Managed Services: Closing the Manpower Gap in Cybersecurity

Klaidas Rimkus

Systems Engineer - Baltics

Fortinet Security Fabric

Broad

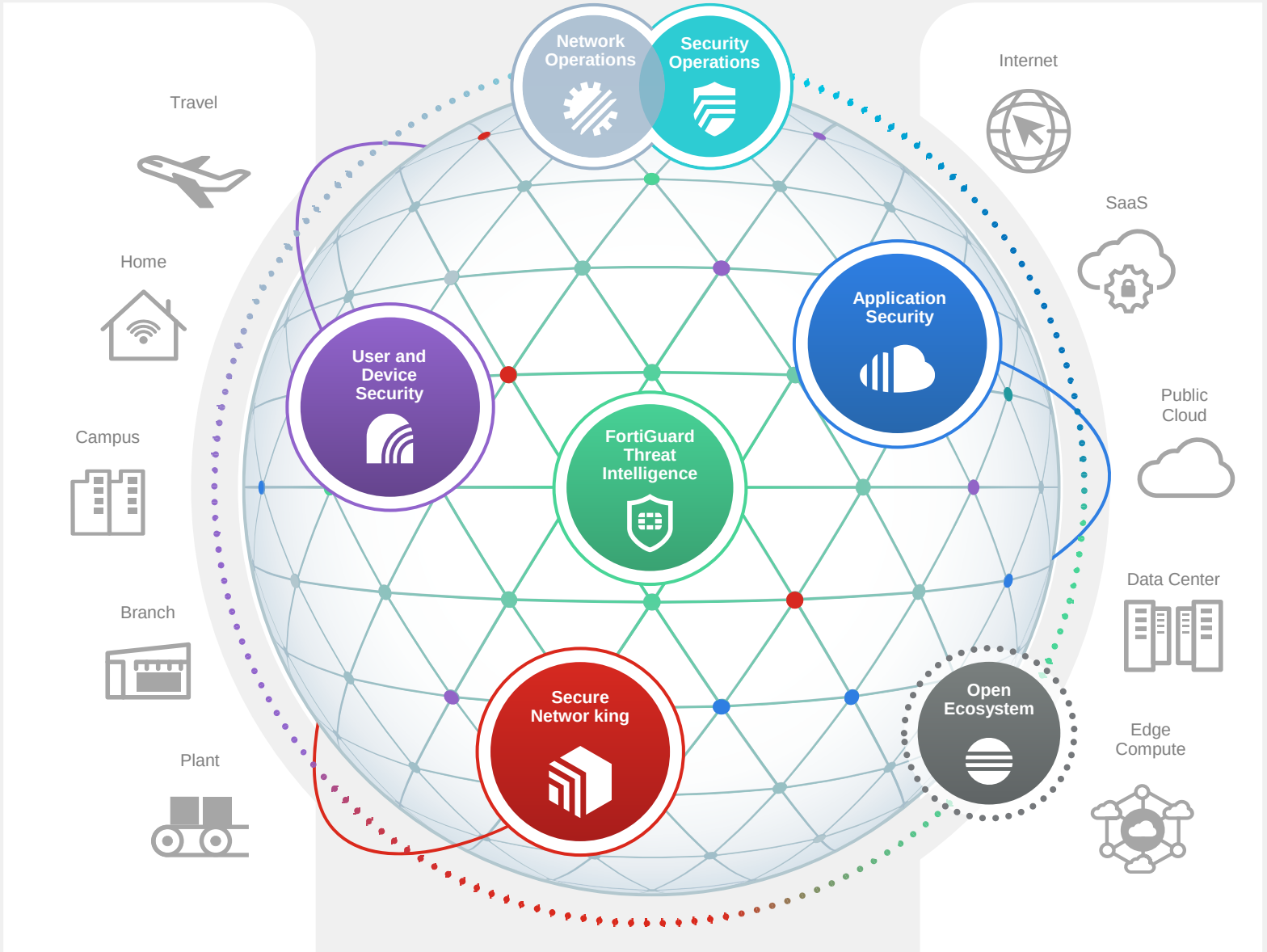
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations



Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiOS
The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiProxy
Enforce internet, compliance and granular application control

FortiIsolator
Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDOS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiMail
Secure mail getaway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

FortiCNF
Offers enterprise-grade protection on Amazon AWS, with inbound and outbound traffic inspection and insights

Zero Trust Access

FortiSASE
Enforce dynamic network access control and network segmentation

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiGuest
Simplified guest access, BYOD, and policy management

FortiPAM
Control & monitoring of elevated & privileged accounts, processes, and critical systems

FortiGuard Threat Intelligence

Powered by FortiGuard Labs

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud
Saas w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage and customize LTE internet access

FNDN
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOp Tools & Script
Fortinet & community-driven

Fabric API Integration
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiRecon
Digital Risk Protection (DRP) for early, actionable warning and fast response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
15% of hardware

FortiCare Premium*
20% of hardware

FortiCare Elite**
25% of hardware

FortiConverter
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

FortiFone
Robust IP Phones w/ HD Audio with centralized management

FortiVoice
Integrated voice, chat, conferencing management, and fax with centralized

FortiCamera
HDTV-quality surveillance cameras for physical safety and security

FortiRecorder
High-performance NVR with AI-powered video management software

False Sense of Security

The Impact from a Lack of Time & Resources is Real

Too Much Noise

41% executives don't feel their security has kept up with digital transformation[1]

Too Many Threats

Misconfigurations will cause 99% of all firewall breaches through 2023[2]

Too Little Talent

Lack of skilled personnel was the #1 factor preventing companies from defending against cyberthreats[3]

Data points sources

[1] "Cybersecurity Solutions for a Riskier World," ThoughtLab, accessed August 18, 2022.

[2] "2022 Cyberthreat Defense Report," CyberEdge Group, accessed August 18, 2022.

[3] "The State of Cybersecurity and Third-Party Remote Access Risk," Ponemon Institute, July 20, 2022.

How do I know what services & products my team needs?

Incident Response and Readiness

Assess

IRR Assessment
Ransomware Readiness Assessment
SOC Assessment “**New**”
Compromise Assessment “**New**”

Improve

Incident Response Plans
Playbook Development
OT & IT Tabletop Exercises
SOC Development Services “**Future**”

Respond

Ransomware Attacks
Business Email Compromise
Web Application Attacks
Advanced Persistent Threats (APT)

Fast-Track Your SOC with FortiGuard SOCaaS

Simply add-on SOCaaS to any FortiGate device — a cost-effective way to rapidly deliver managed security services to your end customers with operational efficiency and flexibility

Monitor, Detect, and Investigate

Let Fortinet monitor and investigate FortiGate alerts and notifications 24x7, only notifying you when something is important and needs attention.

Take Your Time Back

Respond

Fortinet security experts will notify teams in as little as 15 minutes and provide insights into what happened, why it happened, and what steps to take to remediate the incident.

Act When Needed

Improve

A cloud-based portal with intuitive dashboards, on-demand reports, and quarterly meetings with Fortinet Security Experts allowing users to drill into incidents, report up the chain, improve their security posture, and reduce alert noise.

Maximize Investments

Monitor, Detect and Investigate

MITRE Mapped Detection Use Cases

Compromised hosts, Intrusion, Unauthorized Access, Lateral Movement, Botnet / C&C and more

Cyber Kill Chain

SOC Use Cases for IT

PREPARATION — AVAILABLE · BETA · COMING SOON

FortiGate Best Practices

Use cases which detect misconfigurations, gaps in visibility & detection, and logging problems.

Use Case Description	Fabric Device	Log Source	Availability
Device Logging Problems	FortiGate	Not applicable	✓
Device misconfigurations (Tuning Preventive Controls)	FortiGate	UTM logs	✓
Device Logging Problems	Additional Fabric Devices	Fabric Device Logs	✗
Device misconfigurations (Tuning Preventive Controls)	Additional Fabric Devices	Fabric Device Logs	✗

RECONNAISSANCE — AVAILABLE · BETA · COMING SOON

Reconnaissance

Use cases which detect techniques actively or passively gathering information.

MITRE ID	Use Case Description	Fabric Device Log Source	Fabric Device Logs & FortiGuard Service	Availability
T1595	Active Scanning	FortiGate	Traffic, IPS	✓
		FortiDeceptor	Scan Detection	✗
T1598	Phishing for Information	FortiGate	Email Filtering	✗

NOTE: Use Case coverage evolves rapidly, please consult the latest coverage published in FortiGuard at https://www.fortiguard.com/socaas/

4

SOC Use Cases for OT

SOC Use Cases for detecting threats against Industrial Control System networks.

DELIVERY — AVAILABLE · BETA · COMING SOON

Initial Access

Use cases which detect compromised websites, applications, remote access, services or phishing attacks.

MITRE ID	Use Case Description	Fabric Device Log Source	Fabric Device Logs & FortiGuard Service	Availability
T0819	Exploit Public-Facing Applications	FortiGate	IPS IIS (Industrial Security Services)	✗
T0866	Exploitation of Remote Service	FortiGate	IPS IIS (Industrial Security Services)	✗
T0886	Remote Services	FortiGate	Traffic and Application Control	✗

EXPLOITATION — AVAILABLE · BETA · COMING SOON

Discovery

Use cases which detect when attackers are attempting to gain knowledge about system and internal networks.

MITRE ID	Use Case Description	Fabric Device Log Source	Fabric Device Logs & FortiGuard Service	Availability
T0846	Remote System Discovery	FortiGate	Traffic and Application Control	✗

14

SOC Use Cases for OT

SOC Use Cases for detecting threats against Industrial Control System networks.

INSTALLATION — AVAILABLE · BETA · COMING SOON

Lateral Movement

Use cases which detect attempts to gain unauthorized access to systems on a network from a presumably trusted source on the same network.

