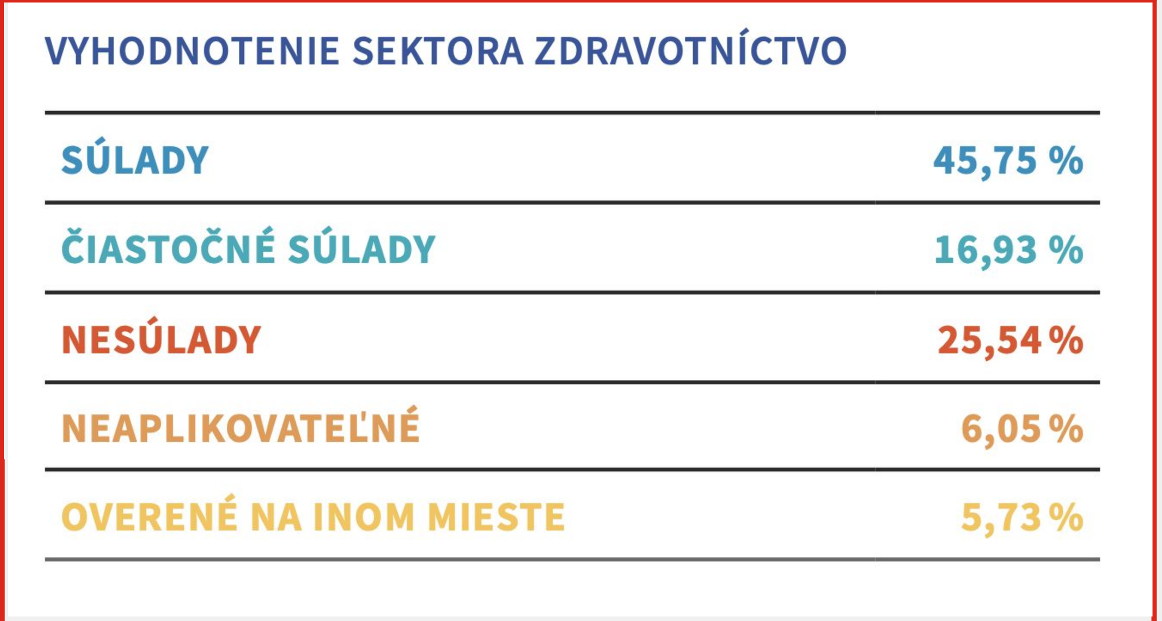
Prečo je prevencia lacnejšia ako obnova a rýchlejšia ako resuscitácia

