat Interfaces

ZTP Enhancements

Firmware Rectification For Model FortiSwitch And FortiAP

FortiSwitch Manager -> Managed Switches -> Create New

Add Model FortiSwitch

FortiGate: test-002 (root) [v]

Device Interface: fortilink [v]

Serial Number: []

Name: []

Enforce Firmware Version: OFF

OK Cancel

AP Manager -> Managed Aps -> Create New

Add Model FortiAP

FortiGate: [] [v]

Serial Number: []

Name: []

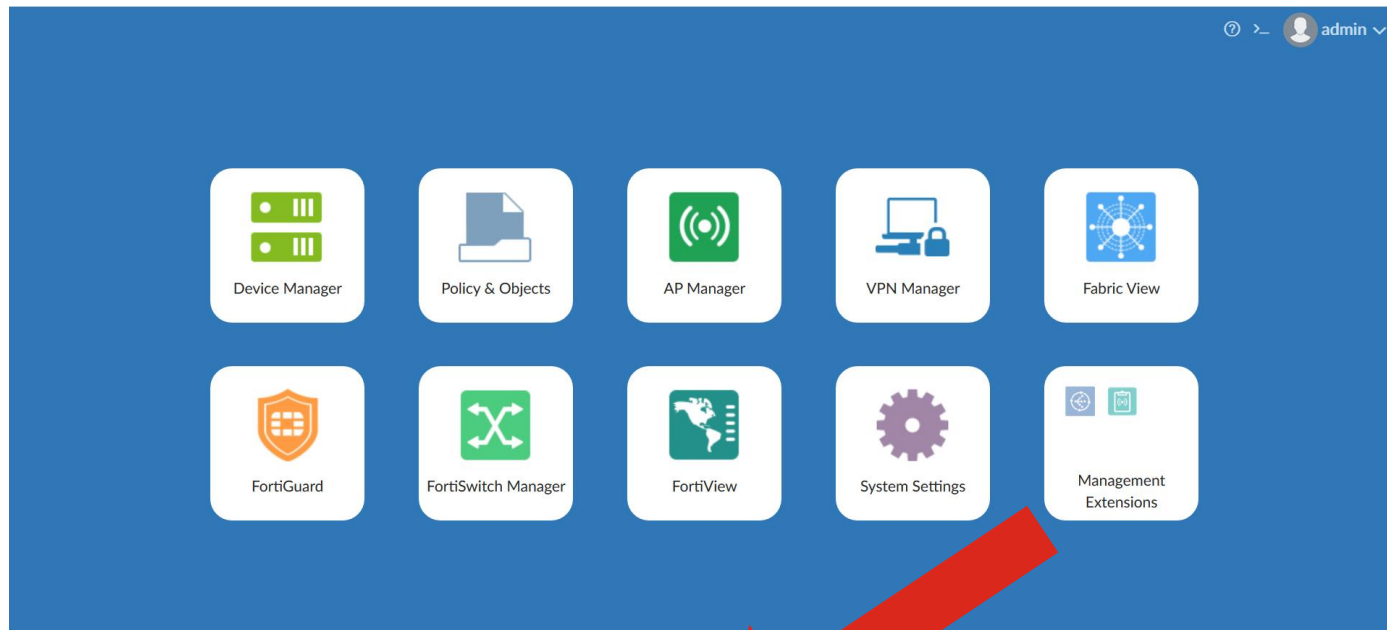
AP Profile: None [v]

Enforce Firmware Version: OFF

OK Cancel

Management Extensions – SD-WAN Orchestration

Enable Your SD-WAN Orchestration



- Login into **FortiManager**
- Click on **Management Extensions**
- Click on **SD-WAN Orchestrator**
- It will free download and install the SD-WAN Orchestrator container into FortiManager
- After the icon color become solid, the SD-WAN Orchestrator is ready

** Managed FortiGate need to have ***SD-WAN Orchestrator Entitlement License***

Management Extensions – SD-WAN Orchestration

Streamline Your SD-WAN Configuration Process

SD-WAN Orchestrator

Quick Access ▾ ADOM: root [?] [A] admin ▾

+ Device ▾ + Region ▾ **Install all configuration** ↵ ↻ Reload

EU 3 Device(s) 3 Online 0 Offline Modified ↵

Device Name	From IP	Status	Policy Package Status	Serial Number	Profile Name	Role	Config Status
EU_HUB	10.106.13.21	Valid	Permit_All	FGVM01TM20000593	Hub_Dialup	Hub	Modified
EU_EDGE1	10.106.13.22	Valid	Permit_All	FGVM01TM19000598	Edge_dialup	Edge	Modified
EU_EDGE2	10.106.13.23	Valid	Permit_All	FGVM01TM19000599	Edge_dialup	Edge	Modified

US 3 Device(s) 3 Online 0 Offline Synchronized ↵

Device Name	From IP	Status	Policy Package Status	Serial Number	Profile Name	Role	Config Status
US_HUB	10.106.13.24	Valid	Permit_All	FGVM01TM19000600	Hub_Dialup	Hub	Synchronized
US_EDGE1	10.106.13.25	Valid	Permit_All	FGVM01TM19000601	Edge_dialup	Edge	Synchronized
US_EDGE2	10.106.13.26	Valid	Permit_All	FGVM01TM19000602	Edge_dialup	Edge	Synchronized

- ✓ Planning Your Network - Define Region / HUB /Edge
- ✓ Creating **Shared Resources**
- ✓ Creating **Profiles** for all roles
- ✓ Adding **Devices** to FMG & SD-WAN Orchestrator
- ✓ **Installing Configurations**
- ✓ Installing Firewall Policies (in **Policy Packages**)
- ✓ **Monitoring Your SD-WAN Network**

Management Extensions – SD-WAN Orchestration

Monitoring SD-WAN Devices And Network Traffic

The screenshot displays the SD-WAN Orchestrator interface. On the left is a navigation menu with sections: Monitor (Dashboard, Traffic, SLA, Devices, Logs), Configuration (Device, Profile, Shared Resources, Intranet Address, IPv4 Address, IPv4 Address Group, Network, SLA, System, Health Threshold), and Maintenance. The main area shows a map of Europe with a dashed blue circle representing the EU region. A search bar at the top right says "Locate a device". A tooltip for "EU_HUB" is open, showing device details.

CPU	DISK	MEM	Underlay Link
Region: EU			
Serial Number: FGVM01TM20000593			
Platform: FortiGate-VM64			
IP: 10.106.13.21			

Management Extensions – SD-WAN Orchestration

Monitoring SD-WAN Devices And Network Traffic

SD-WAN Orchestrator | Quick Access | ADOM: root | admin

Monitor | **EU_HUB**

Overview | Link | Traffic | SLA

Device Name: EU_HUB
 Type: FortiGate-VM64
 Connect Time: 0 day 20 hours 19 minutes
 From IP: 10.106.13.21
 Version: 6.2.2

CPU%: Bad [Progress] Very Good
 DISK%: Bad [Progress] Very Good
 Memory%: Bad [Progress] Very Good
 Underlay Link: Bad [Progress] Very Good

Latest

CPU: Average 2% | DISK: Average 1% | Memory: Average 50%

Past 1 Hour

Top Sources (Total Traffic)

Source IP	Received (bytes)	Sent (bytes)
192.168.0.2	~340K	~100K

Top Destinations (Total Traffic)

Destination IP	Received (bytes)	Sent (bytes)
34.197.120.129	~70K	~15K
104.114.76.170	~40K	~40K
8.8.8.8	~30K	~15K
23.1.245.74	~25K	~10K
34.208.33.228	~20K	~5K

Top Apps (Total Traffic)

App	Received (bytes)	Sent (bytes)
HTTPS.BROWSER	~180K	~40K
HTTP.BROWSER	~50K	~40K
DNS	~40K	~10K
NTP	152bytes	152bytes

Top Cloud Apps (File Size)

No Data Available

Throughput Total Outbound | Throughput Total Inbound

What's New FortiAnalyzer 6.4.0

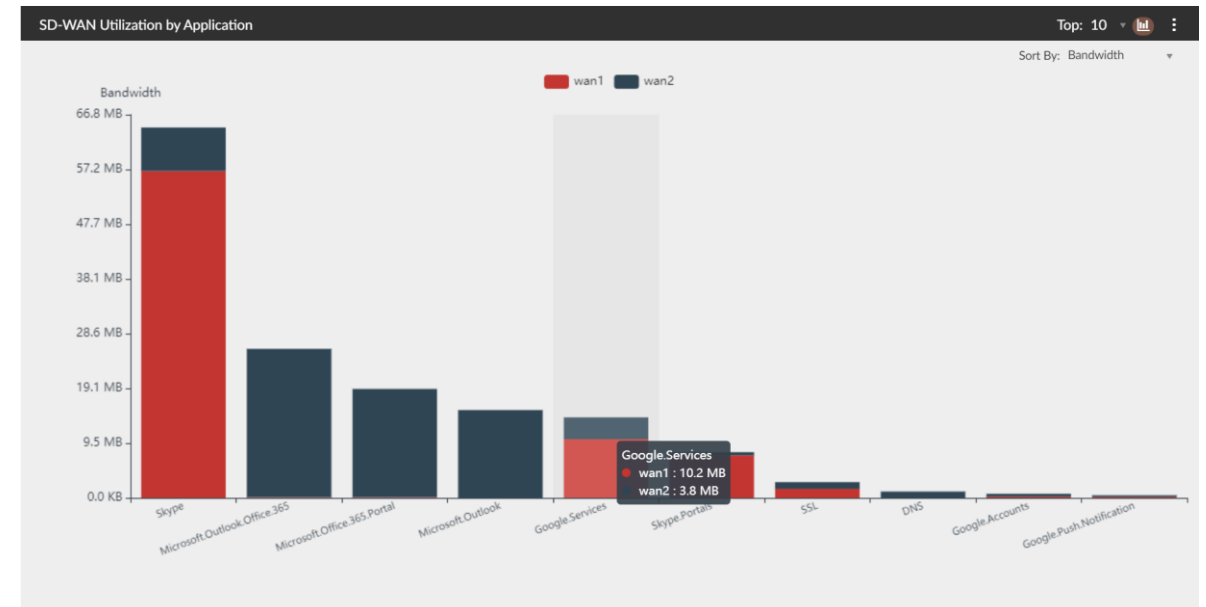
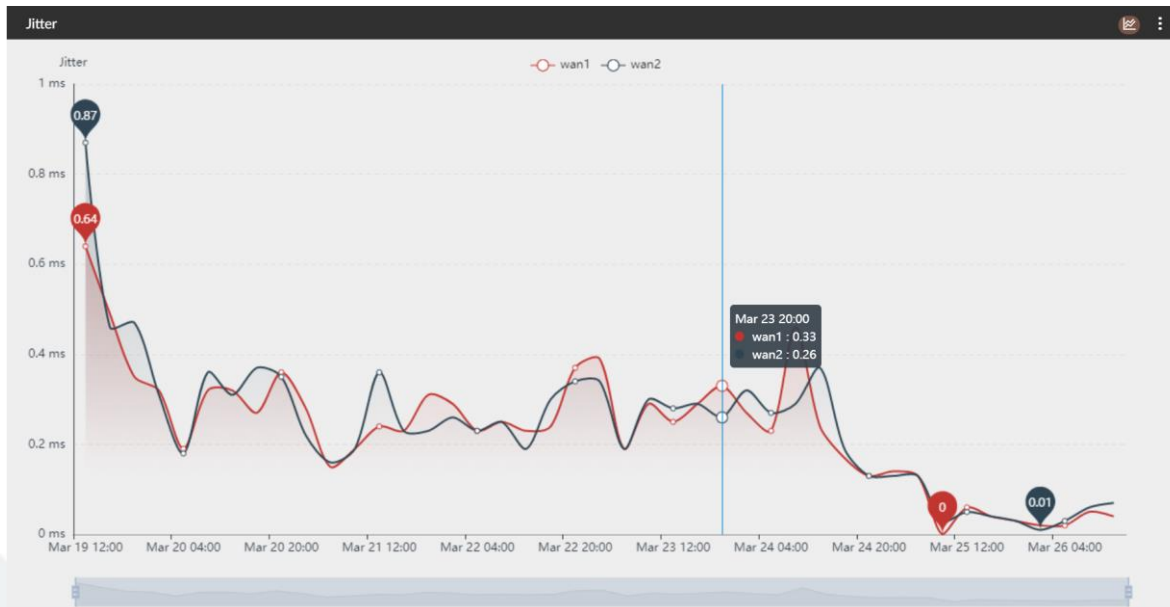
What's New FortiAnalyzer 6.4.0

- SD-WAN Monitoring Dashboard and Reporting
- FortiSOC Introduction
- Fabric Logs Normalization (Fabric ADOM)
- FortiAnalyzer New Licenses Introduction

Security Driven Networking

SD-WAN Monitoring Dashboard

- Charts similar to those available in the Secure SD-WAN Report can be found as widgets in the default SD-WAN dashboard of FortiView.
- The Monitors window in FortiView has a predefined Secure SD-WAN Monitor pane with 8 SD-WAN widgets.