MITRE ID	Use Case Description	Fabric Device Log Source	Fabric Device Logs & FortiGuard Service	Availability
T0866	Exploitation of Remote Service	FortiGate	IPS IIS (Industrial Security Services)	✗
T0891	Hardcoded Credentials	FortiGate	Traffic and Webfilter	✗
T0886	Remote Services	FortiGate	Traffic and Application Control	✗

Persistence

Use cases which detect attempts to keep access to systems across restarts, changed credentials, and other interruptions that could cut off adversary access.

MITRE ID	Use Case Description	Fabric Device Log Source	Fabric Device Logs & FortiGuard Service	Availability
T0891	Hardcoded Credentials	FortiGate	Traffic and Webfilter	✗

ORDER INFORMATION

Product	Description	Managed Service SKU
FortiGate	FortiGate SOCaaS Subscription	FC-10-[FortiGate Model]-464-02-DD
	Managed FortiGate Service	FC-10-[FortiGate Model]-660-02-DD
FortiClient Forensic		FCx-10-EMS05-537-01-DD
		FCx-10-EMS05-538-01-DD
		FCx-10-EMS05-539-01-DD

15

Improve

Continuously improve security posture to protect expanded attack surface

QBRs

- Quarterly Business Review
- Security Posture Assessment
- Feedback loop

Service visibility, feedback loop to get most out of the service

Welcome Meeting

- Review setup and identify gaps
- Orientation on the service
- One week after onboarding

Part of onboarding to ensure customer success

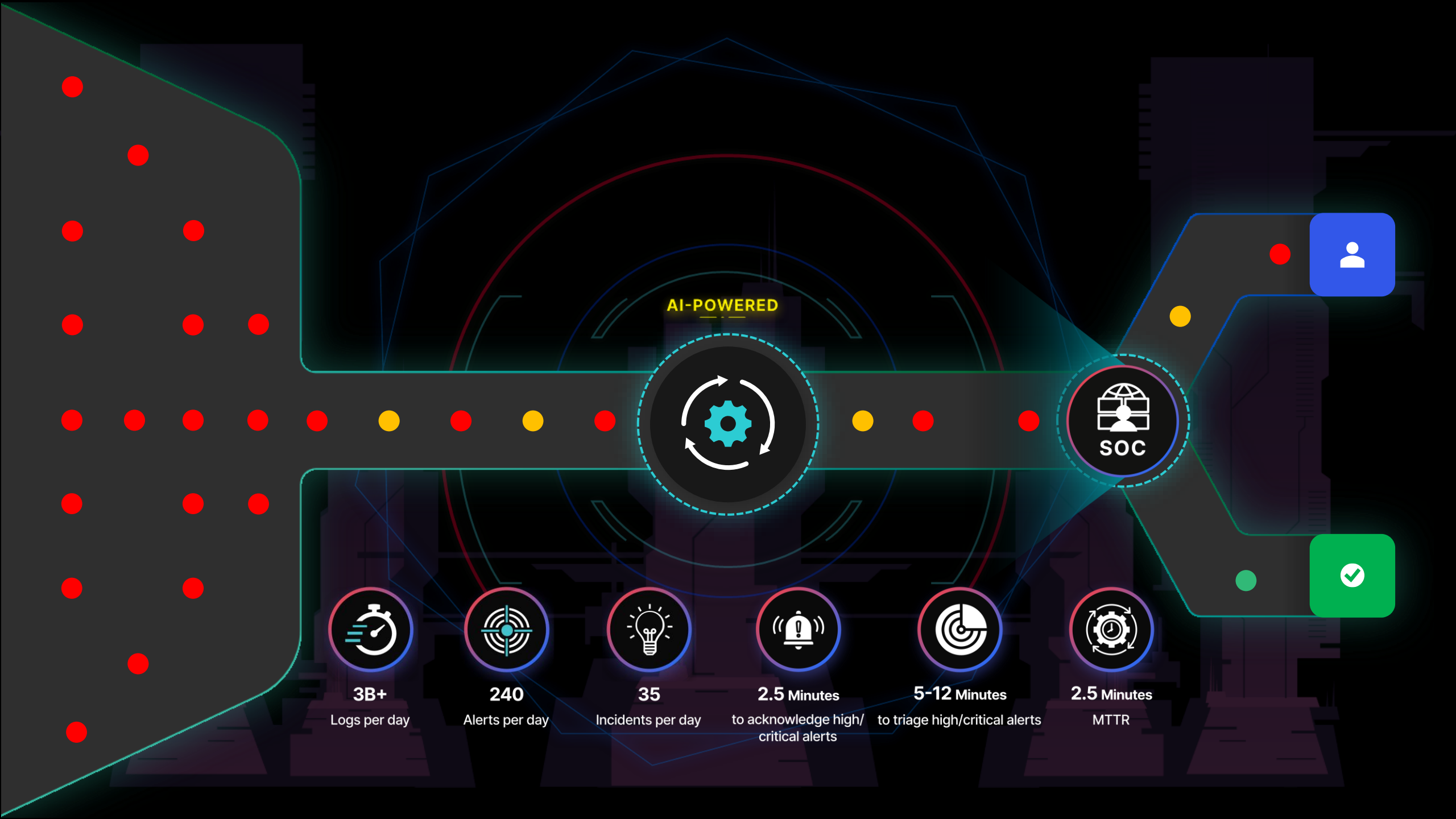
Daily Interaction

- Service Portal Interaction
- Service Request
- Urgent Assistance

Chat, email and phone call to ensure smooth communication

Monitor, Detect and Investigate

Technologies and Process

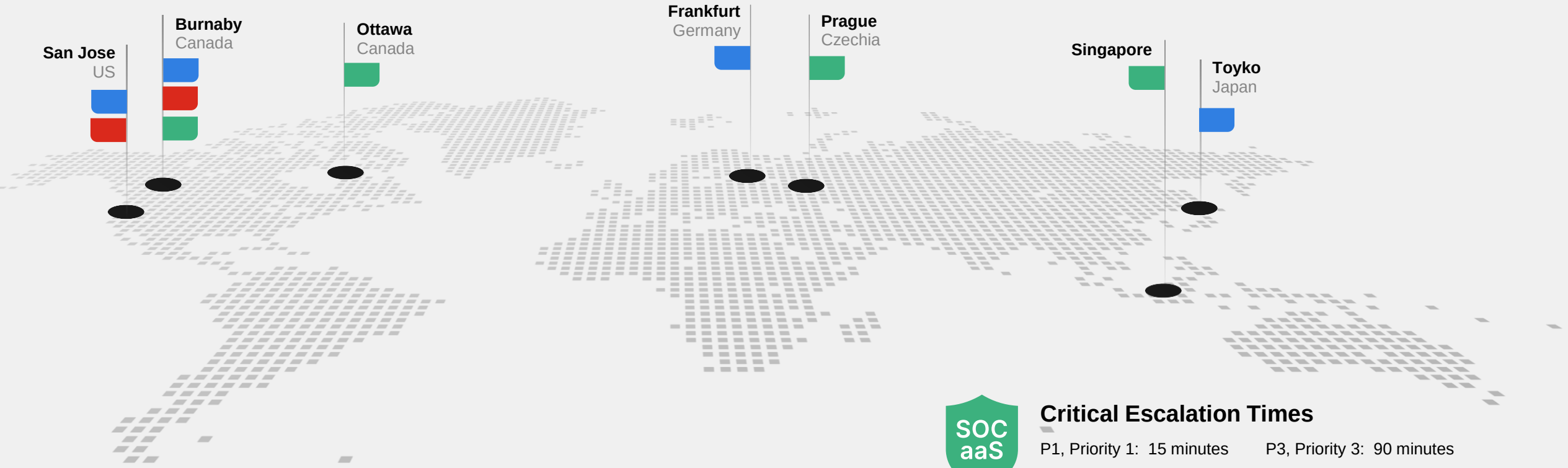

AI-POWERED
SOC
3B+
Logs per day
240
Alerts per day
35
Incidents per day
2.5 Minutes
to acknowledge high/ critical alerts
5-12 Minutes
to triage high/critical alerts
2.5 Minutes
MTTR

Follow The Sun Approach

Global Response Teams

- SOC
- Data Center
- Disaster Recover

99.99%	24x7x365	Unlimited	FortiGate & Security Fabric logs	Fast & Simple
Availability	Service Hours	Log Capacity	Ingest Log Data	Onboarding



SOC aaS

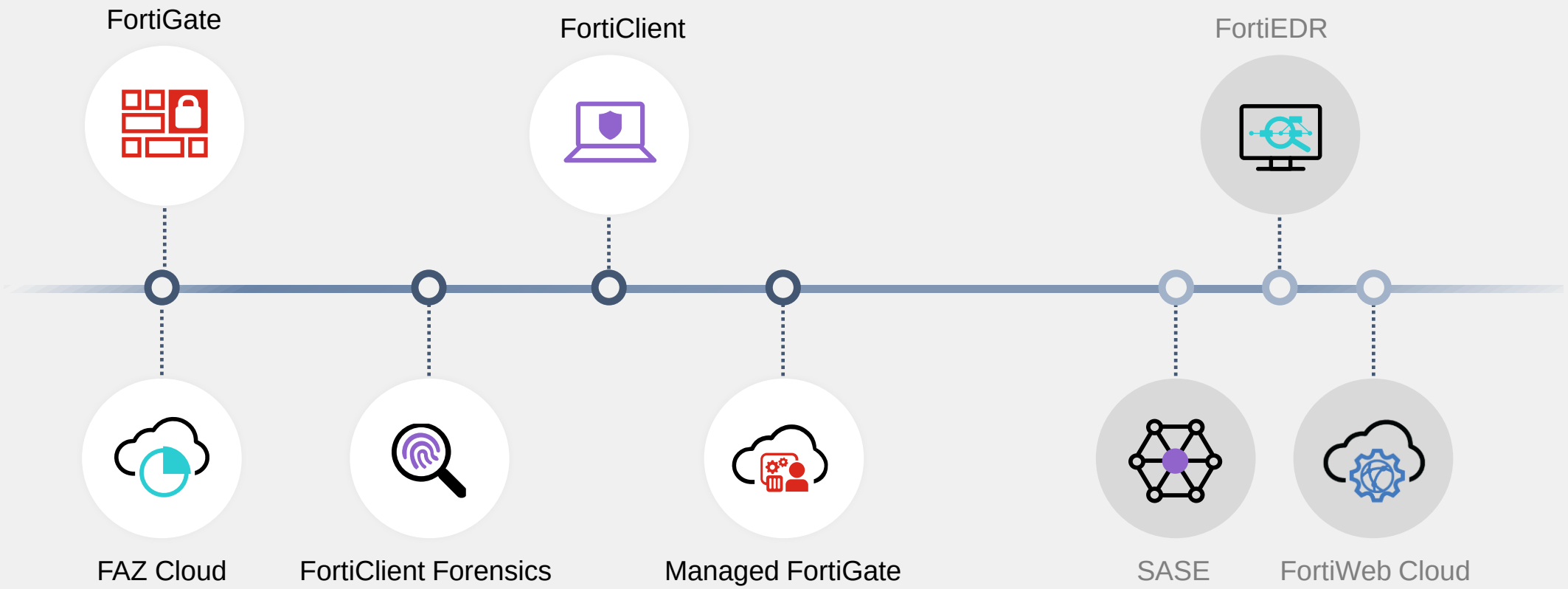
Critical Escalation Times

P1, Priority 1: 15 minutes
P2, Priority 2: 45 minutes
P3, Priority 3: 90 minutes
P4, Priority 4: 6 hours