Peter Kocik
Manager Systems Engineering

Sektor Zdravotníctva z pohľadu NBU

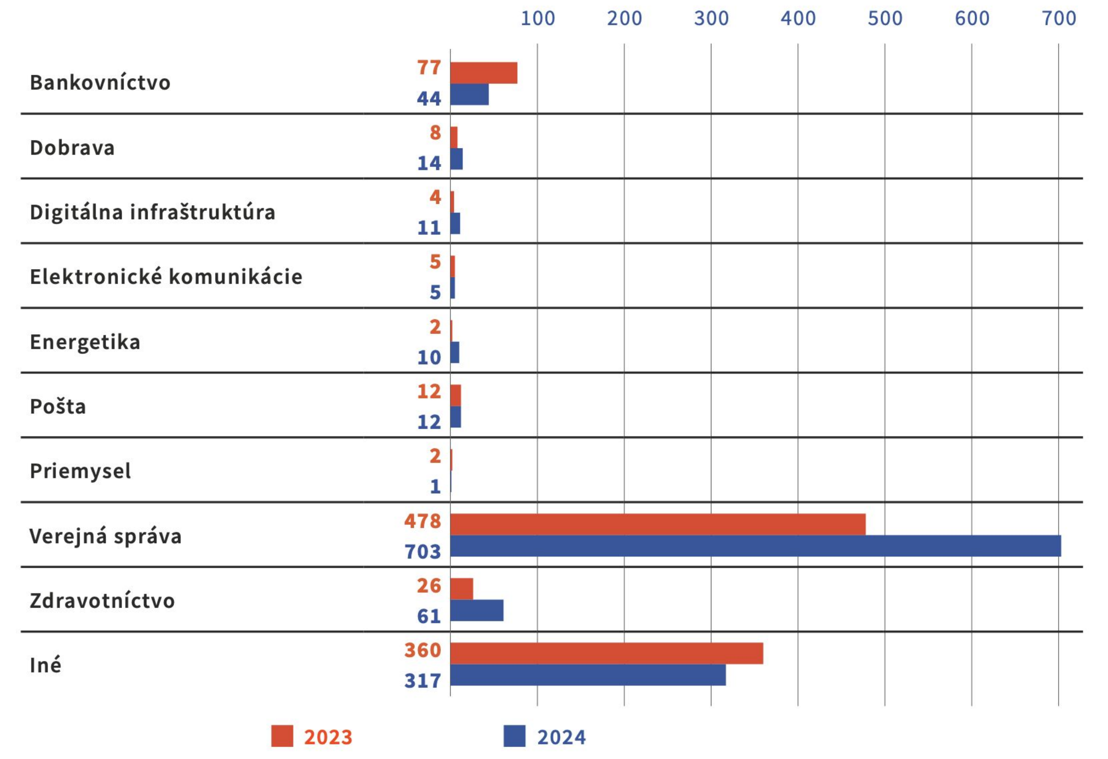
Súlad na základe auditných správ



VYHODNOTENIE SEKTORA ZDRAVOTNÍCTVO

SÚLADY	45,75 %
ČIASTOČNÉ SÚLADY	16,93 %
NESÚLADY	25,54 %
NEAPLIKOVATEĽNÉ	6,05 %
OVERENÉ NA INOM MIESTE	5,73 %

Počet hlásených incidentov v sektoroch



EMEA Healthcare Threat Landscape 2025

TLP: GREEN
Limited disclosure, restricted to the community.
NOT For Media Release