Security Driven Networking

New Secure SD-WAN Report

Introduction Secure SD-WAN

As the use of business-critical, cloud-based applications and too organizations with multiple remote offices are switching from p architectures. SD-WAN offers business application steering, cost ware-as-a-Service (SaaS) applications, as well as unified commur its own shortcomings—especially when it comes to security with We aggregated key findings from the Secure SD-WAN assessme highlights are listed below, a more detailed view of each section

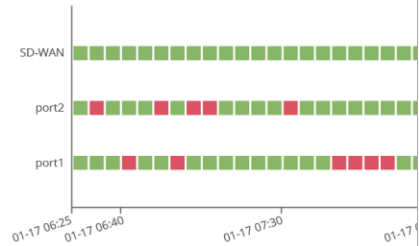


SD-WAN Performance

Performance link monitoring measures the health of li interfaces by sending probing signals through each lin on latency, jitter, and packet loss. If a link is broken, th routed through other links. When the link is working a traffic being sent to a broken link and lost.

Overview

Link Status Quality Before and After SD-WAN Impleme



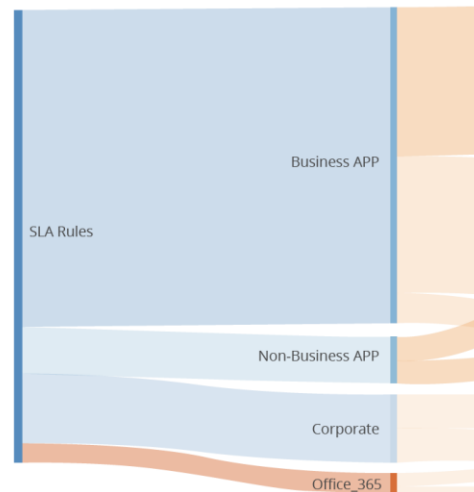
SLAs

Performance SLA by WAN Link (drill-down)

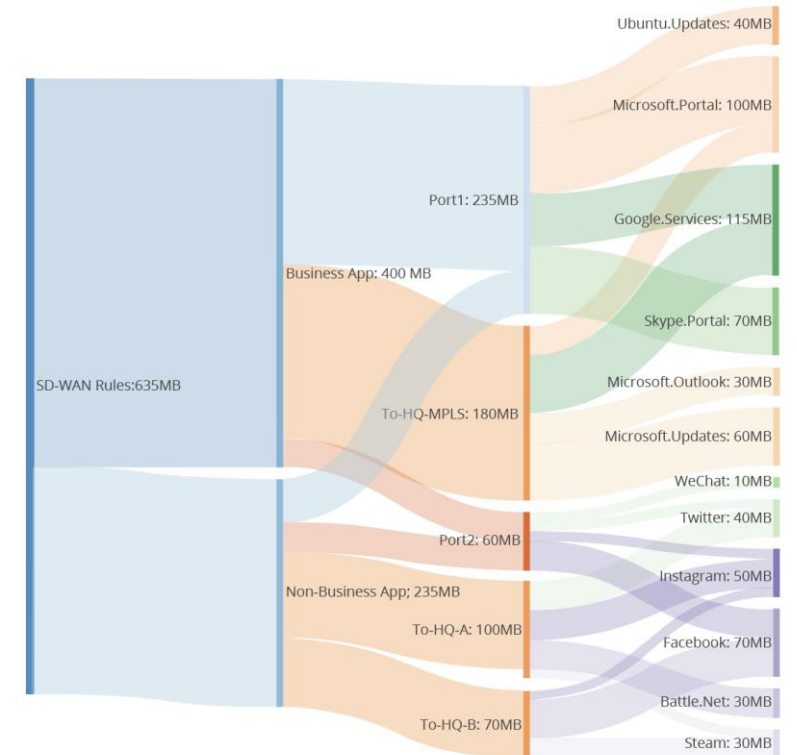
Multi-path technology can automatically fail over to the best avai degrades. This automation is built into the FortiGate, which redu improving their experience and productivity.

SLA Rules	Links	% Passed Latency Threshold	% Pa Jitter
BusinessCritical	Port1	99.8	98.1
	Port2	99.6	99.4
	TO-HQ-MPLS	98.7	89.5
Corporate	TO-HQ-A	89.1	87.9
	TO-HQ-B	99.5	88.3
Office_365	TO-HQ-A	89.5	79.5
	TO-HQ-B	87.9	98.7
LinkA	TO-HQ-A	88.3	89.1
NonBusinessCritical	Port1	99.5	99.5
	Port2	97.9	97.9

SD-WAN Interface Status Change Counts



SD-WAN Bandwidth Utilization by Application and SD-WAN Link



FortiSOC Introduction

Security Analytics, Detection, Response

- FortiSOC (Subscription Licenses)
 - FortiSOC dashboards
 - Automation playbooks
 - Expanded incident analysis page
 - Attach reports to incidents
 - Add comments to incidents
- Normalized Fabric logs



**Security Fabric
Analytics**



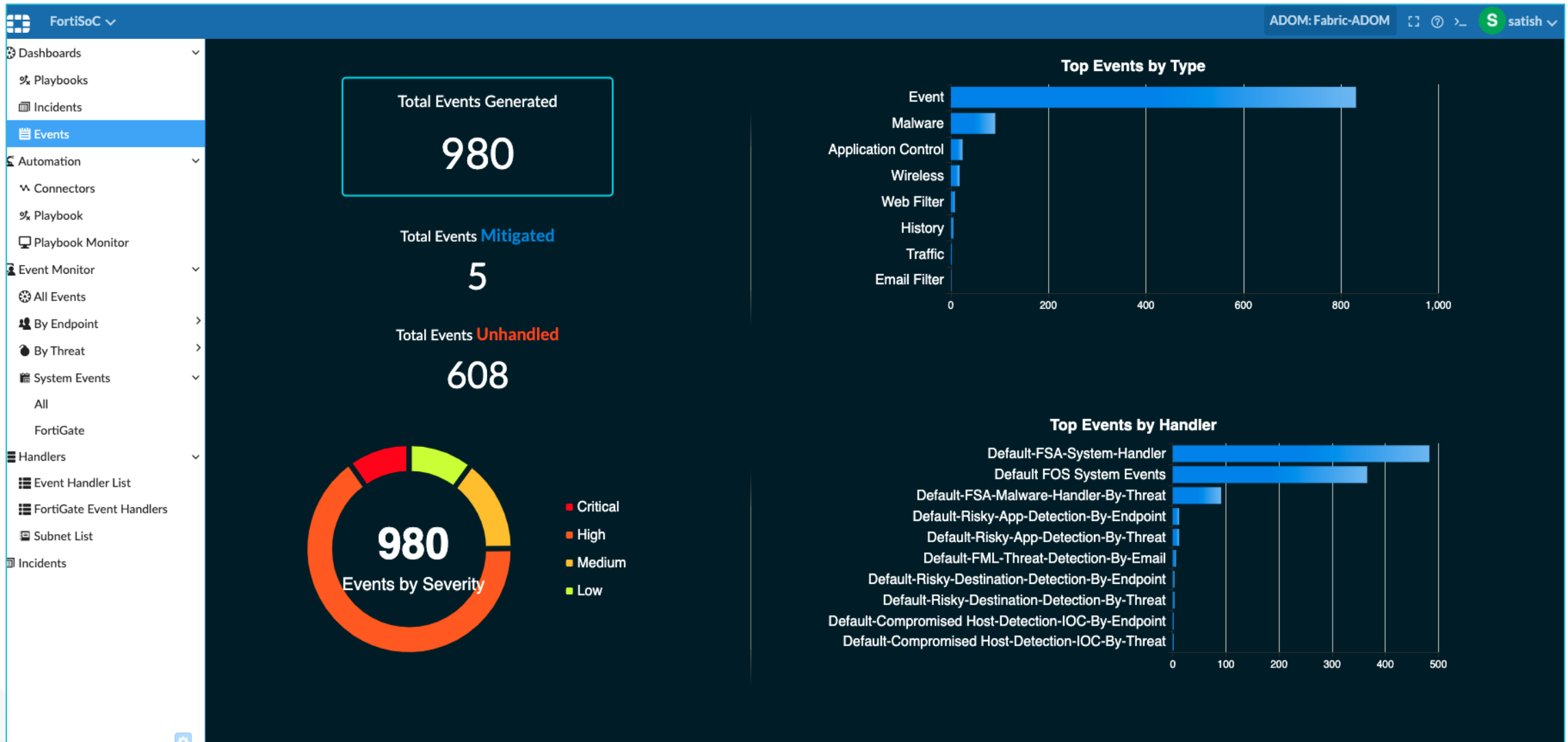
**Advanced
Detection**



**Automated
Response**

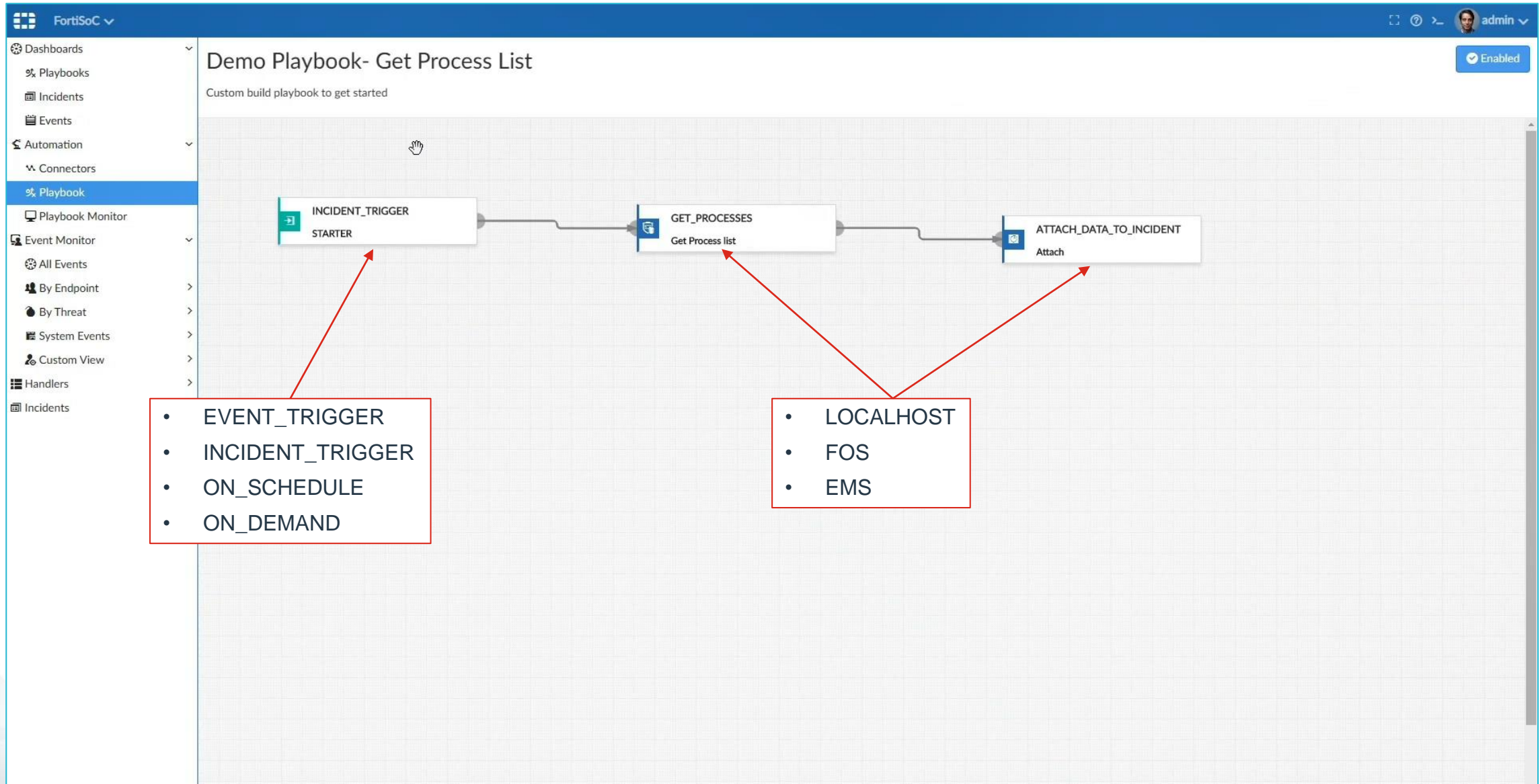
FortiSOC – Dashboards

Playbooks / Incidents / Events Dashboards



FortiSOC – Automation Playbooks

Automation Incident Response Process



Incidents Tracking and Management

Expanded Incidents Analysis Page

The screenshot displays the FortiSoC interface for incident analysis. The top navigation bar includes the FortiSoC logo, user information (ADOM: root, admin), and system status. The main content area is divided into several sections:

- Incident Header:** Shows incident ID IN00000010, severity (High), and details: IPS incident created for endpoint Malicious Code, Not Assigned, Analysis. It also shows creation and modification timestamps.
- Affected Endpoint/User:** Displays details for endpoint FGVM01TM19005285 (Alder), including MAC and IP addresses, and operating system (Windows Microsoft Windows 8.1 Enterprise Edition, 64-bit (build 9600)).
- Executed Playbooks:** A table showing the status of executed playbooks. A red box highlights this section with the annotation "SOC module enabled".
- Audit History:** A vertical timeline showing various events attached to the incident, such as "Note Attached to Incident" and "Report Attached to Incident". A red box highlights this section with the annotation "Incidents Auditing".
- Incident Timeline:** A horizontal timeline showing the sequence of events from 2020-03-20 16:22:08 to 2020-03-20 16:41:12 (Total 13 Events).
- Comments and Reports:** A section for adding and managing comments and reports. A red box highlights this section with the annotation "Attach Reports".