AICPA SOC

SOC 2 TYPE II COMPLIANT

Product and Service Integration



SLA Matrix

Response time by severity

CRITICAL (P1, Priority 1) **Escalation Time** Phone: 15 min. Email: 15 min.

HIGH (P2, Priority 2) **Escalation Time** Phone: 45 min. Email: 90 min.

MEDIUM (P3, Priority 3) **Escalation Time** Phone: NA Email: 90 min.

LOW (P4, Priority 4) **Escalation Time** Phone: N/A. Email: 6 hours

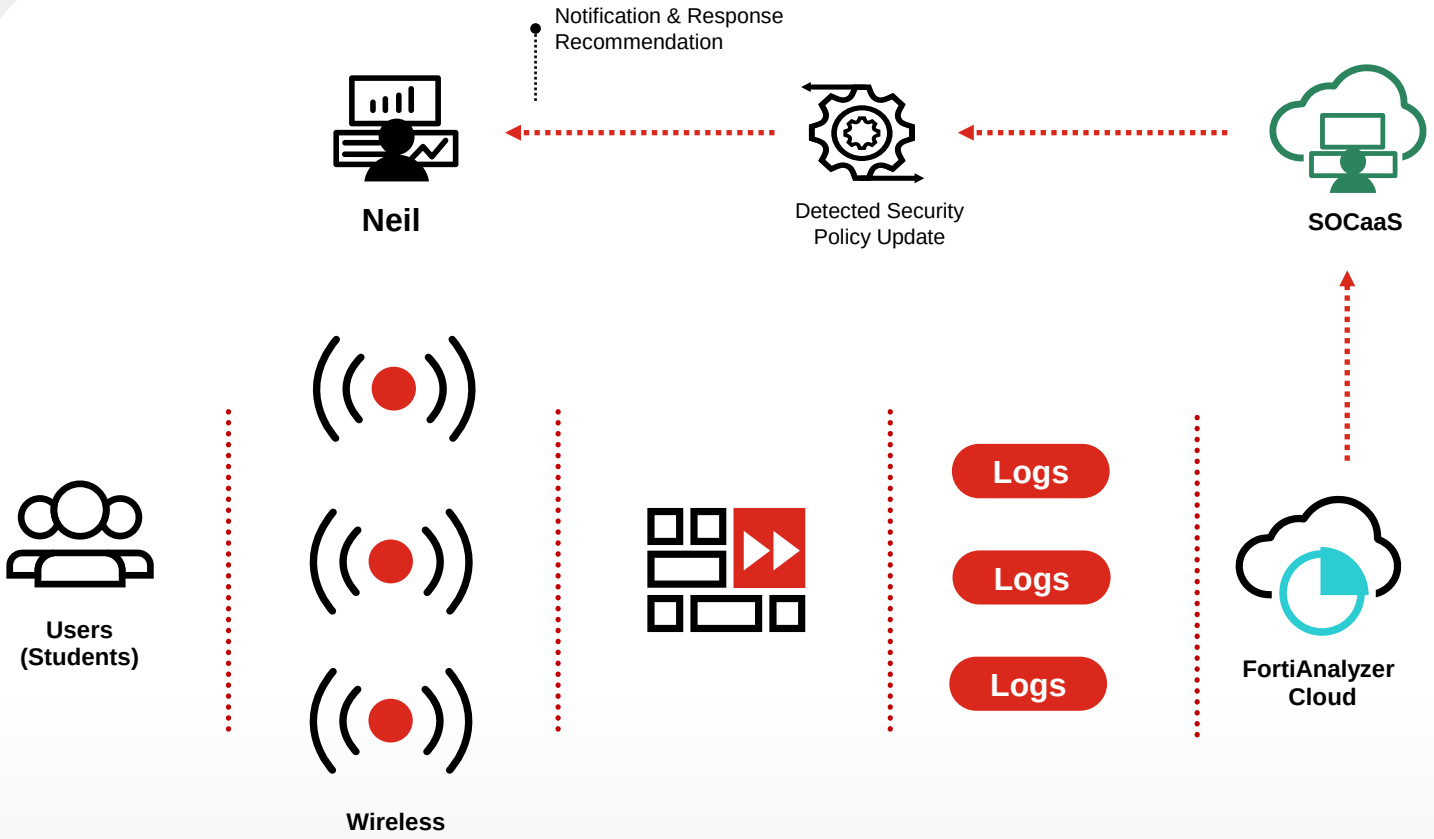
Solution Architecture

Customer Success

Security
- FortiGuard SOC-as-a-Service (SOCaaS)
- FortiGuard MDR
- FortiGuard IOC and Outbreak Detection Services

Network
- FortiGate
- FortiAnalyzer

LAN
- FortiAP

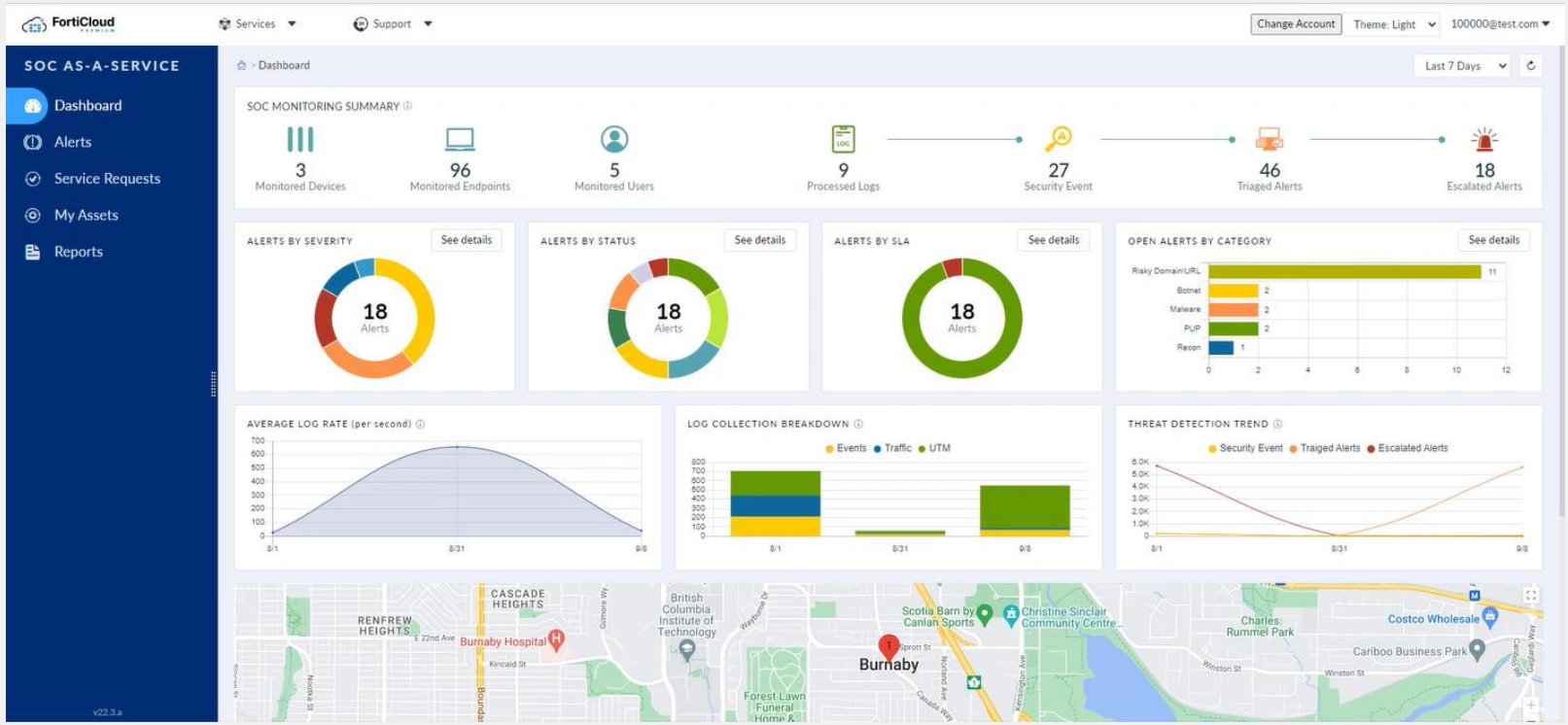


Fortinet’s Turnkey SOCaaS Solution – FortiGuard SOCaaS

Rapidly deliver analyst support, alert monitoring and triage, and recurring services to your businesses

Take Back Your Time

- Supplement FortiGate log and alert monitoring and triage with Fortinet security experts
- Reduce employee burnout and recapture critical work cycles
- 24 x 7 global coverage with live human experts