Powered by FortiGuard Labs

Malicious Activity Detected

5.9bn

Growth Year over Year

63.51%

IPS — **Intrusion Prevention Activity**

5.8bn

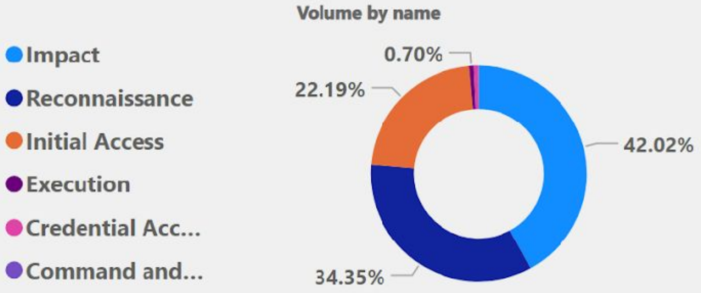
AV — **Malware Distribution Activity**

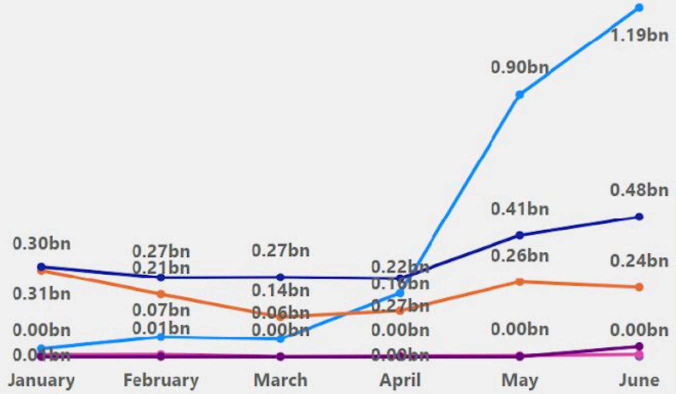
40.8M

C2 — **Botnet Activity Detected**

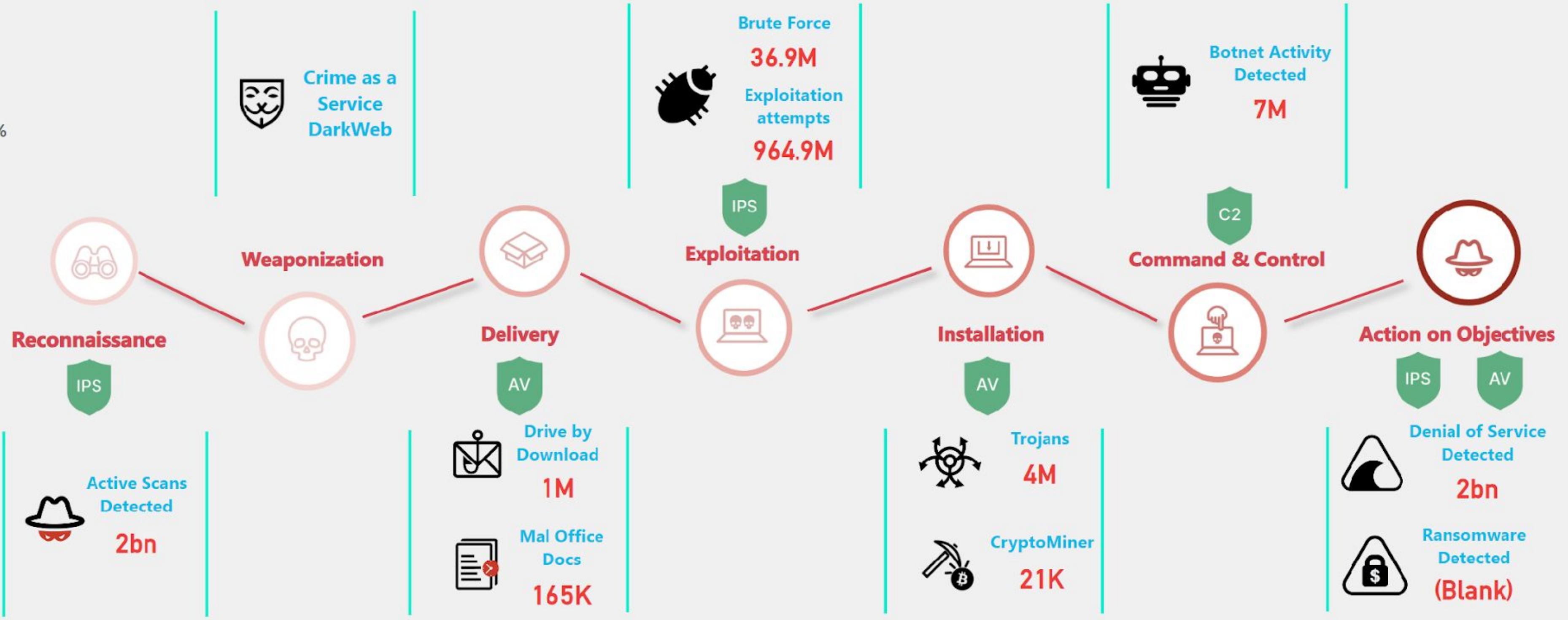
7M

ATT&CK Tactics detected





Cyber Kill Chain Model



Crime as a Service DarkWeb

Brute Force **36.9M**

Exploitation attempts **964.9M**

Botnet Activity Detected **7M**

Active Scans Detected **2bn**

Drive by Download **1M**

Mal Office Docs **165K**

Trojans **4M**

CryptoMiner **21K**

Denial of Service Detected **2bn**

Ransomware Detected **(Blank)**

EMEA Exploitation Attempts 2025

IPS

TLP: GREEN
Limited disclosure, restricted to the community.
NOT For Media Release