Annotations at the bottom of the page indicate specific actions:

- Insert Comments:** Points to the "+ Add" button in the Comments section.
- Attach Reports:** Points to the "Reports" tab and the "Add" button in the Reports section.
- Incidents Auditing:** Points to the Audit History section.

PLAYBOOK	STATUS
Demo Playbook- Get Software Inventory	Success
Demo Playbook- Get Process List	Success
Demo Playbook- Run Vuln Scan	Success

Report Name	Format	Time Range	Devices	Status
Client Reputation-2020-03-20-16...	PDF	2020/03/15 - 2020/03/20	8 Devices	2s

Normalized Fabric logs

All Logs From Different Fabric Devices Are Normalized in Fabric ADOM

The screenshot displays the Fortinet Fabric ADOM Log View interface. The main table shows a list of logs with columns for #, Date/Time, Data Source ID, Event Message, Event Type, Event Severity, Source IP, and Destination. A detailed view of a log entry is shown on the right, with a red box highlighting the 'Data' section.

#	Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destinat
231	13:24:13	FEVM040000152312	to=tme1@fortisolutionsdemo.com, delay=2+04:34:58, xdelay...	event	information		
232	13:24:13	FEVM040000152312		statistics	information	209.87.240.248	172.3
233	13:24:13	FEVM040000152312	FortiGuard-AntiSpam identified spam IP: 185.207.10.151, sco...	spam	information	209.87.240.248	172.3
234	13:24:13	FEVM040000152312	queued for FortiSandbox scan, since it contained uris http://45...	virus	information	209.87.240.248	
235	13:24:13	FEVM040000152312	to=tme1@fortisolutionsdemo.com, delay=18:46:56, xdelay=0...	event	information		
236	13:24:13	FEVM040000152312	FortiGuard-AntiSpam identified spam URI: http://jx.cathaywar...	spam	information	209.87.240.248	172.3
237	13:24:13	FEVM040000152312		statistics	information	209.87.240.248	172.3
238	13:24:12	FEVM040000152312	Email x3FFrKM9000423-x3FFrKMA000423 has been process...	virus	information		
239	13:24:12	FEVM040000152312	to=tme1@fortisolutionsdemo.com, delay=1+10:02:57, xdelay...	event	information		
240	13:24:12	FEVM040000152312		statistics	information	209.87.240.248	172.3
241	13:24:12	FEVM040000152312	FortiGuard-AntiSpam identified spam URI: http://cathaywareh...	spam	information	209.87.240.248	172.3
242	13:23:59	FGVM01TM20001835	URL belongs to an allowed category in policy	webfilter			
243	13:23:59	FGVM01TM20001835	Authentication lockout(User from 1.1.1.1 was locked out)	event	warning	1.1.1.1	2.2.2.:
244	13:23:59	FGVM01TM20001835	Social.Media: Sohu,	utm	information	10.88.54.104	104.2
245	13:23:59	FGVM01TM20001835	Switch-Controller Switch Sync Complete(fsw-firenze-lab Conf...	event	information		
246	13:23:59	FGVM01TM20001835		traffic	notice	172.88.2.42	10.23
247	13:23:59	FGVM01TM20001835		traffic	notice	173.88.84.4	10.23
248	13:23:59	FGVM01TM20001835	Collaboration: Skype_Communication,	utm	information	172.28.1.107	65.55
249	13:23:59	FGVM01TM20001835	URL belongs to an allowed category in policy	webfilter			
250	13:23:59	FGVM01TM20001835	Authentication timed out(User from 1.1.1.1 was timed out)	event	notice	1.1.1.1	2.2.2.:
251	13:23:59	FGVM01TM20001835	Social.Media: Sohu,	utm	information	10.88.54.104	104.2
252	13:23:59	FGVM01TM20001835	Switch-Controller Switch Sync Complete(fsw-firenze-corp Co...	event	information		
253	13:23:59	FGVM01TM20001835		traffic	notice	172.88.2.42	10.23
254	13:23:59	FGVM01TM20001835		traffic	notice	172.88.3.189	10.23
255	13:23:59	FGVM01TM20001835		traffic	notice	172.28.1.107	157.5
256	13:23:59	FGVM01TM20001835	FSSO logoff authentication status(FSSO-logoff event from ser...	event	notice	1.1.1.1	
257	13:23:59	FGVM01TM20001835	URL belongs to an allowed category in policy	webfilter			
258	13:23:59	FGVM01TM20001835	Social.Media: Sohu,	utm	information	10.88.54.104	104.2

Data

- Data Parser Name: FortiMail parser
- Data Source ID: FEVM040000152312
- Data Source Name: FEVM040000152312 root
- Data Source Type: FortiMail
- Data Timestamp
- Date/Time: 13:24:13
- Time Stamp: 2020-06-02 13:24:13

Event

- Event ID: 3013598
- Event Message: to=tme1@fortisolutionsdemo.com mailer=esmtpl, pri=18900000, refered(Reason)
- Event Severity: information
- Event Sub Type: smtp
- Event Type: event

Host

- UEBA Endpoint ID: 0

User

- UEBA User ID: 0
- User Domain: mail
- User ID: mail

Network

- Net Session ID: x5F96QVr016529-x5F96QV50165

Others

- Source Port: 55727

FortiAnalyzer New Licenses

FortiAnalyzer Licenses

New Licenses introduced in Q2/2020

New Licenses (Q2/2020)	FAZ Appliance	FAZ-VM		FAZ-Cloud
		S-Series	Perpetual	
SOC subscription Service	Yes, à la carte and bundle option available	Included in FAZ-VM subscription license	Not supported	No support now. Coming in Q3
FAZ-VM Subscription	Not Applicable	Yes, VM-S, 24X7 FortiCare Contract, IOC & SOC service are included.	Not Applicable	Not Applicable
ADOM License	Perpetual license. Only apply to new platforms introduced in Q2/20 or later	Subscription license. Available to increase the ADOM limit.	Not Applicable	No support now. Coming in Q3

FortiAnalyzer SOC Subscription Service

FortiSOC Subscription Service

- FortiSOC Trial Mode:

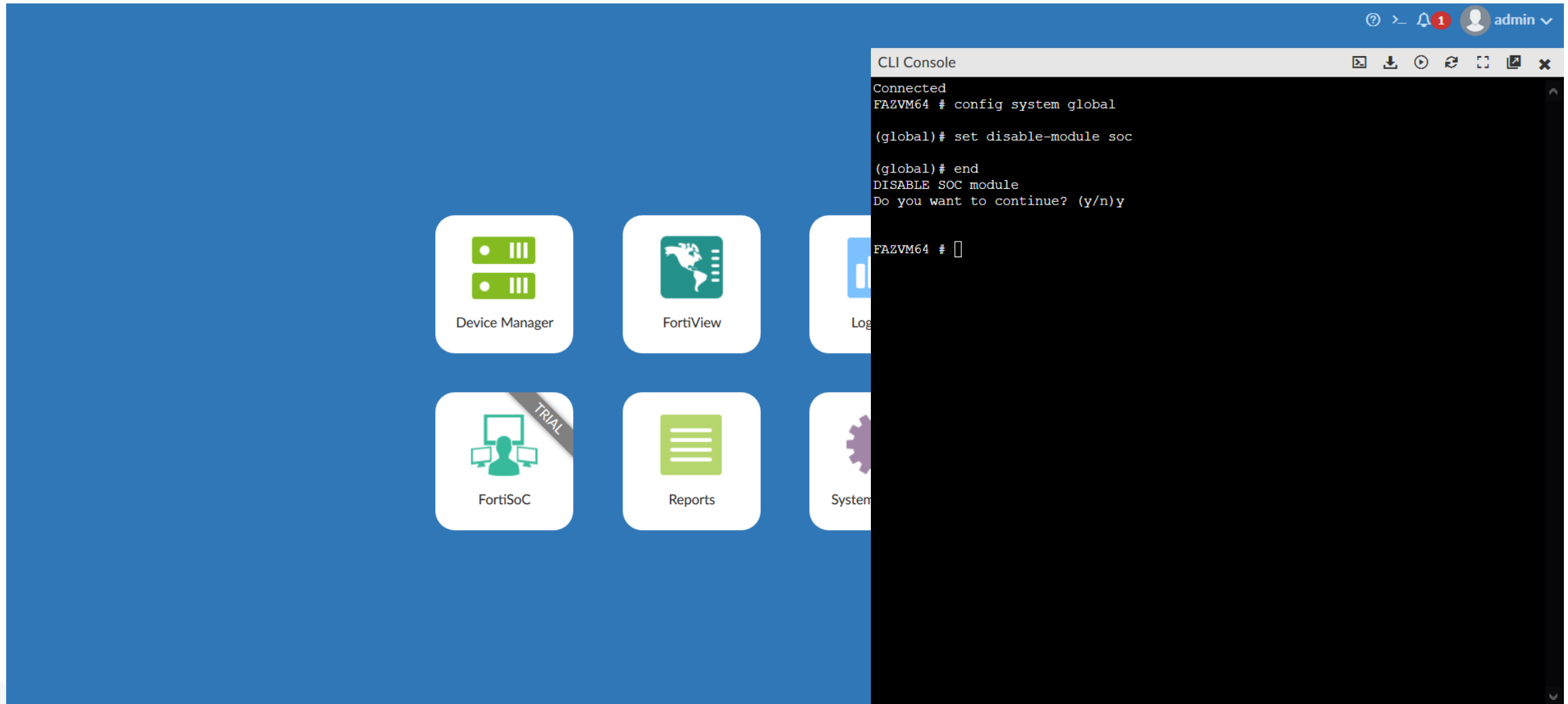
- Enable customers to easily try out SOC automation feature before purchasing the license
- The 'Trial' banner & the license warning are moved
- Try-it-out limits to 5 playbook executions per day

The screenshot displays the FortiSOC web interface. At the top, a yellow warning banner states: "SOC automation is running in a limited capacity of up to 5 playbooks per day. An SOC subscription is required to run at full capacity." The interface is divided into several sections:

- System Information:** Host Name: FAZVM64, Serial Number: FAZ-VMTM19009501, Platform Type: FAZVM64, HA Status: Standalone, System Time: Fri May 08 14:36:55 2020 PDT, Firmware Version: v6.4.0-build2039 200504 (Interim), System Configuration: Last Backup : Fri May 8 11:54:18 2020, Current Administrators: admin / 1 in total, Up Time: 2 hours 50 minutes 39 seconds, Administrative Domain: ON, Operation Mode: Analyzer (selected) and Collector.
- System Resources:** Three circular gauges showing Average CPU Usage (6%), Memory Usage (34%), and Disk Usage (45%).
- License Information:** A table showing license details for VM License, FortiCloud, FortiGuard, Security Operations (SOC Service - No License), Logging, Storage Connector Service, and Update Server.
- Unit Operation:** A section for FortiAnalyzer-VM64 with buttons for Restart and Shutdown.