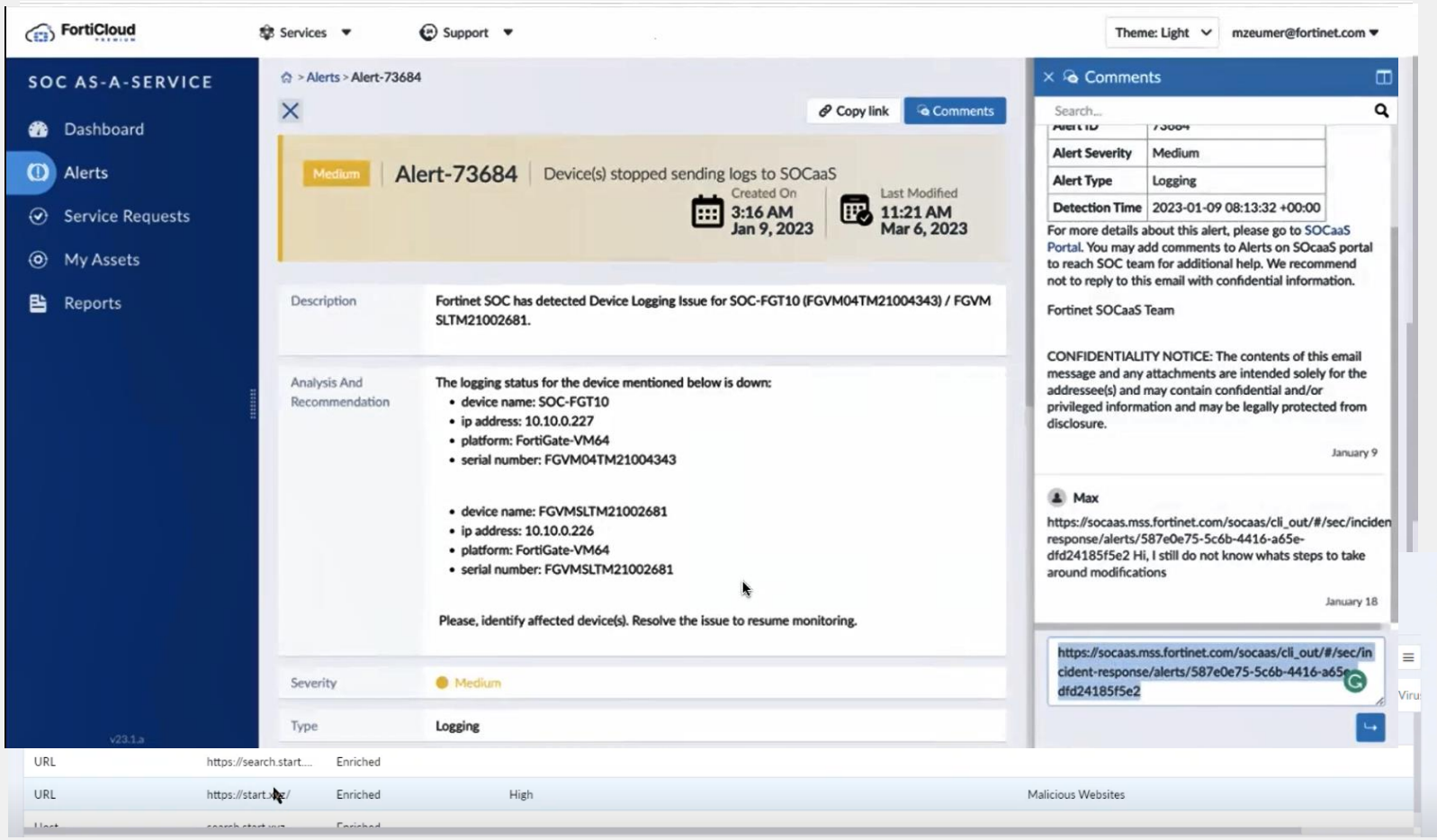


Fortinet’s Turnkey SOCaaS Solution – FortiGuard SOCaaS

Rapidly deliver analyst support, alert monitoring and triage, and recurring services to your businesses

Act When Needed

- Escalation of confirmed issues in as little as 15min
- Step-by-step instruction on:
  - What has happened
  - Why
  - Impact
  - Steps to remediate
- Live support for any questions

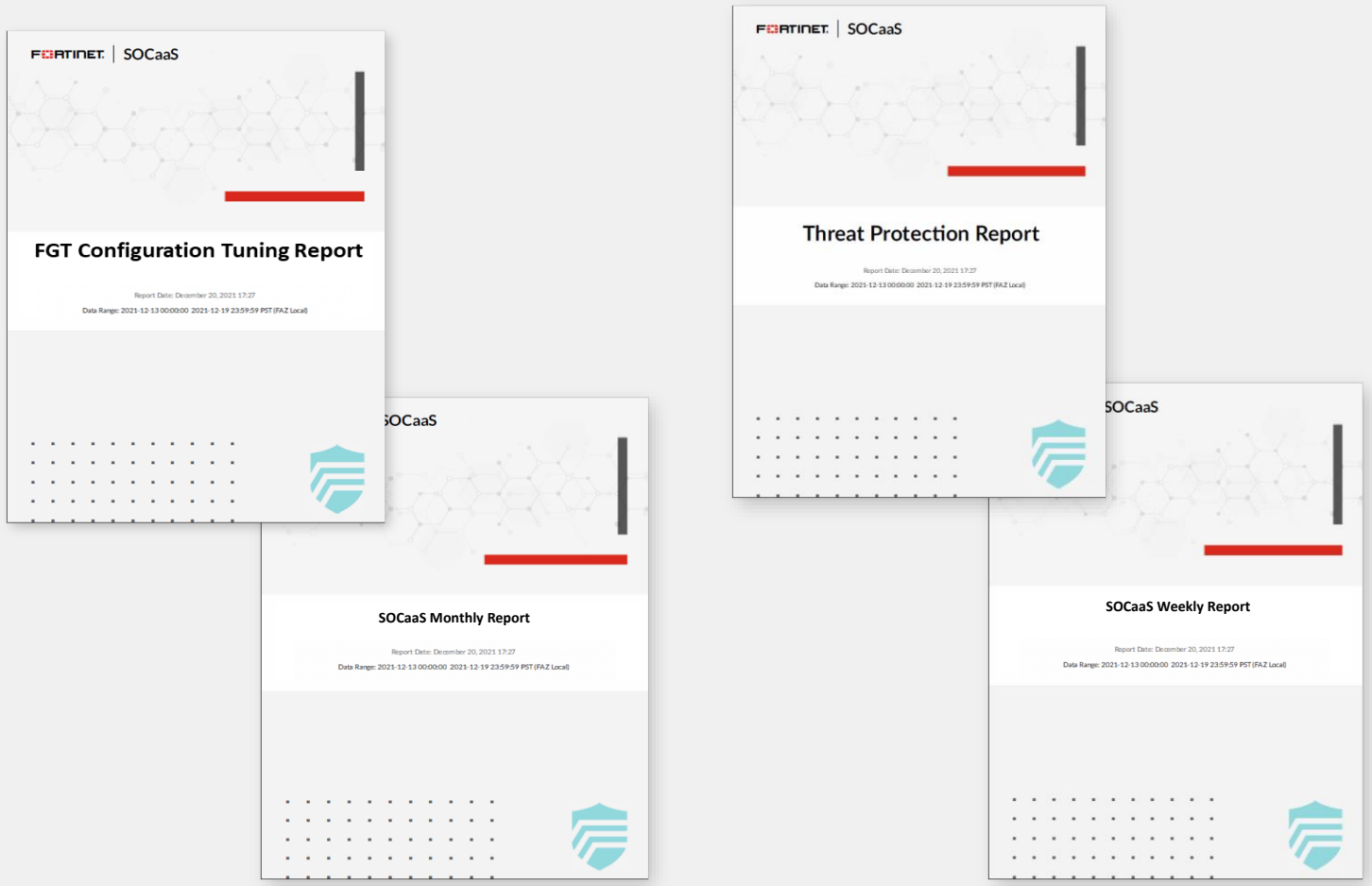


On-demand Reporting – Get the most from your investments

Pre-built reports & templates

Maximize Investments

- Fully customizable out-of-the-box reporting to highlight areas of improvement and progress
- Quarterly meetings with Fortinet to discuss events, hardening tips, and overall improvement



FGT Configuration Report

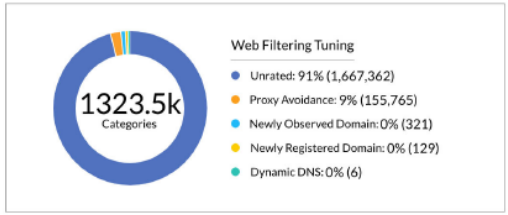
Understand what profiles are being hit the most and where areas of improvement are

SECURITY PROFILES : WEB FILTER

This table shows the web queries to malicious/suspicious domains that are not blocked. It shows the URLs or hostnames, and the corresponding FortiGate names and policy numbers.

Below Charts includes websites from following categories(catdesc) :- Malicious Websites, Phishing, Spam URLs, Newly Observed Domain, Newly Registered Domain, Dynamic DNS, Proxy Avoidance, Unrated

WEB FILTERING TUNING SUMMARY



WEB FILTERING TUNING CATEGORIES

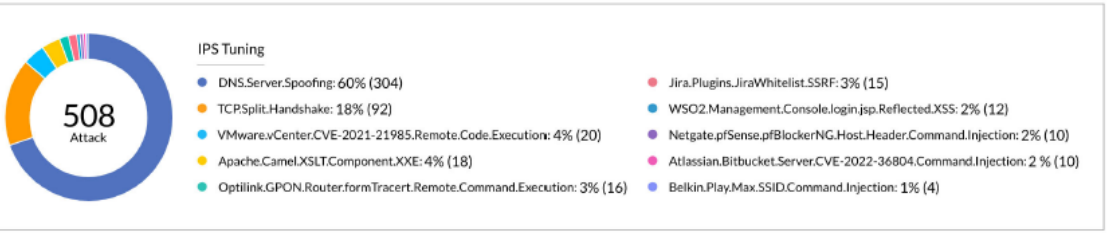
#	Device (Security Profile)	Categories	Hits	% of Total
1	[redacted]	Unrated	1664302	91
		Newly Observed Domain	39	0
		Newly Registered Domain	13	0
2	[redacted]	Proxy Avoidance	155763	8
		Unrated	11574	0
		Newly Observed Domain	144	0
		Newly Registered Domain	62	0
3	[redacted]	Unrated	1162	0
		Newly Observed Domain	102	0
4	[redacted]	Unrated	324	0
		Newly Observed Domain	7	0
		Proxy Avoidance	2	0

SECURITY PROFILES : INTRUSION PREVENTATION

This table shows the attacks observed in IPS logs that are not blocked, the signatures that are hit, and the corresponding FortiGate names, policy ids, Security Profile and total hits.