Healthcare

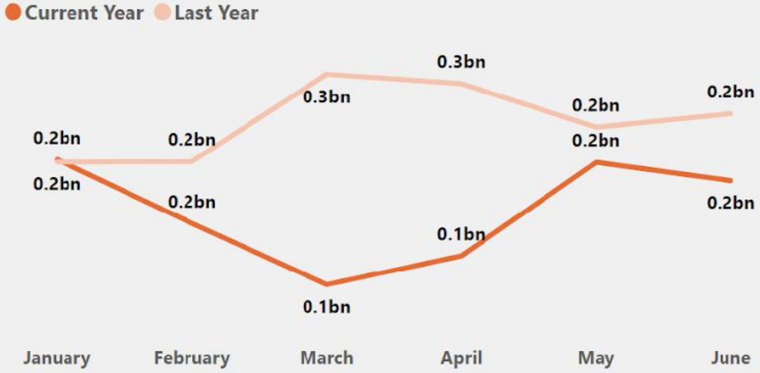
ATT&CK®

TA0001 - Initial Access

T1190 - Exploit Public Facing Application

T1195 - Supply Chain Compromise

Behavioral Trend Analysis by Month



Current detections

964.87M

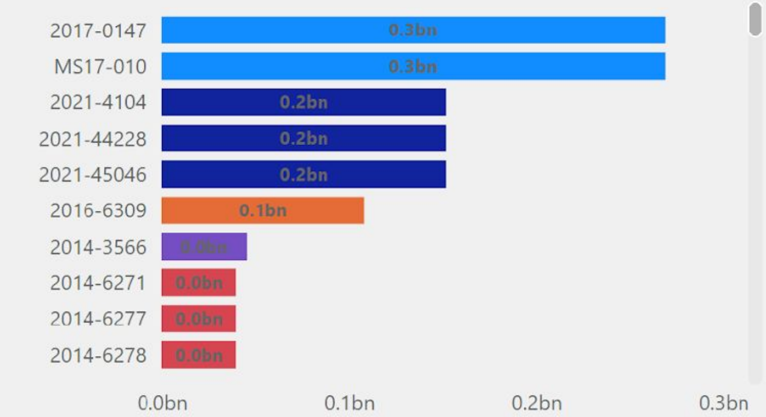
Last year detections

1.44bn

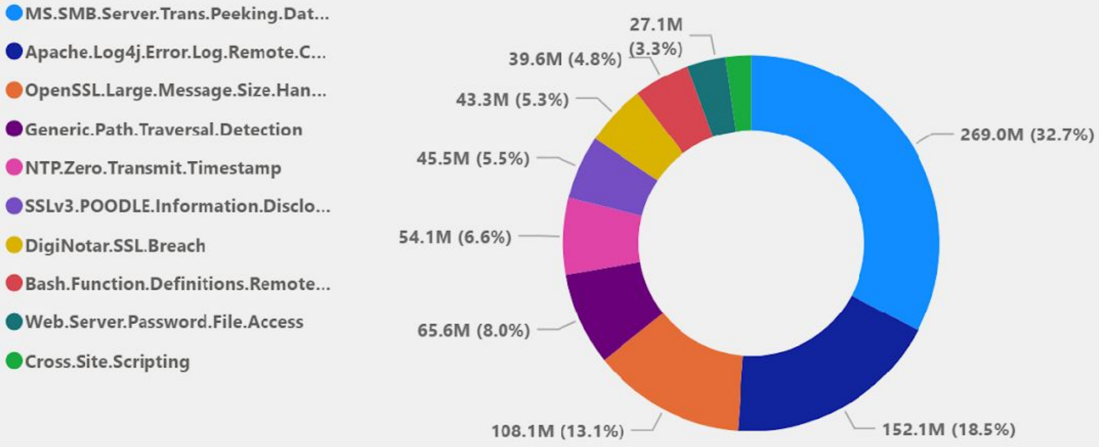
Growth YoY

-32.77%

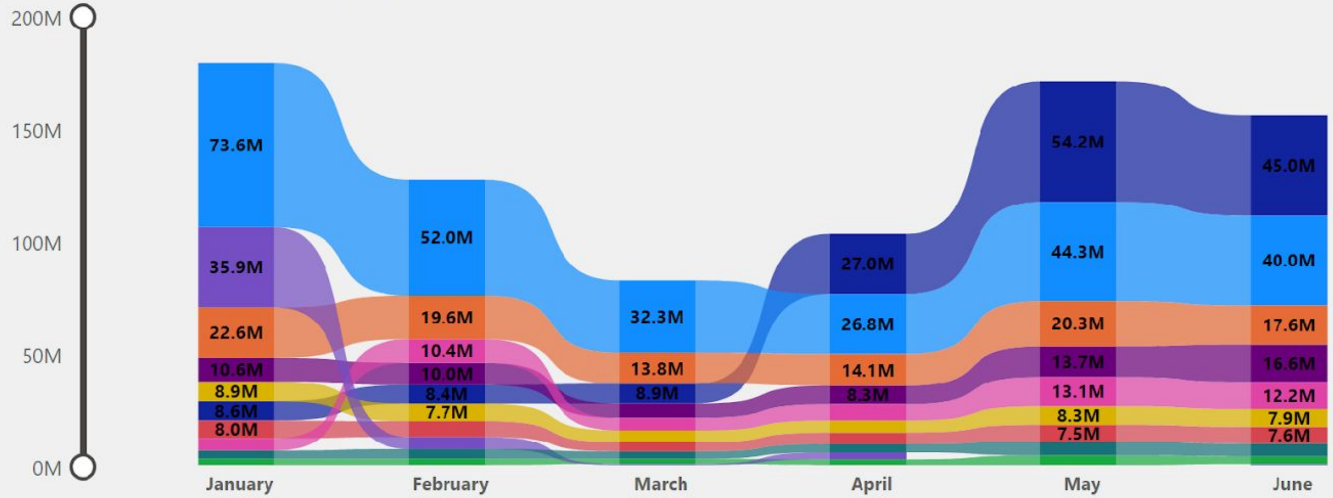
Targeted Vulnerabilities



Exploit Attempts Distribution by Signature



Behavioral Trend Analysis by Signature



EMEA Brute Force Attacks 2025

IPS

TLP: GREEN
Limited disclosure, restricted to the community.
NOT For Media Release