FortiSOC Trial Mode

Trial Mode Can Be Disable from CLI



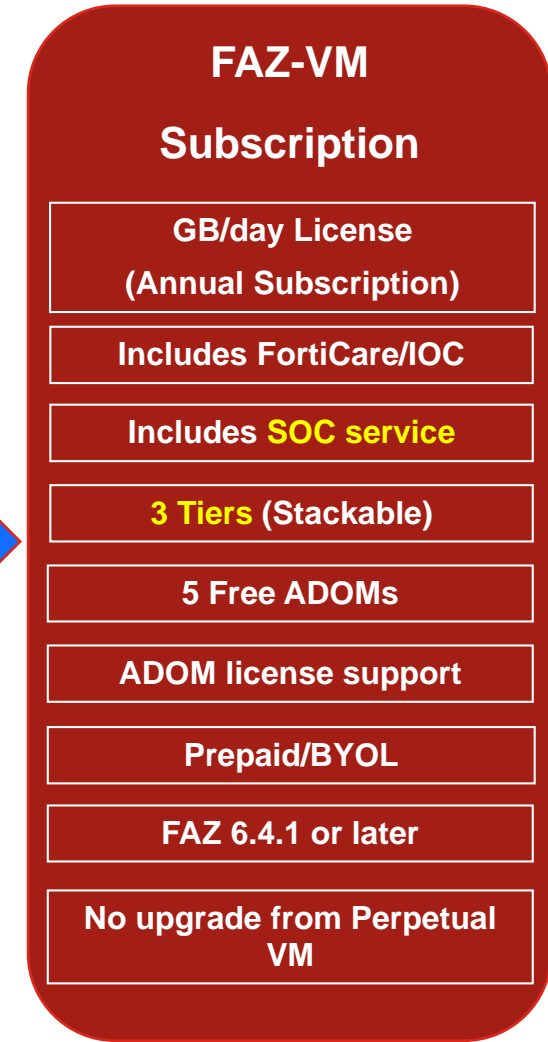
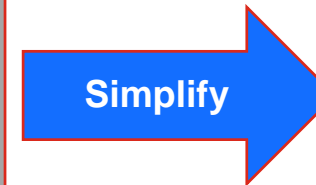
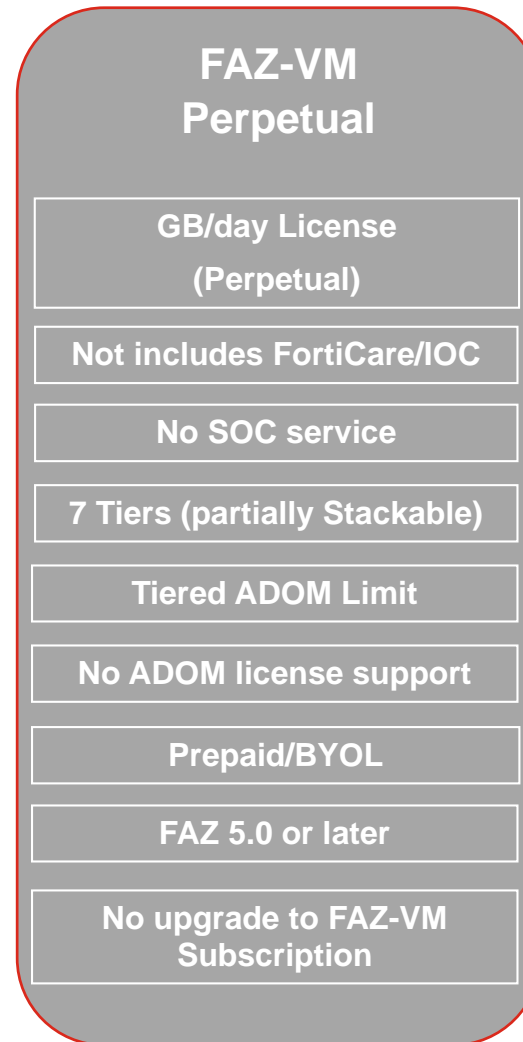
The image shows a screenshot of the FortiSOC web interface on a blue background. On the left, there are several white rounded square icons: 'Device Manager' (green server rack), 'FortiView' (green globe), 'Log' (blue document), 'FortiSoC' (green person at computer with a 'TRIAL' banner), 'Reports' (green document), and 'System' (purple gear). On the right, a 'CLI Console' window is open, showing a terminal session. The terminal text is as follows:

```
Connected
FAZVM64 # config system global
(global)# set disable-module soc
(global)# end
DISABLE SOC module
Do you want to continue? (y/n)y
FAZVM64 #
```

FortiAnalyzer VM Licenses – Perpetual & Subscription

Simplify **VM** licensing to make it easier to order and renew

- Simplify licensing SKUs
- Everything included
 - VM
 - 24x7 FortiCare support
 - IOC service
 - New SOC service
- 3 Tiers Stackable
 - 5GB, 50GB and 500GB
- Fully stackable
 - No base license need
 - ADOMs, GB/day



ADOM License

A new license for using ADOM on FortiAnalyzer and FortiManager

- **5 free ADOMs by default**
- Customer will be charged a flat fee per ADOM for extra ADOMs they add
- This is only for the **new NPI hardware** models and **FAZ/FMG S-Series** (subscription based). **No change for existing models.**

FortiAnalyzer CLOUD Licenses

Update

FAZ Cloud Base	Base subscription for Cloud-based Events and Security Log Management plus IOC Service
FAZ Cloud ADVANCED**	Advanced subscription to extend BASE for Cloud-based Events and Log Management with All log types plus IOC Service
FortiAnalyzer Cloud Premium	Available in mid Q3 – Q4 time frame Include all logs + FortiCare + IOC + SOC service Support for FGT 1U in initial roll-out
FortiCloud Premium Subscription***	Any customers choosing FortiManager or FortiAnalyzer Cloud will need FortiCloud Premium Subscription.

Q3/20

** Will be Removed from Pricelist

*** FortiCloud Premium is per FortiCare Account

FortiAnalyzer-VM / FortiManager-VM Free Trial

Prompt admin To Login & Register With FortiCloud

- Register VM license or get a trial VM license
- If a VM license is not associated with your FortiCloud account, **you can get a free trial license for up to three devices/VDOM and 5GB/day logs.**

Trial licenses do **not** expire.

- FortiCloud account required
- FAZ-VM / FMG-VM ONLY with ONE trial license per account
- 5GB/Day logs with 3 devices:
- FortiCare contract not included
- No support for VM-Subscription
- Not available for accounts with existing FAZ-VM / FMG-VM license

FortiAnalyzer-VM64

This product requires a valid license. If you already purchased the license, please upload it now. If you want to evaluate this product, please log in your FortiCloud account to start the free trial.

Upload License Login with FortiCloud

chutter@fortinet.com

.....

Login

Create Account Forgot Password

FortiAnalyzer-VM Free Trial

Free Trial License Status

The screenshot displays the FortiAnalyzer-VM System Settings interface. The left sidebar contains navigation options: Dashboard, Logging Topology, All ADOMs, Storage Info, Network, HA, Admin (Administrators, Profile, Remote Authentication Server, Admin Settings, SAML SSO), Certificates (Local, CA, CRL, Remote), and Log Forwarding. The main content area is divided into two panels: System Information and License Information.

System Information

Host Name	FAZVM64
Serial Number	FAZ-VMTM20008325
Platform Type	FAZVM64
HA Status	Standalone
System Time	Tue Jul 21 05:09:21 2020 PDT
Firmware Version	v6.4.1-build2072 200615 (GA)
System Configuration	Last Backup : N/A
Current Administrators	admin /1 in total
Up Time	2 minutes 54 seconds
Administrative Domain	<input type="checkbox"/> OFF
Operation Mode	Analyzer Collector

License Information

VM License	Type	Trial License
FortiCloud	Registered	kmyang@fortinet.com
FortiGuard	Indicators of Compromise Service Server Location	No License Servers located in US only
Security Operations	SOC Service	No License
Logging	Devices/VDOMs	0 of 3 (0.0%)
	GB/Day	0.0 of 5 (0.0%)
	VM Storage	Unlimited
Storage Connector Service	Cloud	No License
Update	AntiVirus and	96.45.33.88 Sunnyvale,

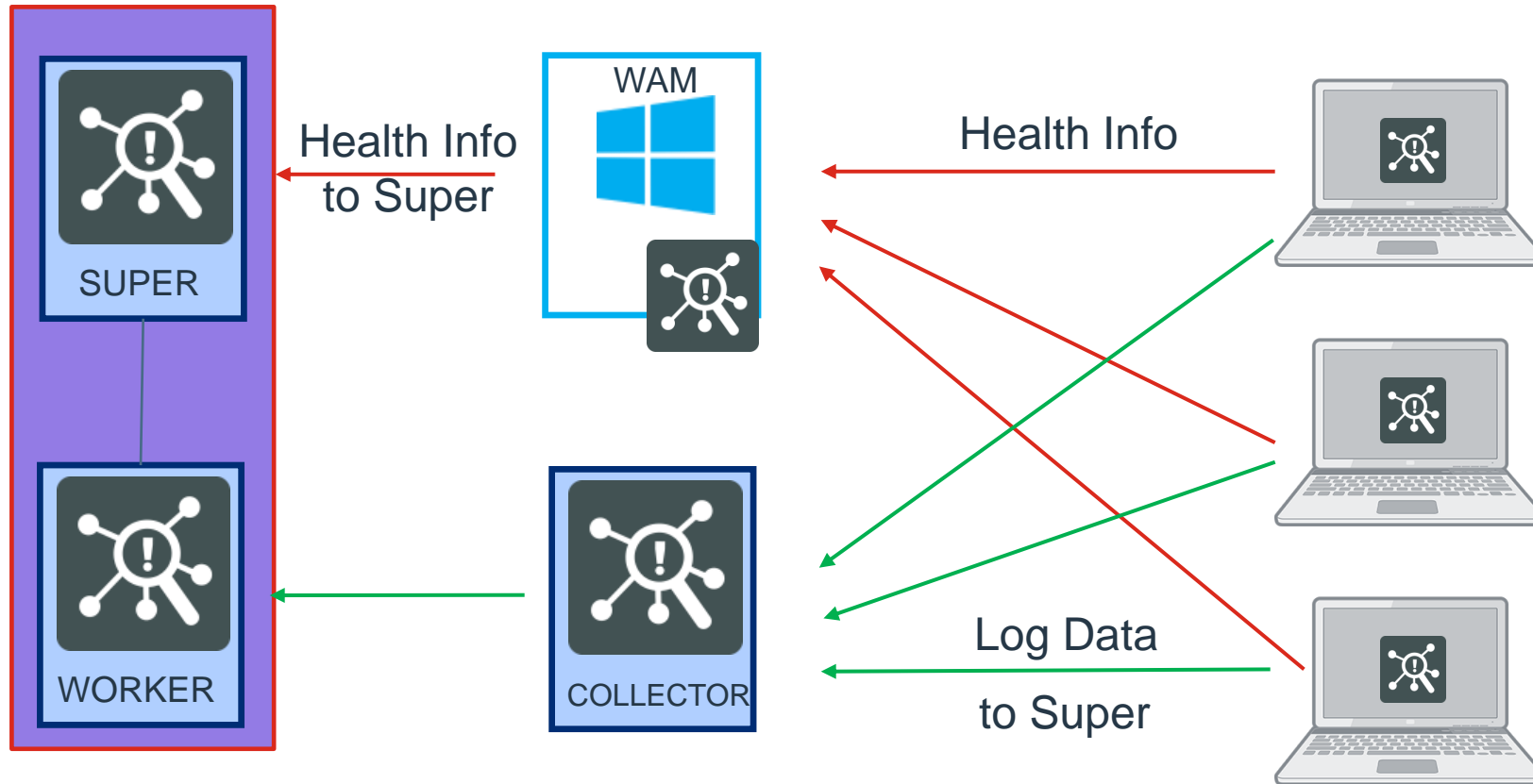
What's New FortiSIEM 5.3.0

What's New FortiSIEM 5.3.0

- Architecture Update - Agents Architecture and Features Recap
- Users Experience Optimization - Analytics & Forensics Enhancements
- Streamline Incident Response Process - Incidents & Cases Management

Agents Architecture and Features

Legacy Agent Architecture (Pre 5.2.1)



Tips



To offload event processing from Agents use a collector. Collectors typically forward to Super/Workers.

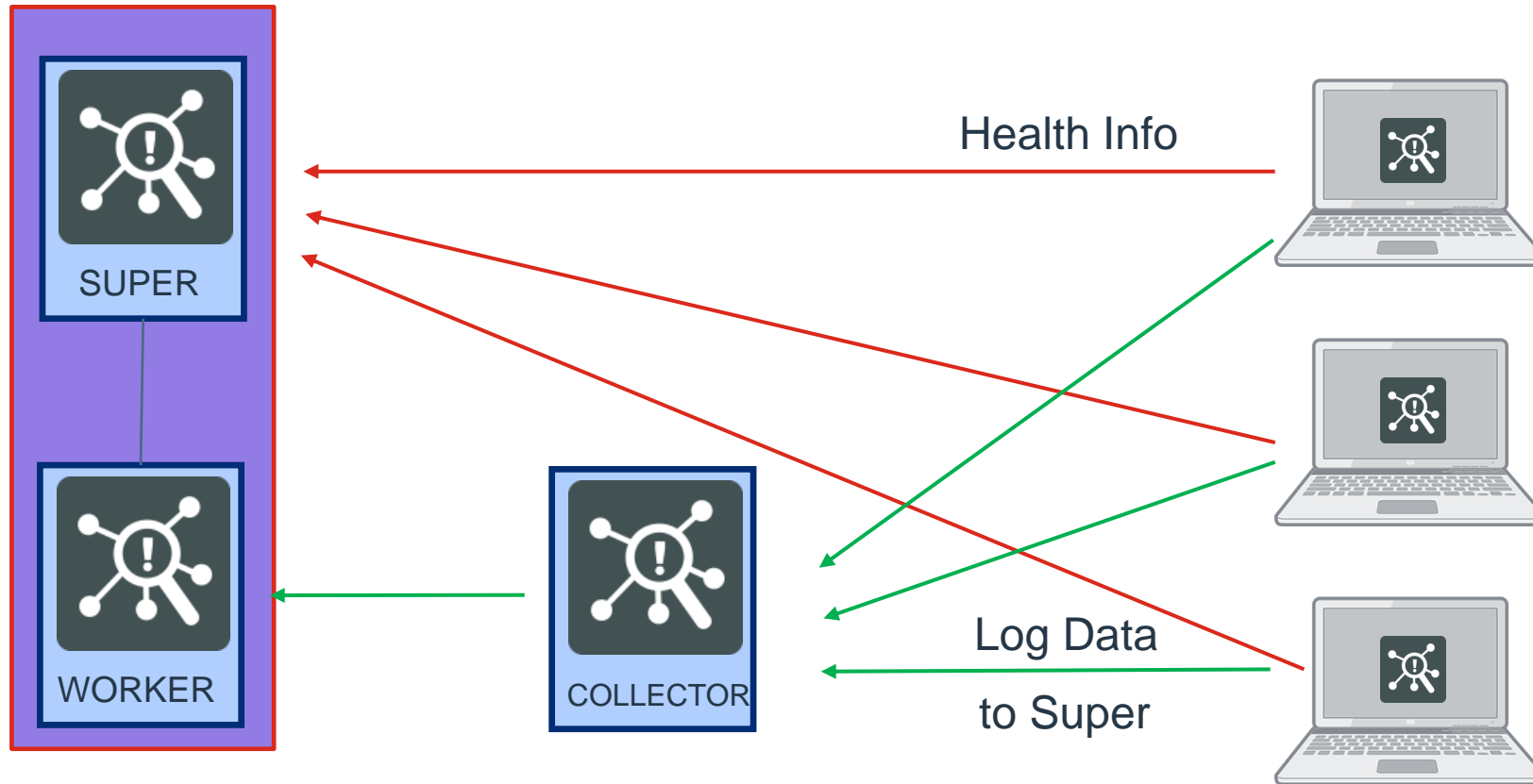
Tips



Collectors can be in remote location but agent must still be able to communicate with WAM.