Below chart are included only Critical, High and Medium Intrusions.

IPS TUNING SUMMARY



IPS SIGNATURE TUNING DETAILS

#	Device (Security Profile)	Attack (Action)	Hits	% of Total
1	[redacted]	DNS.Server.Spoofing(detected)	304	60
		TCP.Split.Handshake(detected)	91	18
2	[redacted]	Apache.Camel.XSLT.Component.XXE(detected)	8	2
		Jira.Plugins.JiraWhitelist.SSRF(detected)	8	2
		Optilink.GPON.Router.formTracert.Remote. Command. Execution(detected)	8	2
		VMware.vCenter.CVE-2021-21985.Remote. Code.Execution(detected)	4	0
		Atlassian.Bitbucket.Server.CVE-2022-36804. Command. Injection(detected)	4	0
		Belkin.Play.Max.SSID.Command.Injection(detected)	4	0
		Netgate.pfSense.pfBlockerNG.Host.Header. Command. Injection(detected)	4	0
		WSO2.Management.Console.login.jsp.Reflected. XSS(detected)	4	0

SOCaaS Weekly Report

Easy to keep track of everything that's been or being worked on – keep things organized

ID	TENANT	CREATED ON	RESOLVED DATE	NAME	STATUS	TYPE	SEVERI...	DESCRIPTION	CLOSURE NOTES
								Malware detection in [redacted] Sandbox detected Malware Action = quarantinefailed	
7208	[redacted]	03/11/2022 06:15 PM	03/15/2022 02:44 PM	Malware Activity detected from [redacted]	Closed (Risk Accepted)	Malware	High	File Name = C:\Users\[redacted]\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\LocalState\Files\S0\28\Attachments\Ваш счет пополнен. - DzMNa37mTnCxobr4jeFDRqcguByVAhdSEl86wfkIZYPW1UJKiX[2639].xhtml	BYOD PC has been ban from [redacted] network
7109	[redacted]	03/02/2022 06:18 PM	03/15/2022 02:19 PM	Malware Activity detected from [redacted]	Closed (Risk Accepted)	Malware	High	Malware detected on host [redacted]	ran full malware scan, no malware detected.
7068	[redacted]	02/23/2022 09:12 PM	03/15/2022 02:17 PM	Malware Activity detected from [redacted]	Closed (Risk Accepted)	Malware	High	Unhandled malware detections for files in [redacted]	ran full malware scan, no malware detected, PC is clean
6742	[redacted]	01/09/2022 11:18 PM	03/11/2022 10:45 AM	FCT detected unhandled malware from [redacted]	Closed (Risk Accepted)	Malware	High	FCT detected unhandled malware from [redacted]	user was not connected to ems (possibly why the file failed to quarantine) confirmed with user that file is no longer there full av scan results are clean
7274	[redacted]	03/18/2022 06:30 PM	03/21/2022 03:20 PM	Malware Activity detected from [redacted]	Closed (Resolved)	Malware	High	Unhandled malware declared in [redacted]	file was quarantined and removed
7054	[redacted]	02/22/2022 07:54 PM	03/16/2022 10:22 AM	Malware Activity detected from [redacted]	Closed (Resolved)	Malware	High	Quarantine failed for [redacted]	manual scan via EMS came clean, archiving the case.
7275	[redacted]	03/18/2022 07:03 PM	03/21/2022 04:37 PM	High Risk Traffic detected from [redacted]	Closed (Risk Accepted)	High Risk Traffic	Mediu...	CryptoMiner detected on [redacted]	this is FGD one time event
7270	[redacted]	03/18/2022 12:57 AM	03/21/2022 09:14 AM	Malicious Email detected from [redacted]	Closed (Risk Accepted)	Malicious Email	Mediu...	Virus detected in mail from [redacted]	was a test
7259	[redacted]	03/16/2022 04:06 PM	03/22/2022 12:11 PM	High Risk Traffic detected from [redacted]	Closed (Risk Accepted)	High Risk Traffic	Mediu...	Potential dataexfil from [redacted]	was a test
7228	[redacted]	03/14/2022 05:51 PM	03/17/2022 12:15 PM	High Risk App Usage detected from [redacted]	Closed (Risk Accepted)	High Risk App	Mediu...	Tor app detected	The traffic is being blocked by our FW. We are not able to find the owner of this IP.
7198	[redacted]	03/10/2022 11:36 PM	03/15/2022 02:41 PM	Botnet traffic detected to CnC server: [redacted] related to [redacted]	Closed (Risk Accepted)	High Risk Traffic	Mediu...	Fortinet SOC has repeatedly detected Botnet traffic attempts Sunburst from [redacted] to [redacted]	Endpoint Quarantine, ongoing investigation

Differentiators

SOCaaS

One source of truth -
Fortinet Security Fabric

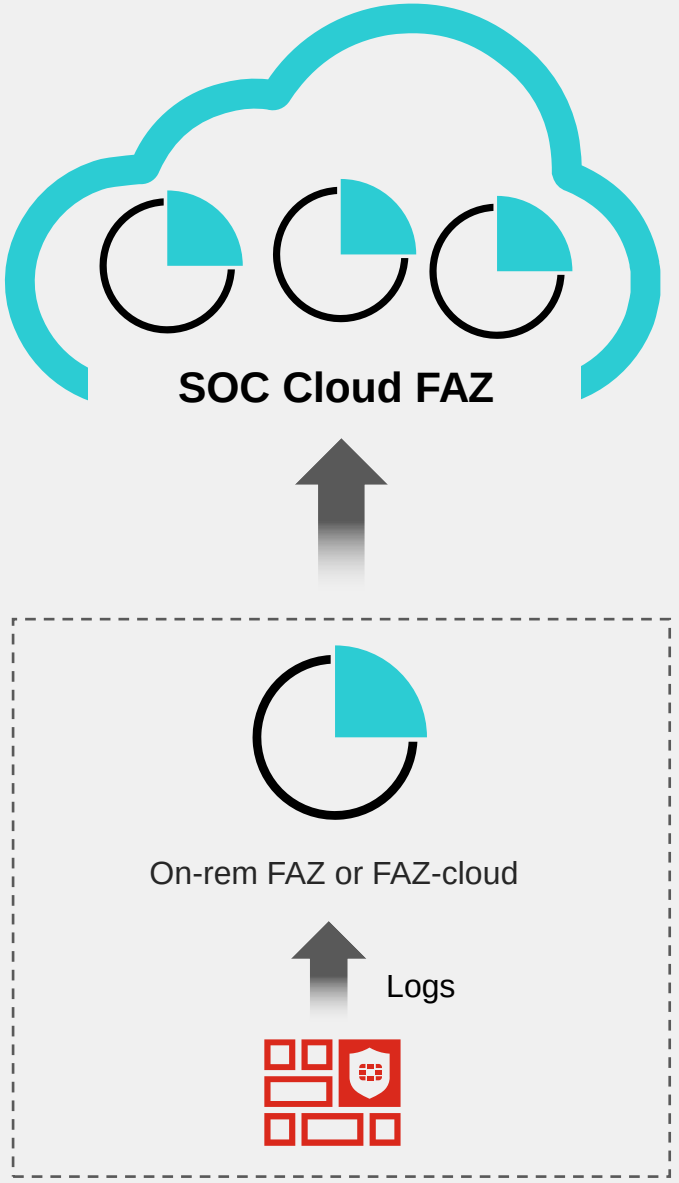
FortiGuard threat intelligence visibility across entire attack chain

Availability of technology and technical resources

Onboarding

Get data into SOC for monitoring

1. **Purchase**
   SKU for each FG
2. **Register**
   license in FortiCare
3. **Onboard**
   from the SOCaaS Portal



Customer Success

Grand View University

Learn what you love and you'll love to learn.

Grand View University

Founded: 1896

Headquarters: Des Moines, IA

Our mission

- Leadership Inspired
- Meaningful Connections
- Transformational Opportunities

Leading the way

Our creative, innovative, hands-on learning style means that no two experiences are the same. It's all about making your education your own. Our theory? Learn what you love and you'll love to learn.

18
Campus Buildings

Servicing Students
2K+

FortiGate Firewall
2 (High-range)
300 APS+
Devices

Headcount of
500+
Employees

Business Drivers for Managed Security Services

Business Driver 1

Cyber insurance requirements

Get ahead of cyber insurance mandates with Managed Detection and Response

Business Driver 2

Too much noise

Due to the log and alert volume it was hard to keep up with our policy updates - driving us to pursue a proactive posture

Business Driver 3

24/7 operations

Costs ranged from the MSP, to the MPLS lines, to the impact of poor performance

Objectives for Managed Security Projects

GRAND VIEW UNIVERSITY

Rapid deployment, partner had a breach

Meet cyber insurance requirements

Breath of coverage and capabilities

Offload security expertise

Charter Schools USA

Charter Schools USA

Founded: Jonathan Hage in 1997

Headquarters: Florida

CSUSA provides world–class educational solutions with:

- An unwavering dedication to student success
- An unyielding commitment to ethical and sound business practices

Providing a choice for our stakeholders that fosters and promotes educational excellence.