Current Agent Architecture

- All Agent Communication is over HTTPS (TCP 443)



Tips



Agents MUST forward logs to a Collector.
Collectors typically forward to Super/Worker.

Tips



Collectors can be in remote location but agent must still be able to communicate with Super.

FortiSIEM Agent Feature Summary

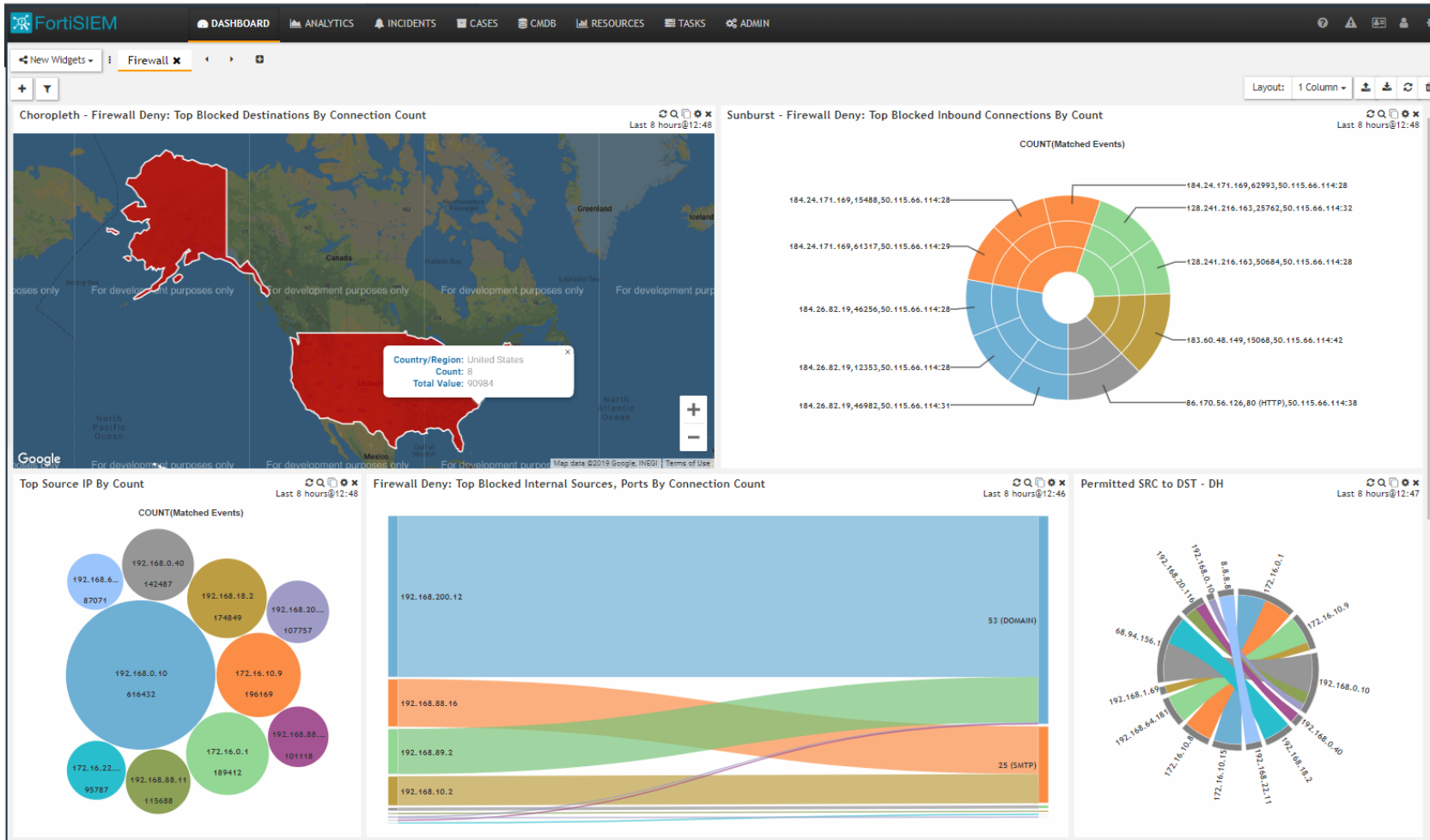
Advanced Log Collection Features

	Feature	Windows	Linux
Agentless	Discovery	✓	✓
	Performance Monitoring	✓	✓
	Log Collection	✓	✓
FortiSIEM Agent Key Features	Secure Log Collection (TLS)	✓	✓
	File Integrity Monitoring (FIM)	✓	✓
	Custom Log File Monitoring	✓	✓
	Central Management	✓	✓
	DNS, DHCP, IIS logs	✓	
	Installed Software Detection	✓	
	Registry Change Monitoring	✓	

Analytics & Forensics Enhancements

More Visualizations Charts

More Charts For Dashboard & Reports



Wide range of data visualizations, including:

- Bar and line chart
- Table
- GEO map
- Sankey and chord
- Choropleth
- Starburst
- Bubble
- Donut
- Heat map
- ... and more!

Analytics – Click Reduction

Users Experience Optimizations

Filter Operator as an Option

Group By and Display Fields

Attribute	Order	Display As	Row	Move
Event Receive Time	DESC		+ -	↑ ↓
Reporting IP			+ -	↑ ↓
Event Type			+ -	↑ ↓
Type in attribute...			+ -	↑ ↓

* COUNT(Matched Events)

Apply & Run Apply Cancel

Count is now a shortcut

Event Name

Raw Event Log

Disk Utilization stats for a device

[PH_DEV_MON_SYS_DISK_UTIL]:[eventSev...

Filter operators: =, !=, <, >, <=, >=, IN, NOT IN, CONTAIN, NOT CONTAIN

Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+ -	Event Type	!=	PH_DEV_MON_SYS_DISK_UTIL	+ -	AND	+ -

Event Attribute

CMDB Attribute

Analytics – Run CMDB Reports in Analytics

The screenshot shows the FortiSIEM Analytics interface. At the top, there are navigation tabs for DASHBOARD, ANALYTICS, INCIDENTS, CASES, CMDB, RESOURCES, and TASKS. Below the navigation, there are several tabs for search results: [2] Search, [3] Raw Messages, [4] Search, [5] Search, and [6] Raw Messages. The main search bar contains the query 'Processor Name IS NOT null'. Below the search bar, there are buttons for 'Load', 'Save', and 'Clear All'. The 'Filter' section is expanded, showing options for 'Event Keyword', 'Event Attribute', and 'CMDB Attribute'. The 'CMDB Attribute' option is selected, and the 'Target' is set to 'DEVICE'. Below this, there is a table with columns for 'Paren', 'Attribute', 'Operator', 'Value', 'Paren', 'Next', and 'Row'. The table contains one row with the following values: '+', '-', 'Processor Name', 'IS NOT', 'null', '+', '-', 'AND', '↓', '+', '-'. At the bottom of the filter section, there are buttons for 'Apply & Run', 'Apply', and 'Cancel'.

Create Under Analytics as well as under CMDB

Execute Save Report from Analytics as well as under CMDB

The screenshot shows the FortiSIEM Analytics interface with a list of reports. The search bar contains the query 'Process Name IS NOT Null'. Below the search bar, there are buttons for 'Apply & Run', 'Apply', and 'Cancel'. The 'Saved Results' section is expanded, showing a list of reports. The 'CMDB Reports' section is highlighted, and a list of reports is displayed. The reports are: Server OS Distribution, Server Inventory, Server Hardware: Processor, Windows Installed Patches, Server Hardware: Memory and Storage, Windows Installed Software, Windows Installed Software Distribution, Windows Auto Running Services, Windows Auto Stopped Services, Windows Manual Running Services, and Windows Manual Stopped Services.

Analytics – Display Conditions

Limit The Search Results – Similar To SQL HAVING Command.

Display Conditions

Paren	Attribute	Operator	Value	Paren	Next	Row
+ -	COUNT(Matched Events)	>=	5	+ -	AND	+ -

Apply & Run Apply Cancel

Search - Last 10 Minutes

Chart for COUNT(Matched Events)

Reporting IP	Event Name	COUNT(Matched Events)
192.168.10.2	TCP/UDP IPv4 connections created by a process	5
192.168.19.1	System uptime for a device	5
192.168.19.65	IPsec/WebVPN AAA user authentication successful	5
192.168.19.65	IPsec/WebVPN AAA local user authentication success	5
192.168.19.65	Appliance admin user authentication succeeded	5
192.168.19.65	Free system memory stats for a device	5
192.168.19.65	System uptime for a device	5
192.168.20.100	System uptime for a device	5
192.168.26.7	Ping Statistics	5
192.168.26.7	System uptime for a device	5

Group By and Display Fields

Attribute	Order	Display As	Row	Move
Reporting IP			+ -	↑ ↓
Event Type			+ -	↑ ↓
SUM(Sent Bytes)			+ -	↑ ↓
COUNT(Matched Events)			+ -	↑ ↓

Display Conditions

Paren	Attribute	Operator	Value	Paren	Next	Row
+ -	SUM(Sent Bytes)	>=	500	+ -	AND	+ -
+ -	COUNT(Matched Events)	>	3	+ -	AND	+ -

Apply & Run Apply Cancel

Event Name	SUM(sentBytes)	COUNT(Matched Events)
Permitted traffic flow ended	442.02 KB	4
Permitted traffic flow started	4.3 KB	11

Analytics – Nested Searches

Nested search addresses a range of analytical questions such as:

- Show me all users with password a change within the last 2 days and no subsequent logins.
- Users with 20 failed logins and a Successful login.
- All devices that have not reported events within the last hour.

Realtime correlation engine can detect similar activity, but Nested searching supports queries on historical data.

The screenshot shows a search configuration interface. At the top, a search bar contains the query: `Event Type = win-security-4722 AND Target User NOT IN Target User: Password Changes La`. Below the search bar are buttons for `Load`, `Save`, and `Clear All`. The main configuration area is titled `Filter` and has three radio button options: `Event Keyword`, `Event Attribute` (which is selected), and `CMDB Attribute`. Under `Event Attribute`, there is a table with columns: `Paren`, `Attribute`, `Operator`, `Value`, `Paren`, `Next`, and `Row`. The table contains two rows:

Paren	Attribute	Operator	Value	Paren	Next	Row
<input type="checkbox"/>	Event Type	=	win-security-4722	<input type="checkbox"/>	AND	<input type="checkbox"/>
<input type="checkbox"/>	Target User	NOT IN	Target User: Password Changes La:	<input type="checkbox"/>	AND	<input type="checkbox"/>

A red arrow points from a red-bordered box labeled `Nested Query` to the `Value` field of the second row. Below the table are three radio button options: `Real Time`, `Relative` (selected), and `Absolute`. The `Relative` option is set to `Last 1 Hour`. Below that are `Nested Time Range` options: `Relative` (selected) and `Absolute`. The `Relative` option is set to `Last 2 Hours`. At the bottom right are buttons for `Apply & Run`, `Apply`, and `Cancel`.

Analytics – Search Archive Without Restoration First

Query online or offline events data without restoration first.

- Reduces time to query archive.
- Reduces requirement for larger online event storage.
- Improves search experience.

Filter

Event Keyword

Event Attribute

CMDB Attribute

Time Range

Real Time Relative Last

Absolute

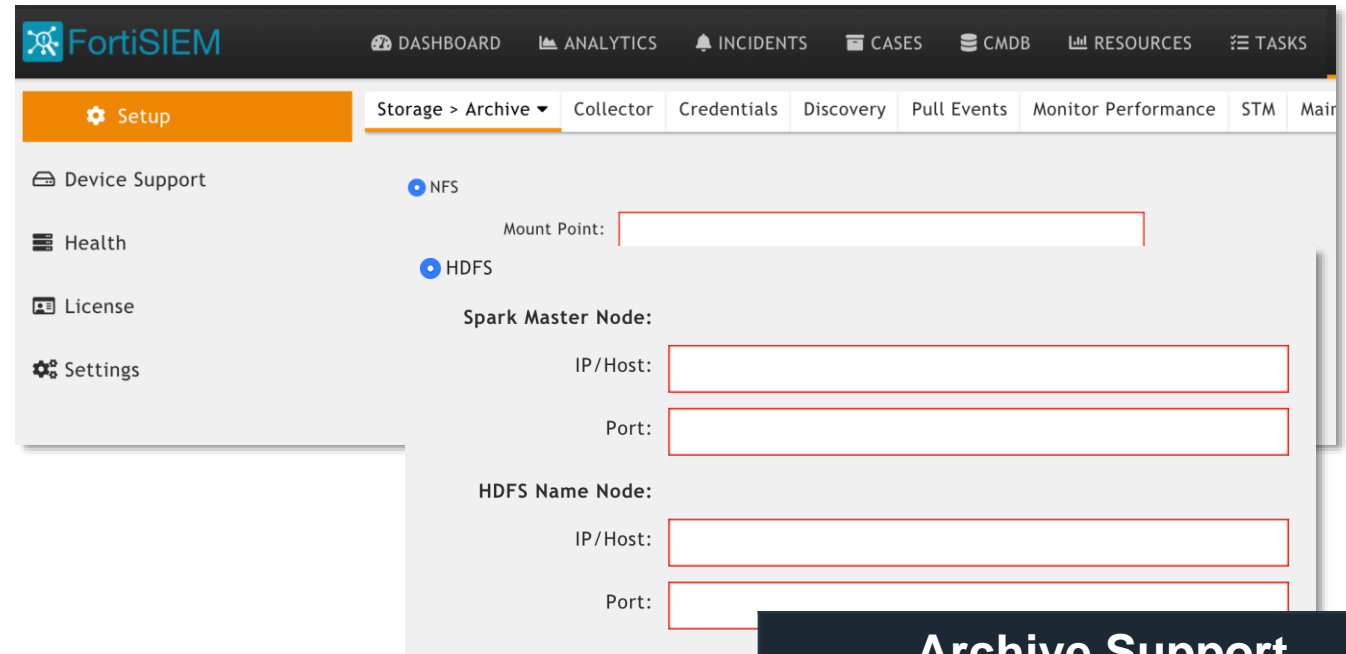
Event Source Online Archive

Events Archive – Archive Destination Setting From GUI

Archiving events allows for scalable and cost effective storage of event Data.

Expanded Archive Destination

- FortiSIEM event DB to NFS
- FortiSIEM ES to NFS
- FortiSIEM ES to HDFS with SPARK

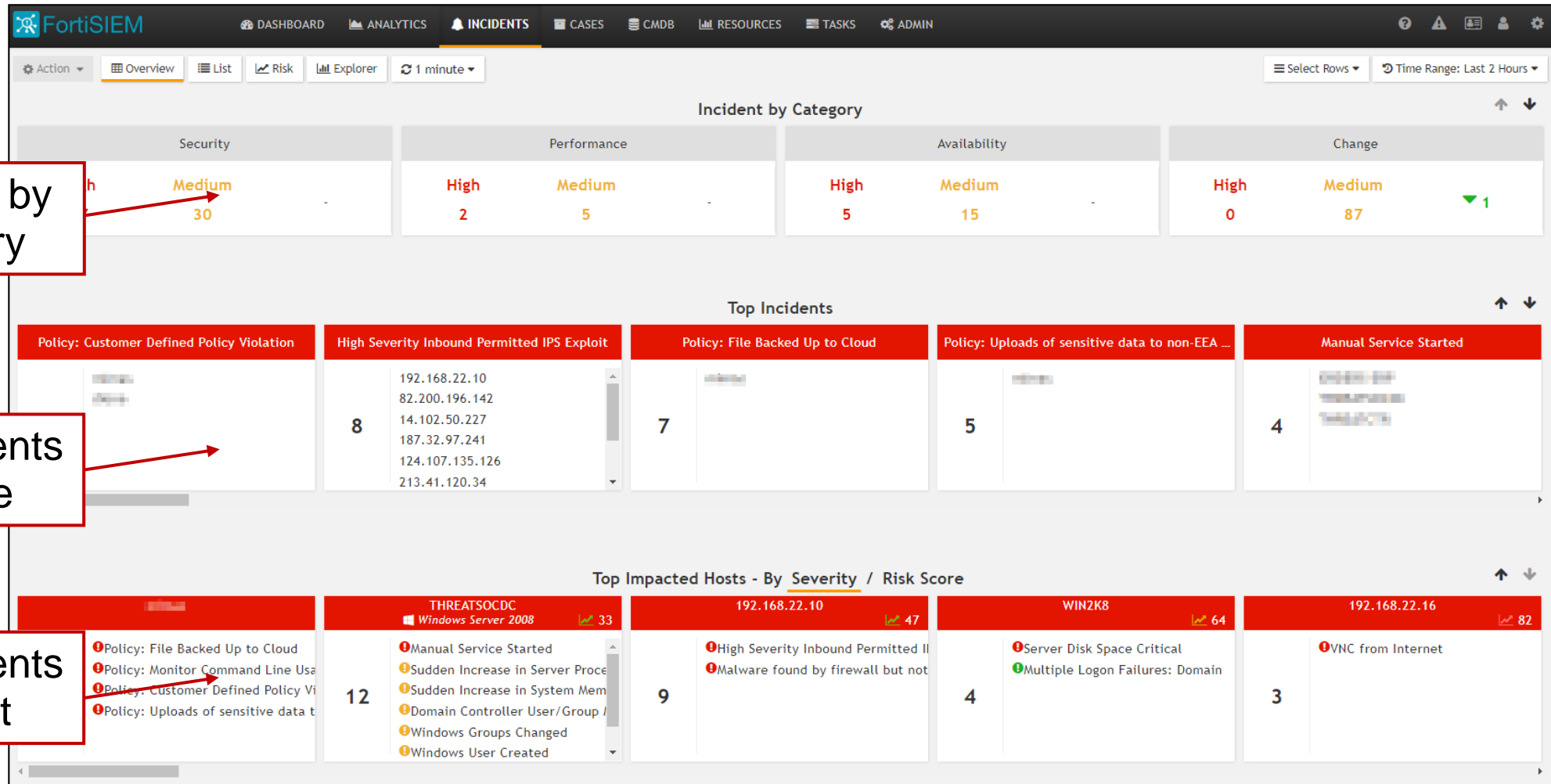


Archive Support	
Online	Archive
NFS	NFS
ElasticSearch	NFS NEW
ElasticSearch	HDFS NEW

Incidents & Cases Management

Incident Views – Summary Dashboard

At-A-Glance View Of Triggered Incidents

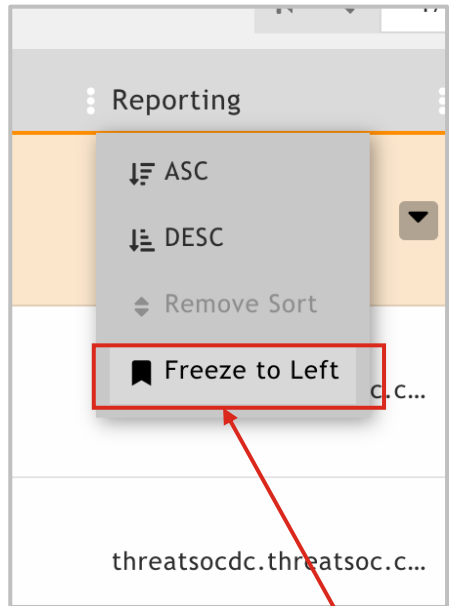


Incidents by Category

Top Incidents by Type

Top Incidents by Host

Incident Views – List by Time (Incident Column Freeze)

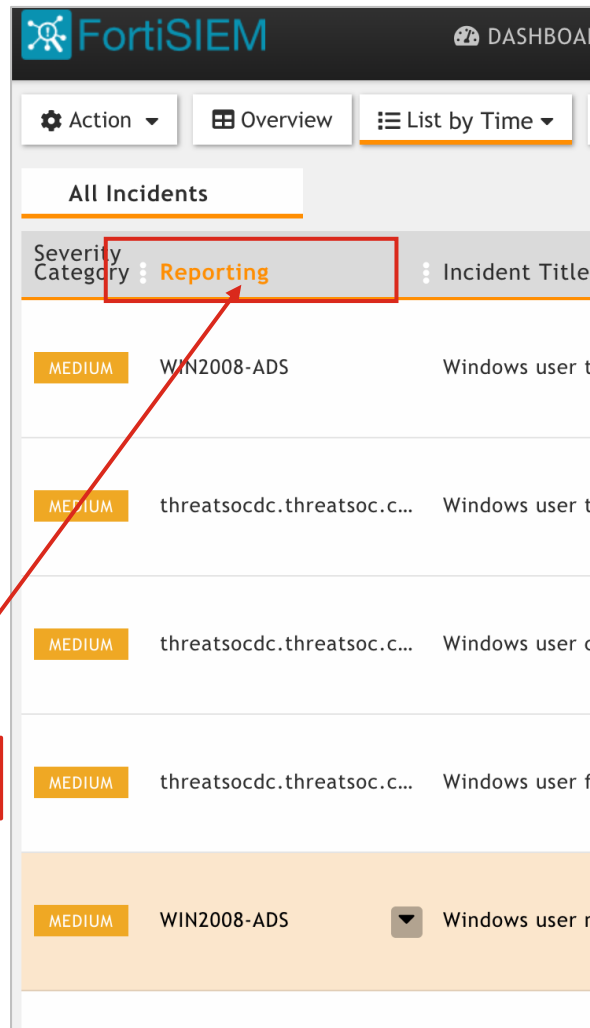


Reporting

- ASC
- DESC
- Remove Sort
- Freeze to Left**

threatsocdc.threatsoc.c...

Freeze a Column



FortiSIEM DASHBOARD

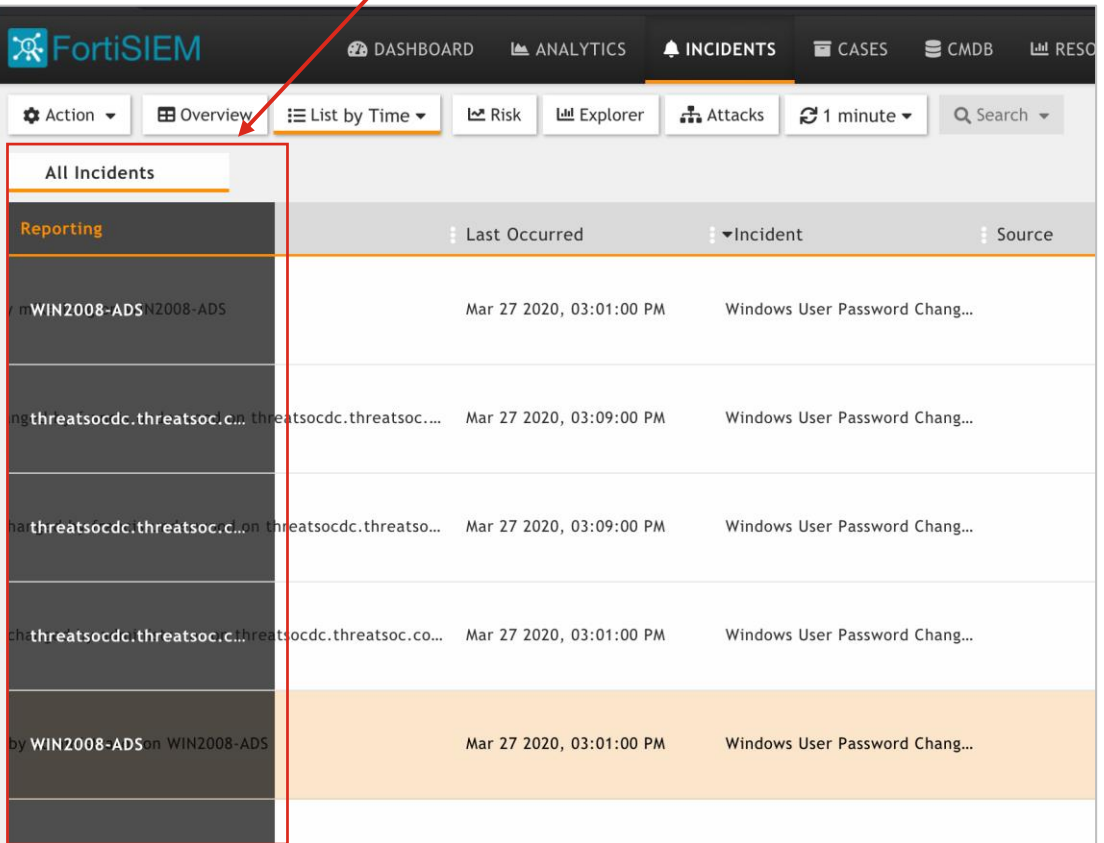
Action Overview **List by Time**

All Incidents

Severity Category: **Reporting** Incident Title

Severity	Incident Title
MEDIUM	WIN2008-ADS Windows user t
MEDIUM	threatsocdc.threatsoc.c... Windows user t
MEDIUM	threatsocdc.threatsoc.c... Windows user c
MEDIUM	threatsocdc.threatsoc.c... Windows user f
MEDIUM	WIN2008-ADS Windows user n

Viewable when scrolled off screen



FortiSIEM DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESO

Action Overview **List by Time** Risk Explorer Attacks 1 minute Search

All Incidents

Reporting Last Occurred Incident Source

Reporting	Last Occurred	Incident	Source
WIN2008-ADS	Mar 27 2020, 03:01:00 PM	Windows User Password Chang...	
WIN2008-ADS	Mar 27 2020, 03:09:00 PM	Windows User Password Chang...	
WIN2008-ADS	Mar 27 2020, 03:01:00 PM	Windows User Password Chang...	
WIN2008-ADS	Mar 27 2020, 03:01:00 PM	Windows User Password Chang...	
WIN2008-ADS	Mar 27 2020, 03:01:00 PM	Windows User Password Chang...	