Vision

CSUSA will have a dramatic impact on the world's next generation – changing lives and leaving a legacy. Our brand will be the standard by which quality is measured in education.

Values

- Purpose
- Passion
- Integrity
- Grit

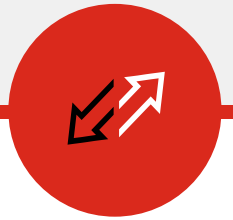
Across 5 States	Servicing Students	FortiGate Firewall	Headcount of
80+	**75K+**	**20+**	**700+**
Schools		Devices	Employees

Objectives for Managed Security Projects

CHARTER SCHOOLS USA

Digital Transformation

Central Management



Optimize Migration

Offload security expertise

How Customers Continue to use SOCaaS

Continue vendor consolidation by taking advantage of Fortinet's Security Fabric Interoperability to synergize tools and simplify operations

Maximize product stack and the next deployment of 100 FortiAP's by working with vendor expert services to gain more out of our investment

Migrate 50 remaining sites to Fortinet's SOC as a service offering to free up time for IT specific activities (helpdesk etc.)

Our SOC Journey

Over the past 6 years, our SOC has undergone an amazing transformation. It started with a proof of concept, expanded to provide monitoring services for our corporate network. In 2021, we started offering SOCaaS to our global customers, helping them tackle their security challenges

Monitoring **2000+** FortiGates	Customers from **10+** Industries	Protect **650K+** *endpoints*
Skills **31** Highly Trained Experts	Operations Centers **3** Regions	Global **24x7** Operation

SOCaaS

Cloud monitoring, incident triage and escalation service

Monitor & Detect

Continuous monitoring & rapid detection using our cutting-edge technology

Investigate & Escalate

Fortinet experts delve deep into alerts, perform investigate and escalate actionable alerts.

Respond

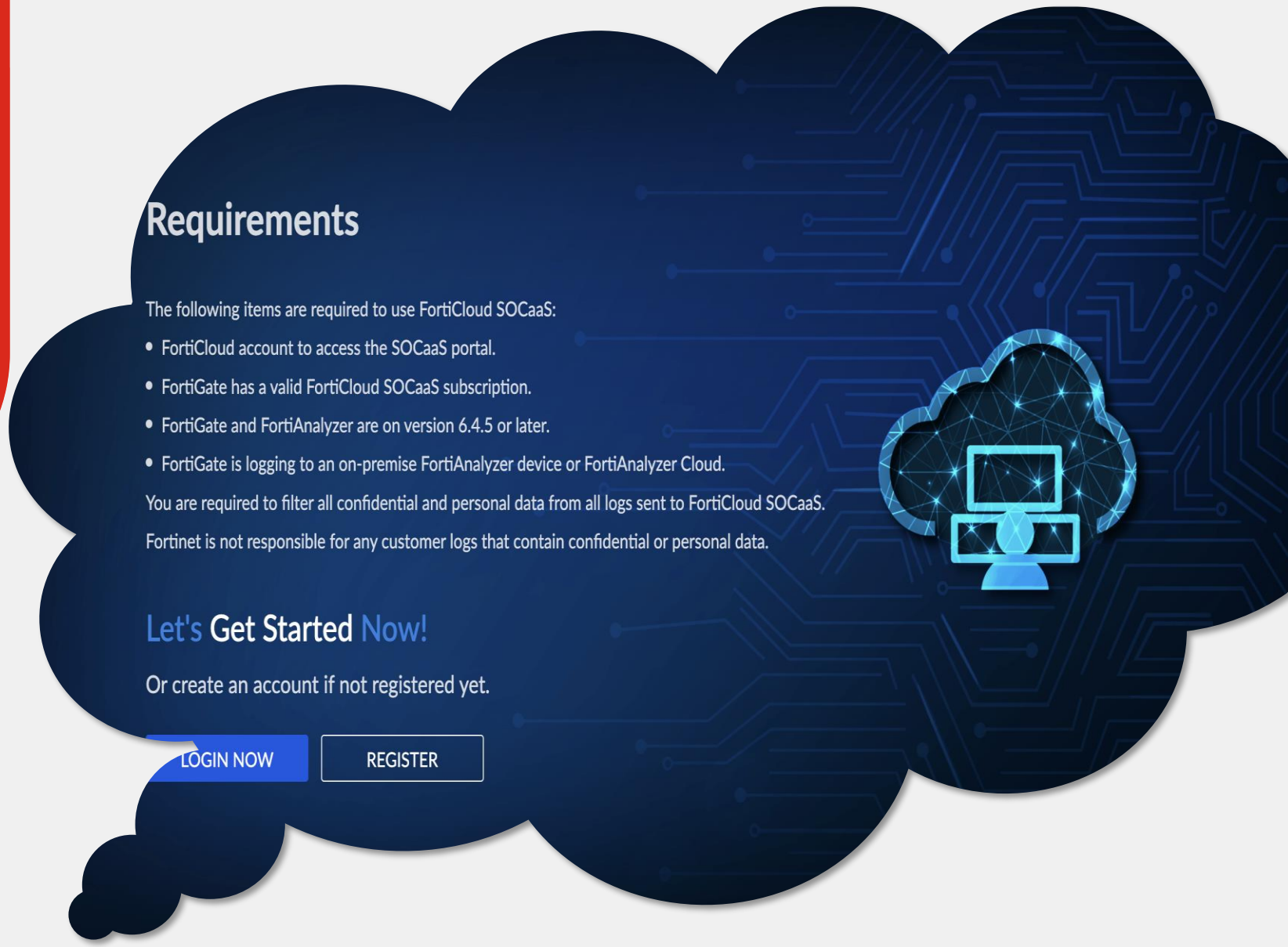
Live experts access around the clock via our service portal for immediate assistance

Improve

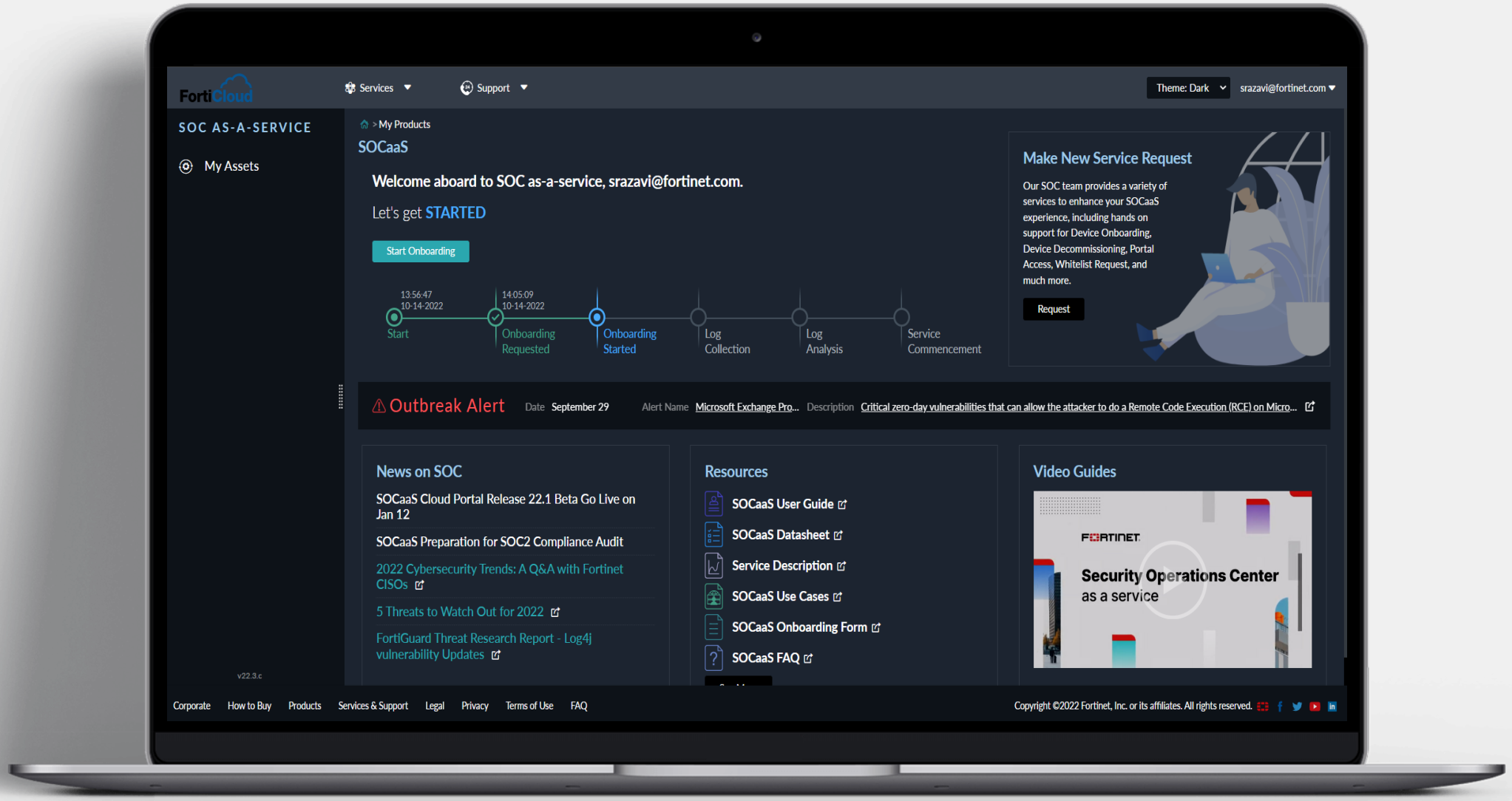
Stay informed with real-time incident reporting and QBRs for security posture improvement