Incident Views – List by Time (Incident Title)

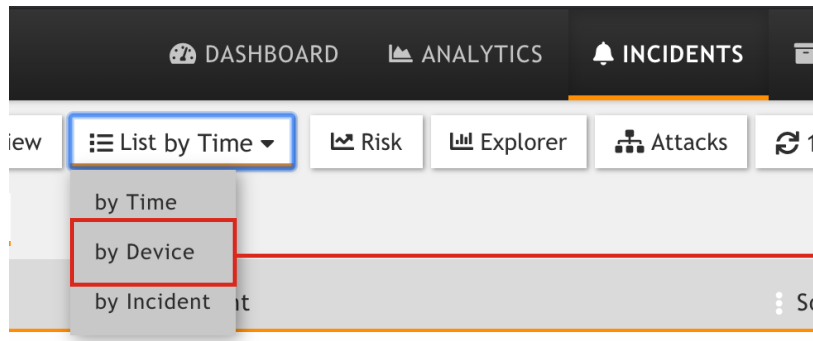
The screenshot shows the FortiSIEM interface with the 'INCIDENTS' tab selected. The 'List by Time' view is active. A single incident is displayed with the following details:

Severity Category	Reporting	Incident	Source	Target	Detail	Last Occurred
MEDIUM	FG240D3913800441	Successful VPN Logon From Outside My Country	85.243.247.32	User: eve.dropper		Mar 27 2020,

The screenshot shows the FortiSIEM interface with the 'INCIDENTS' tab selected. The 'List by Time' view is active. A list of incidents is displayed with the following details:

Severity Category	Reporting	Incident Title	Detail	Last Occurred
HIGH	FG240D3913800441	High Severity Inbound Permitted IPS Exploit FortiGate-ips-signature-15995 from 114.36.65...	Component Event Type: FortiGate-ips-signat... Signature Id: 15995 Triggered Event Count: 6	Mar 27 2020, 04:10
MEDIUM	FG240D3913800441	Excessive End User Mail from 192.168.88.16	Triggered Event Count: 43	Mar 27 2020, 04:24
MEDIUM	FG240D3913800441	Successful VPN login from eve.dropper at IP 85.243.247.32 from outside my country		Mar 27 2020, 04:21
MEDIUM	FG240D3913800441	9 login failures for user from 112.163.191.79 on network device FG240D3913800441	Triggered Event Count: 9	Mar 27 2020, 04:22
HIGH	FG240D3913800441	VNC from Internet 185.56.80.120 to 192.168.22.16		Mar 27 2020, 04:12
MEDIUM	FG240D3913800441	Excessive End User DNS Queries from 192.168.22.11	Triggered Event Count: 541	Mar 27 2020, 04:22
HIGH	FG240D3913800441	High Severity Inbound Permitted IPS Exploit FortiGate-ips-signature-15995 from 187.32.97...	Component Event Type: FortiGate-ips-signat... Signature Id: 15995 Triggered Event Count: 6	Mar 27 2020, 04:18

Incident Views – List by Device



Grouped By Device and Count

The screenshot shows the main incident view. At the top, there's a navigation bar with 'DASHBOARD', 'ANALYTICS', 'INCIDENTS', 'CASES', 'CMDB', 'RESOURCES', 'TASKS', and 'ADMIN'. Below it, a 'View' dropdown menu is open, showing options: 'Action', 'Overview', 'List by Device', 'Risk', 'Explorer', 'Attacks', and '1 minute'. The 'List by Device' option is highlighted. Below the navigation bar, there's a table titled 'Top Impacted Devices' with columns for device names and counts. Below the table, there's a section titled 'Incidents for WIN2008-ADS' with a table of incident details.

Device	Count	Device	Count	Device	Count	Device	Count				
WIN2008-ADS	(33)	threatsocdc.threatsoc.com	(28)	192.168.22.10	(8)	BOB-PC	(8)	42.83.201.2	(7)	2900xl.threatsoc.com	(4)
FG240D3913800441	(4)	FGT_Edge	(4)	10.10.50.13	(3)	192.168.1.124	(3)	192.168.18.2	(3)	192.168.22.16	(3)
85.243.247.32	(3)	AD	(3)	SJ-Main-Cat6500	(3)	WIN2K8	(3)	ibmaix	(3)	intranet.fortilabs.org	(3)

Severity Category	Reporting	Incident	Source	Target	Last Occurred	Incident Status
MEDIUM	WIN2008-ADS	Windows User Created		WIN2008-ADS User: mike.long Target User: testuser Domain: ACCELOPS	Mar 27 2020, 04:01:00 PM	Active
MEDIUM	WIN2008-ADS	Windows User Password Changed		WIN2008-ADS User: administrator Target User: mike.long Domain: ACCELOPS	Mar 27 2020, 04:01:00 PM	Active
MEDIUM	WIN2008-ADS	Windows User Password Changed		WIN2008-ADS User: mike.long Target User: testuser Domain: ACCELOPS	Mar 27 2020, 04:01:00 PM	Active
MEDIUM	WIN2008-ADS	Windows User Account Properties Changed		WIN2008-ADS User: administrator Target User: mike.long Domain: ACCELOPS	Mar 27 2020, 04:01:00 PM	Active

Incident Views – List by Incident

Navigation menu with options: DASHBOARD, ANALYTICS, INCIDENTS. A dropdown menu is open under 'List by Time', showing options: by Time, by Device, and by Incident. The 'by Incident' option is highlighted with a red box.

Grouped By Incident and Count

Incident view interface showing 'Top Impacted Incidents' and a detailed table for 'Incidents for Windows User Added to Groups'.

Top Impacted Incidents

Windows Groups Changed (18)	No logs from a device (17)	Windows User Added to Grou... (12)	Successful VPN Logon from o... (10)	High Severity Inbound Permitt... (9)	Multiple Logon Failures: Server (7)
Windows User Created (6)	IPS detected network scan fro... (6)	Multiple Logon Failures: Net D... (6)	Windows User Account Proper... (5)	Windows User Password Chang... (5)	Windows User Account Enabled (5)
User added to Remote Desko... (4)	User added to Administrator ... (4)	Sudden User Location Change (4)	Excessive End User DNS Queries (4)	Windows PowerShell Opening ... (4)	Manual Service started (4)

Incidents for Windows User Added to Groups

Severity Category	Reporting	Incident	Source	Target	Last Occurred	Incident Status
MEDIUM	WIN2008-ADS	Windows User Added to Groups		WIN2008-ADS User: mike.long Target User: cn=testuser CN=User: CN=Users DC=accelop: DC=accelops DC=ne: DC=net Target User Group: Administrators Domain: ACCELOPS	Mar 27 2020, 05:01:00 PM	Active
MEDIUM	WIN2008-ADS	Windows User Added to Groups		WIN2008-ADS User: mike.long Target User: cn=testuser CN=User: CN=Users DC=accelop: DC=accelops DC=ne: DC=net Target User Group: Domain Admins Domain: ACCELOPS	Mar 27 2020, 05:01:00 PM	Active

Incident Views – Risk Dashboard

User And Entity Risk View

The screenshot displays the FortiSIEM Risk Dashboard. At the top, the navigation bar includes 'DASHBOARD', 'ANALYTICS', 'INCIDENTS', 'CASES', 'CMDDB', 'RESOURCES', 'TASKS', and 'ADMIN'. The main section is titled 'Entities by Risk' and shows a summary bar with the following data: 73 Devices, 20 Users, 6 High Risk, 4 Medium Risk, and 83 Low Risk. Below this, there are tabs for 'Overview', 'List', 'Risk', and 'Explorer'. The 'Risk' tab is active, showing a 'Current Risk' of 83 and a '1 day Trend' graph. The 'Incidents in Last 1 day' section lists several incidents, including 'Multiple Admin Login Failures: Net Device', 'Sudden Decrease in Reported Events From A Host', and 'Sudden Increase In Firewall Connections'. The 'Risk Score Trend' graph shows a score of 83 over a 24-hour period. The 'Incident Timeline' section lists several incidents with their details, including IP addresses, severity levels, and incident counts. A context menu is open over one of the incidents, showing actions such as 'Clear Incident', 'Create Event Dropping Rule', 'Create Ticket', 'Disable Rule', 'Edit Comment', 'Edit Rule', 'Edit Rule Exception', 'Export Incident', 'Notify via Email', 'Remediate Incident', 'Resolve Incident', 'Run External Integration...', and 'Show in Incident List View'. The bottom of the dashboard shows the Fortinet logo, copyright information, organization name, user name, and version number.

Summary Bar

Device Risk Score

Click to Action

Device Risk Timeline

Incident Views – Explorer

Instinct Exploring Incidents

FortiSIEM DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES TASKS ADMIN

Action Overview List Risk Explorer Attacks 1 minute Category: 4 Selected Status: Active Time Range: Last 2 Hours

Incident Trend by Severity

Search Groups

Incident	Host	IP	User
Windows Groups Changed 18	[Empty] 68	[Empty] 71	[Empty] 82
No logs from a device 17	win2008-ads 33	192.168.22.10 8	administrator 34
Windows User Added to Groups 12	threatsocdc.threatsoc.com 28	42.83.201.2 7	francis.underwood 20
Successful VPN Logon from outside my co... 10	bob-pc 8	10.10.100.1 4	mike.long 19
High Severity Inbound Permitted IPS Exploit 9	fg240d3913800441 4	192.168.0.10 4	users 10
Multiple Logon Failures: Server 7	2900xl.threatsoc.com 4	192.168.3.1 4	don.freeman 8

Related Incidents 1/9 167

Severity Category	Last Occurred	Incident	Subcategory	Source	Target	Detail	Incident Status	Resolution
MEDIUM	Mar 27 2020, 08:44:30 PM	Excessive End User DNS Queries	Command and Control	172.16.0.1		Triggered Event Count...	Active	Open
MEDIUM	Mar 27 2020, 08:44:30 PM	Excessive Denied DNS Queries	Command and Control	192.168.200.12		Triggered Event Count...	Active	Open
HIGH	Mar 27 2020, 08:44:30 PM	System Archive Directory Unavailable	FortiSIEM				Active	Open
MEDIUM	Mar 27 2020, 08:44:30 PM	Excessive End User DNS Queries	Command and Control	192.168.18.2		Triggered Event Count...	Active	Open
MEDIUM	Mar 27 2020, 08:44:30 PM	Excessive End User Mail	Exfiltration	192.168.88.16		Triggered Event Count...	Active	Open
MEDIUM	Mar 27 2020, 08:44:30 PM	Heavy ICMP Ping sweep	Discovery	172.16.22.137		Triggered Event Count...	Active	Open
MEDIUM	Mar 27 2020, 08:44:00 PM	Excessive End User Mail To Unauthori...	Exfiltration	192.168.88.16			Active	Open

Incident Views – Attacks

MITRE ATT&CK Stages Are Mapped To The Rule Subcategory.

The screenshot displays the FortiSIEM interface for incident views. The top navigation bar includes 'FortiSIEM', 'DASHBOARD', 'ANALYTICS', 'INCIDENTS', 'CASES', 'CMDB', 'RESOURCES', 'TASKS', and 'ADMIN'. The main view is 'Attacks' with a refresh rate of '1 minute'. Filters include 'Status: Active' and 'Time Range: Last 1 Day'. A search bar shows '(133/133)' results.