The SOCaaS FortiCloud Portal

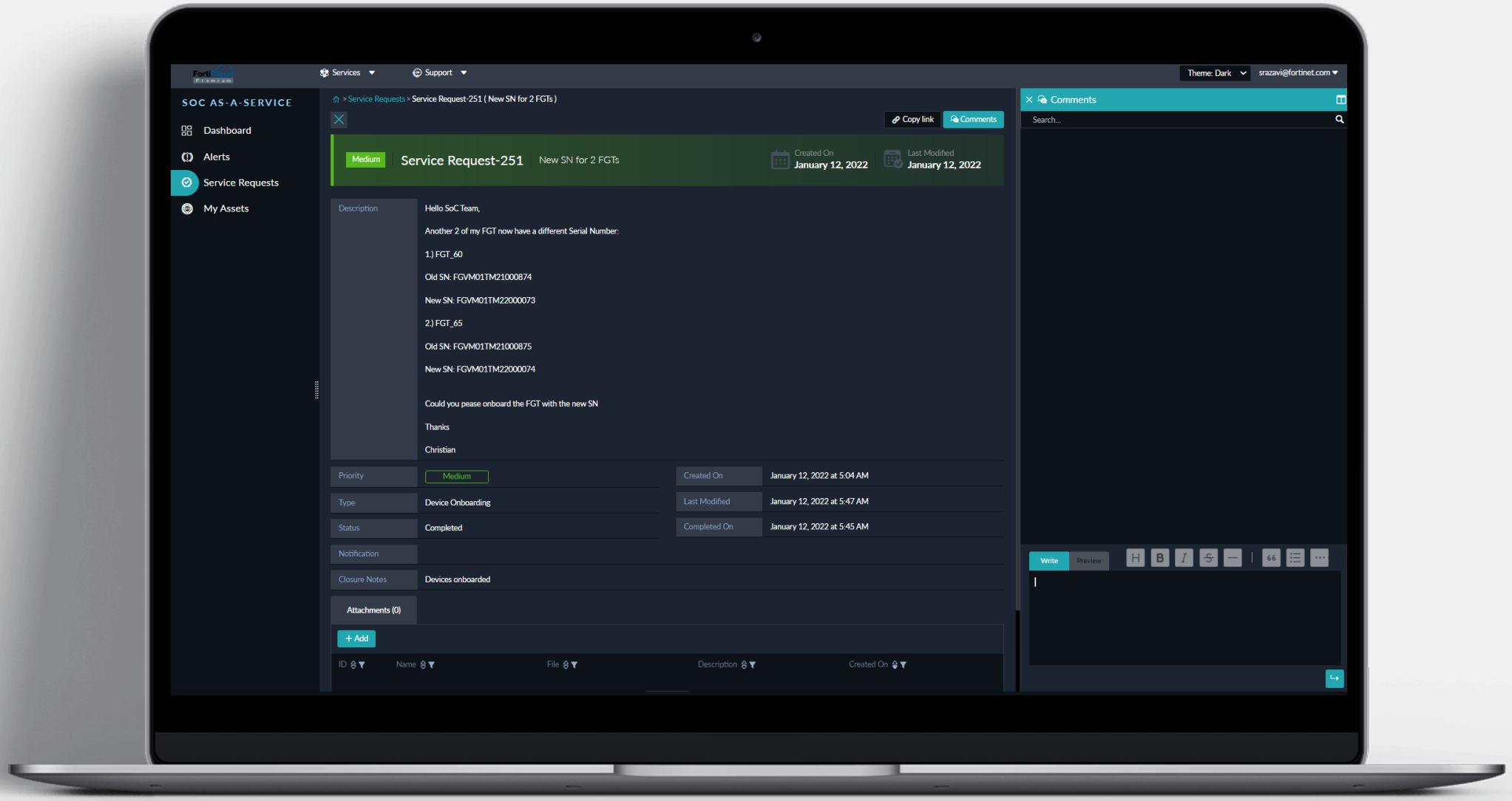
How Does SOCaaS integrate into your Day to Day?



Service Portal



Service Portal – Incident Response



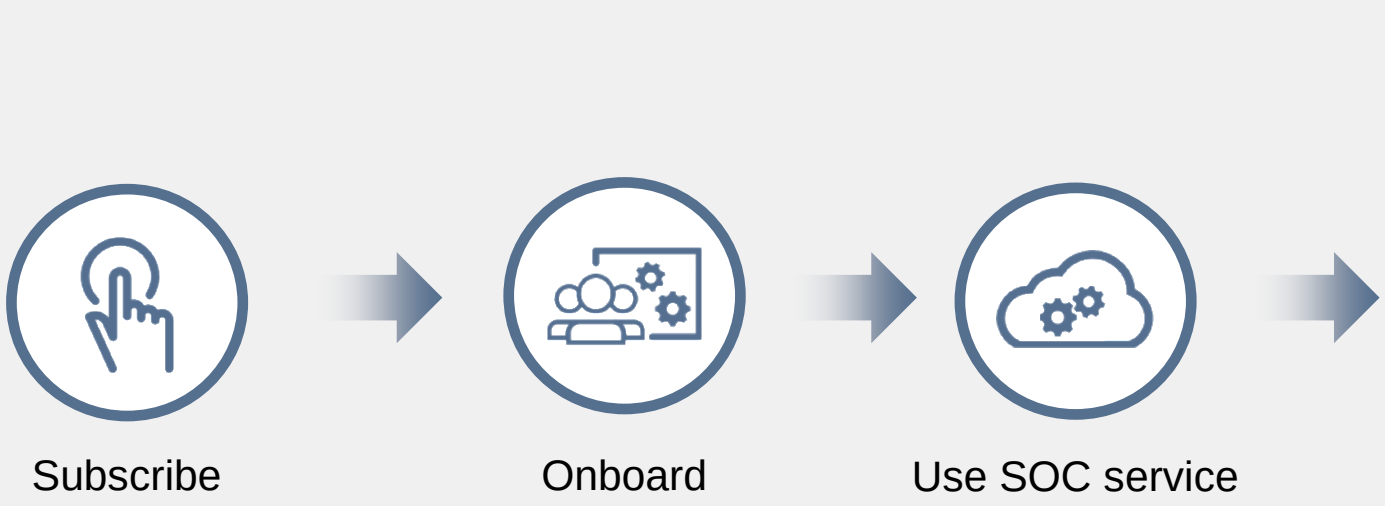
Service Portal – Reports

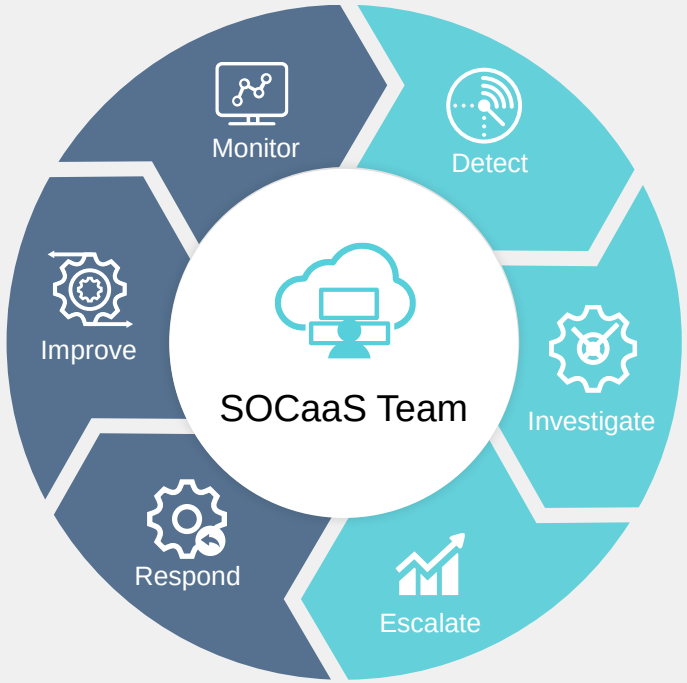
Continuous Security Posture Review

Multi-tenancy Support

Designed for MSSP partners

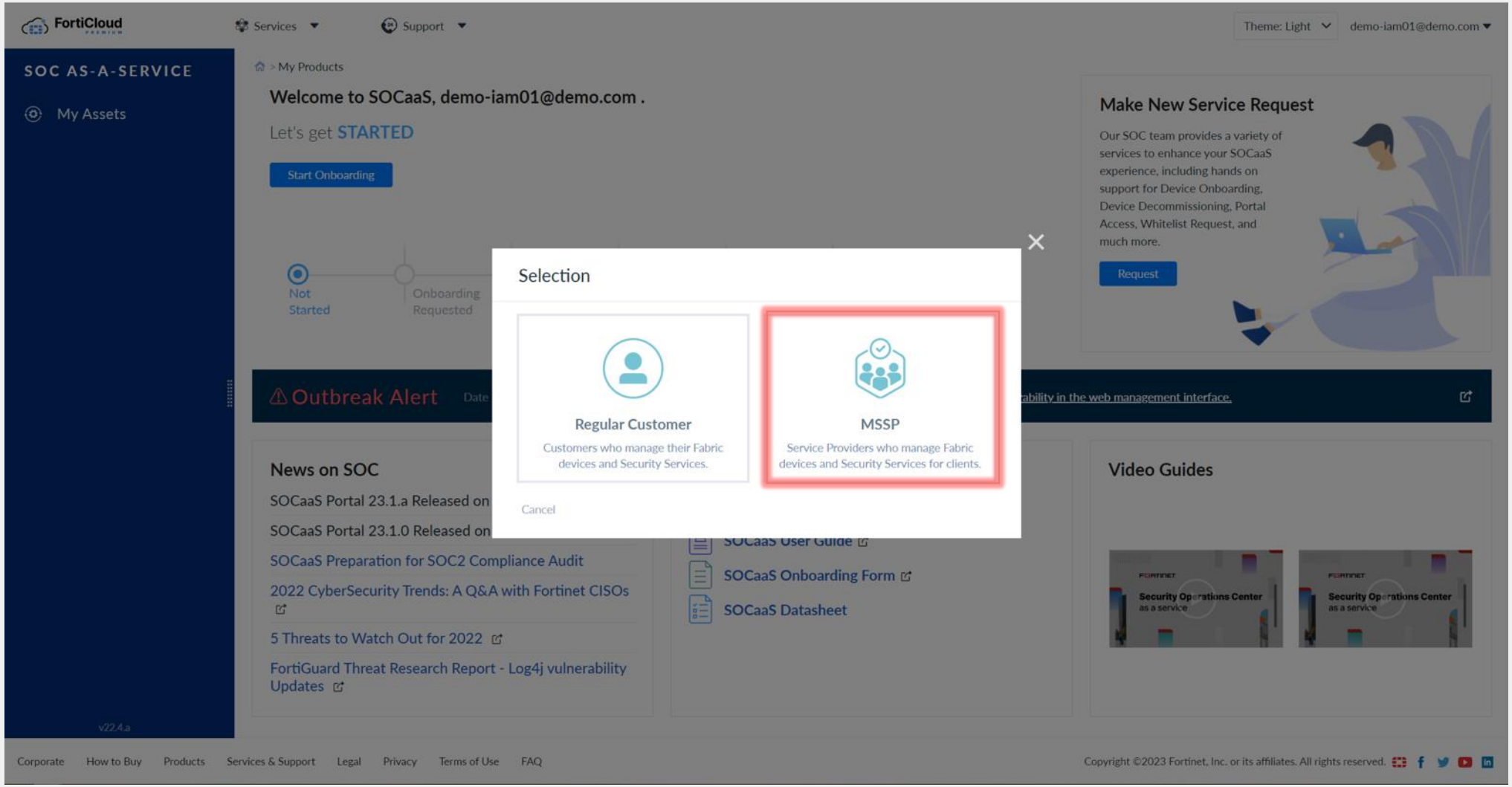
Partners can subscribe to SOCaaS for each deployed device, enabling seamless delivery of SOC services to their clients.