Device	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10.1.206.154							1			30		
10.1.206.150										18		
[Empty]	2						16					
FAP320C-default										9		
HOST-1.1.1.1	2	1	2							3		
10.1.206.192										5		
FGT51E	2						1					
10.1.213.141							1			2		

Command and Control Incidents for HOST-1.1.1.1:

Severity Category	Last Occurred	Incident	Subcategory	Source	Target	Detail	Incident Status	Resolution
MEDIUM	Jul 20 2020, 06:55:00 PM	Dynamically generated host name: m...	Command and Control	1.1.1.1	www.xyz.com	Domain Name Entrop...	Active	Open
MEDIUM	Jul 20 2020, 06:55:00 PM	Dynamically generated host name: m...	Command and Control	1.1.1.1	www.abcd.com	Domain Name Entrop...	Active	Open

Incident Visualization – Anomalous User Login Behavior

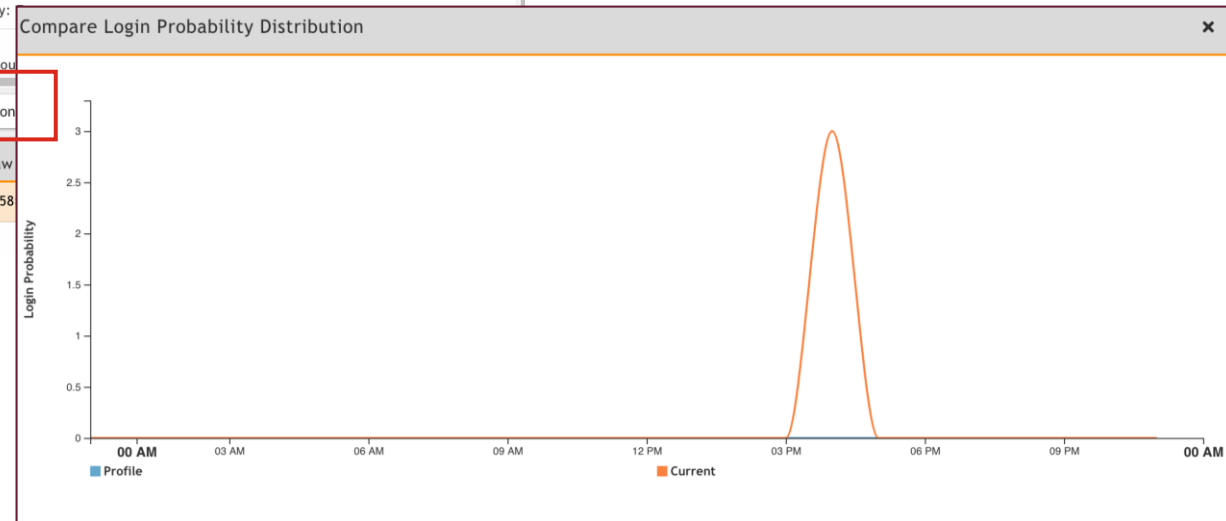
Anomalous User Login Behavior

The screenshot shows the FortiSIEM interface with the 'INCIDENTS' tab selected. A table lists several incidents, with the first one highlighted in orange. Below the table, the 'Events' tab is active, showing a list of events. A red box highlights the 'Compare Distribution' button, and a red arrow points from it to the 'Change in user login distribution pattern' event in the table below.

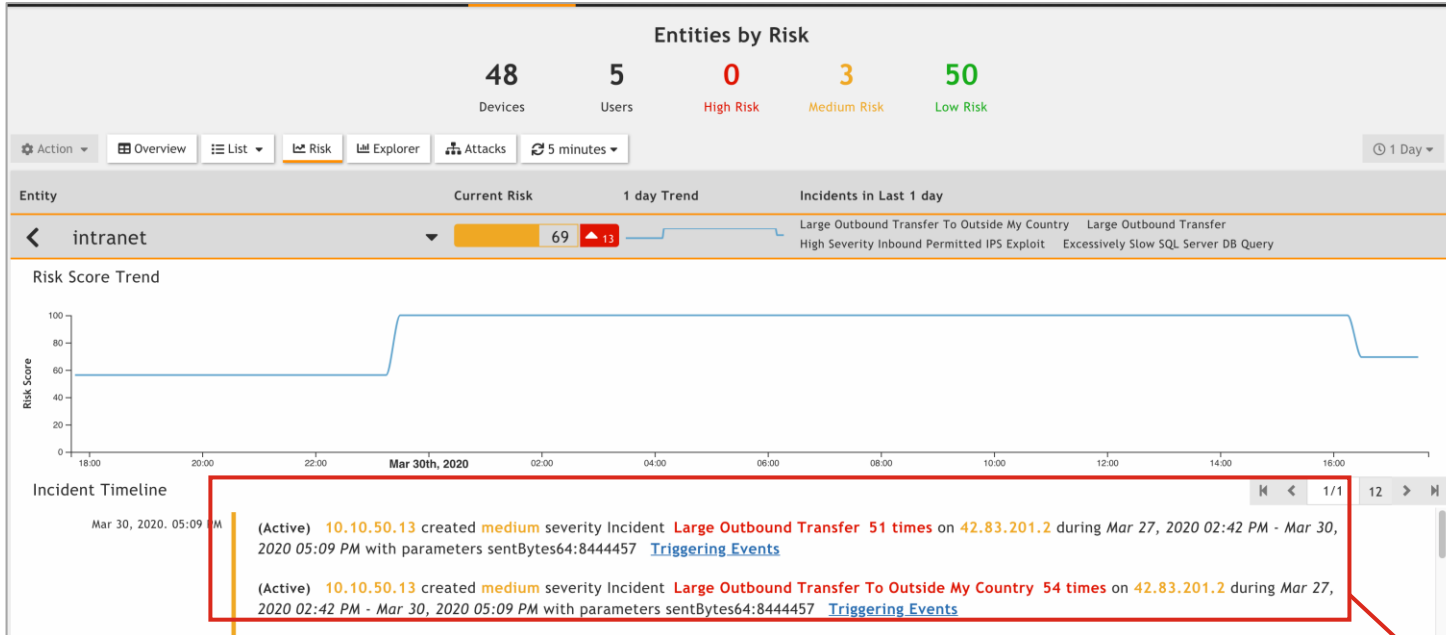
Severity Category	Reporting	Incident	Source	Target	Last Occurred	Incident Status
MEDIUM	fsm-va.fortipoc.test	Sudden User Login Pattern Change		User: operator BOB-PC	Mar 30 2020, 12:07:00 PM	Active
HIGH	fsm-va.fortipoc.test	Sudden User Location Change	Source City: Houston Source State: Texas Source Country: United States	User: don.freeman Destination City: London Destination State: England Destination Country: United Kingdom	Mar 30 2020, 12:01:00 PM	Active
HIGH	fsm-va.fortipoc.test	Sudden User Location Change	Source City: London Source State: England Source Country: United Kingdom	User: don.freeman Destination City: Houston Destination State: Texas Destination Country: United States	Mar 30 2020, 12:01:00 PM	Active
HIGH	fsm-va.fortipoc.test	Sudden User Location Change	Source City: Houston Source State: Texas Source Country: United States	User: don.freeman Destination City: Paris Destination State: Ile-de-France Destination Country:	Mar 30 2020, 11:01:00 AM	Active
HIGH	fsm-va.fortipoc.test	Sudden User Location Change	Source City: Paris Source State: Ile-de-France Source Country:	User: don.freeman Destination City: Houston Destination State: Texas Destination Country: United States	Mar 30 2020, 11:01:00 AM	Active

Event Receive Time	Event Name	Computer	User	Destination Host Name	Raw
Mar 30 2020, 12:06:02 PM	Change in user login distribution pattern		operator	BOB-PC	<158

Incidents triggered by Machine Learning have to be quickly understood



Incident Noise Reduction – Risk Score Filter



Some Rules in particular environments need to trigger, but not contribute to the Risk score

Edit Risk Filter

Include
 Exclude

Groups:

- Rules

Rules:

- large out
- Large Outbound Transfer
- Large Outbound Transfer To Outside My Country

Selections:

- Large Outbound Transfer
- Large Outbound Transfer To Outside My Country

Incident Noise Reduction – IPS False Positive Check

FortiSIEM can check if the IPS target is vulnerable to the attack and update the incident state.

- Reduces Incident False Positive Rate
- Provides more immediate context to the Analyst regarding the Threat.
- Integrates with FortiGuard to lookup the FortiGate IPS attack ID to CVE.

The screenshot displays the FortiSIEM interface for an incident. The incident is titled "High Severity Outbound Permitted IPS Exploit" with a severity of "HIGH". The source IP is 172.16.6.6. The incident title includes a FortiGate IPS signature ID: "High Severity IPS Exploit FortiGate-ips-signature-39577 from 172.16.6.6 to 10.0.1.11". The resolution is "True Positive" and the ticket ID is "924550". The incident status is "Active". The incident comments section contains a note about a CVE lookup for CVE-2014-6321 and a case creation for 924550. A red box highlights the "Change Incident Status", "Add Context from FortiGuard", and "Create a Case" actions, with arrows pointing to the "Resolution" and "Ticket ID" fields.

Case Management – Action Timeline

Tracking All Activities Of Case & Incidents

Cases help manage multiple incidents and analyst activity.

- Understand MTTR values
- New case timeline view
- Improved Case search and view
- Pivot between Incidents, Cases, notes and events.

The screenshot displays the FortiSIEM interface for Case Management. At the top, there is a navigation bar with tabs for DASHBOARD, ANALYTICS, INCIDENTS, CASES, CMDB, RESOURCES, TASKS, and ADMIN. Below the navigation bar, a summary row shows statistics: 0 New, 0 Assigned, 1 High, 0 Overdue, 0 Late, 1 Closed, and 38m MTTR. A table below this row lists cases with columns for Elapsed, State, Priority, Ticket ID, Summary, Incident ID, Assignee, Creator, Resolution Time, and Due Date. One case is highlighted: 2% Elapsed, Closed State, High Priority, Ticket ID 924550, Summary 'High Severity Outbound Permitted IPS Exploit', Incident ID 1003, Assignee admin, Creator admin <ad..., Resolution Time 38m 9s, and Due Date Mar 31. Below the table, there is a 'Details' section with a dropdown menu set to 'Action History > Timeline'. A timeline view shows incident and case actions. Incident actions include 'User admin Integration triggered - Raise severity to HIGH; Set resolution to TRUE positive;' and 'User admin created Case 924550'. Case actions include 'User Super/admin created Case', 'User Super/admin added Notes', and 'User admin Integration triggered - Raise severity to...'.

See all actions by timeline

Refactored the Screen
MTTR indicator,
Linking to the Incidents,
Case History, Evidence

Case Management – Evidence

The screenshot shows the FortiSIEM interface for Case Management. At the top, a navigation bar includes 'FortiSIEM' and menu items: DASHBOARD, ANALYTICS, INCIDENTS, CASES (highlighted), CMDB, RESOURCES, TASKS, and ADMIN. Below the navigation bar, a summary row displays statistics: 0 New, 0 Assigned, 1 High, 0 Overdue, 0 Late, 1 Closed, and 38m MTTR. A table below shows a list of cases with columns: Elapsed, State, Priority, Ticket ID, Summary, Incident ID, Assignee, Creator, Resolution Time, Due Date, Creation Date, and Closed Date. The first row is highlighted in orange and contains: 2%, Closed, High, 924550, High Severity Outbound Permitted IPS Exploit, 1003, admin, admin <ad..., 38m 9s, Mar 31 2020, 07:58:03 PM, Mar 30 2020, 08:58:03 PM, Mar 30 2020, 08:36:03 PM. Below the table, a tabbed interface shows 'Evidence' selected. The 'Evidence' tab is divided into 'Attachment' and 'Triggering Event'. The 'Attachment' tab is empty. The 'Triggering Event' tab shows event details: Incident ID: 1003, Rule Name: High Severity Outbound Permitted IPS Exploit, Sub Pattern: NonCiscoIPSHighSev, and a log entry: <185>date=2010-06-17 time=03:46:02 devname=FGT50B000000000 device_id=FGT50B0000000000 log_id=0419016384 type=ips subtype=signature pri=alert fwver=040002 severity=low car... Two red boxes with arrows point from a central text box to the 'Evidence' tab and the 'Triggering Event' content.

Evidence TAB containing Incident Events & Files

Elapsed	State	Priority	Ticket ID	Summary	Incident ID	Assignee	Creator	Resolution Time	Due Date	Creation Date	Closed Date
2 %	Closed	High	924550	High Severity Outbound Permitted IPS Exploit	1003	admin	admin <ad...	38m 9s	Mar 31 2020, 07:58:03 PM	Mar 30 2020, 08:58:03 PM	Mar 30 2020, 08:36:03 PM

Detail | Action History | **Evidence** | Auto expand

Attachment | **Triggering Event** | Wrap Raw Events

Incident ID: 1003 Rule Name: High Severity Outbound Permitted IPS Exploit Sub Pattern: NonCiscoIPSHighSev

<185>date=2010-06-17 time=03:46:02 devname=FGT50B000000000 device_id=FGT50B0000000000 log_id=0419016384 type=ips subtype=signature pri=alert fwver=040002 severity=low car...

FORTINET®

BMW i Motorsport
Official Partner