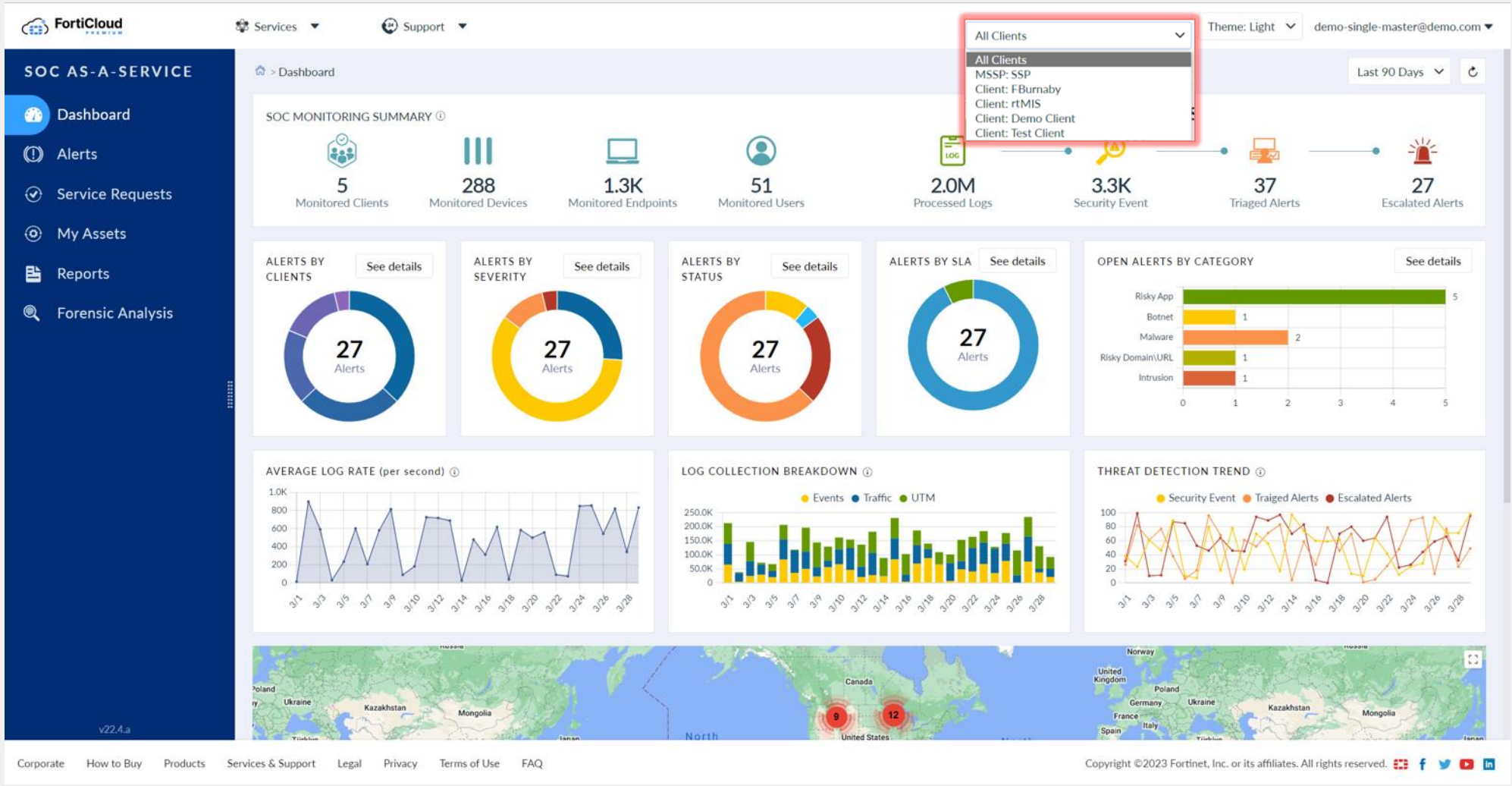
Onboard SOCaaS as An MSSP

Partners can onboard as an MSSP to provide SOC services to their clients

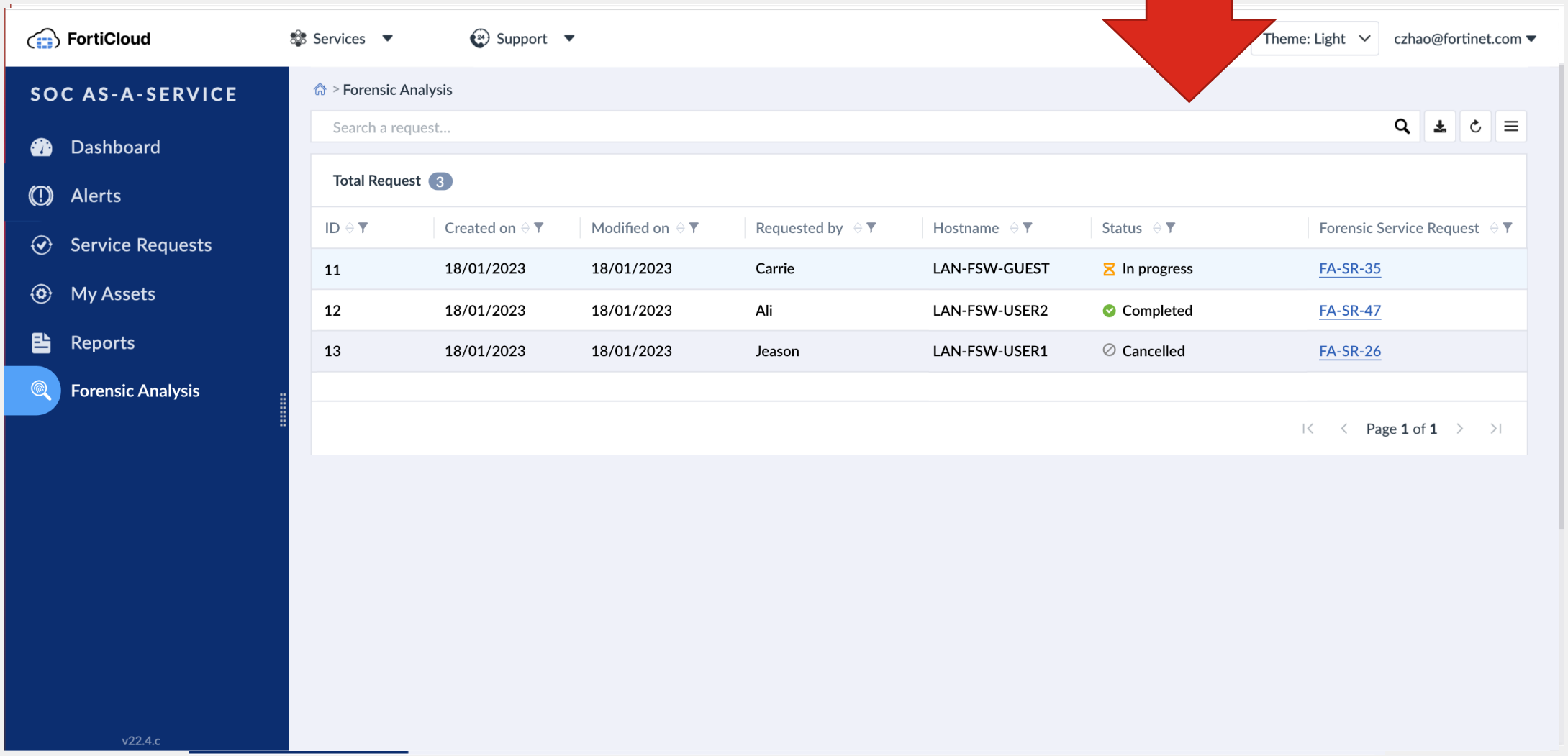


MSSP Service Portal

MSSP portal has a central dashboard for all clients with the ability to select and view individual client dashboards. Clients can log in to their individual portals to view their respective dashboards.



FCT Monitoring & Forensic Analysis



NIS2 Technology Mapping

Promoting an Integrated Security Platform for Automation, Orchestration, and Compliance

NIS2 Security Pillars

Asset Management
SIEM NAC NGFW API

Access Control to Networks & Assets
NGFW NAC IAM EPP 2FAs Proxy

Segmentation, Protection & Response
NGFW Switch WIFI EDR 2FAs Proxy

Events, Alerts and Incident Detection
SOAR SIEM Logger

Risk Management
Config Manager SIEM Logger Tester

Single Pane Management

Threat Intelligence

Interoperability


FORTINET