Healthcare

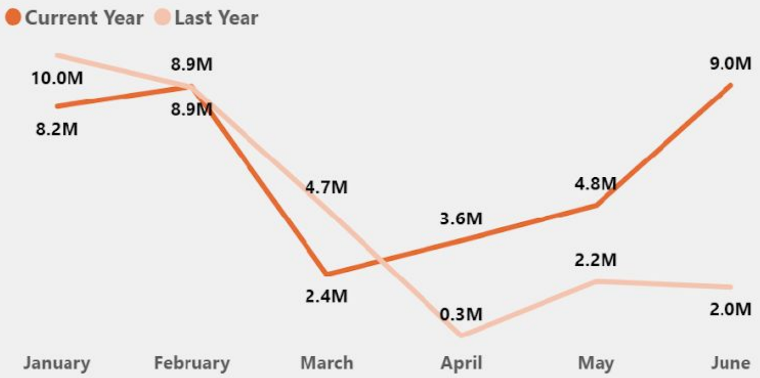
ATT&CK®

TA006 - Credential Access

T1110 - Brute Force

- **T1110.001** - Password Guessing
- **T1110.003** - Password Spraying
- **T1110.004** - Password Stuffing

Behavioral Trend Analysis by Month



Current detections

36.90M

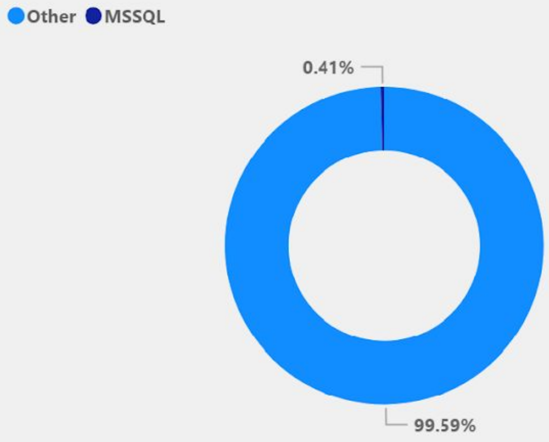
Last year detections

27.98M

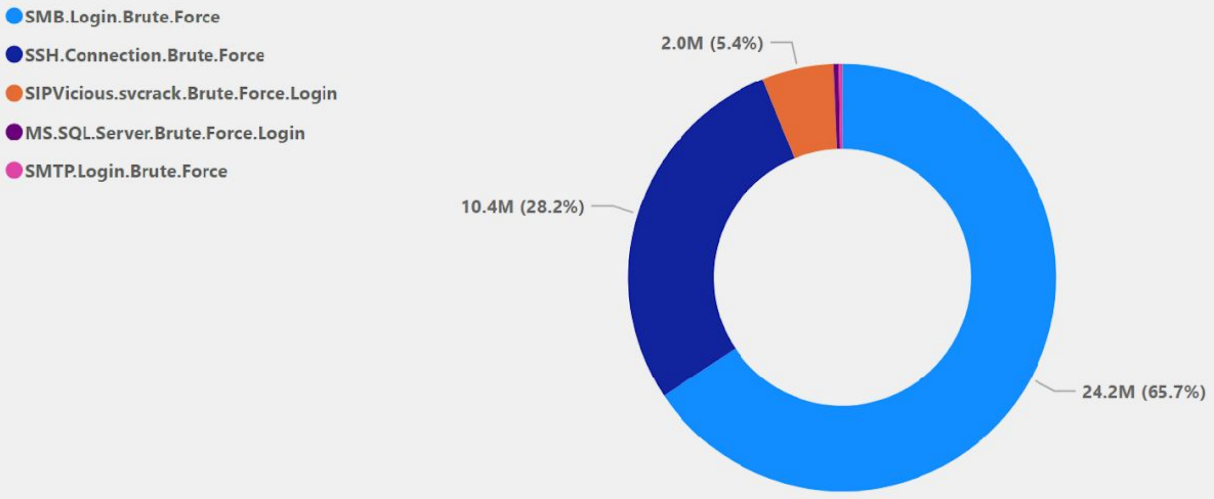
Growth YoY

31.89%

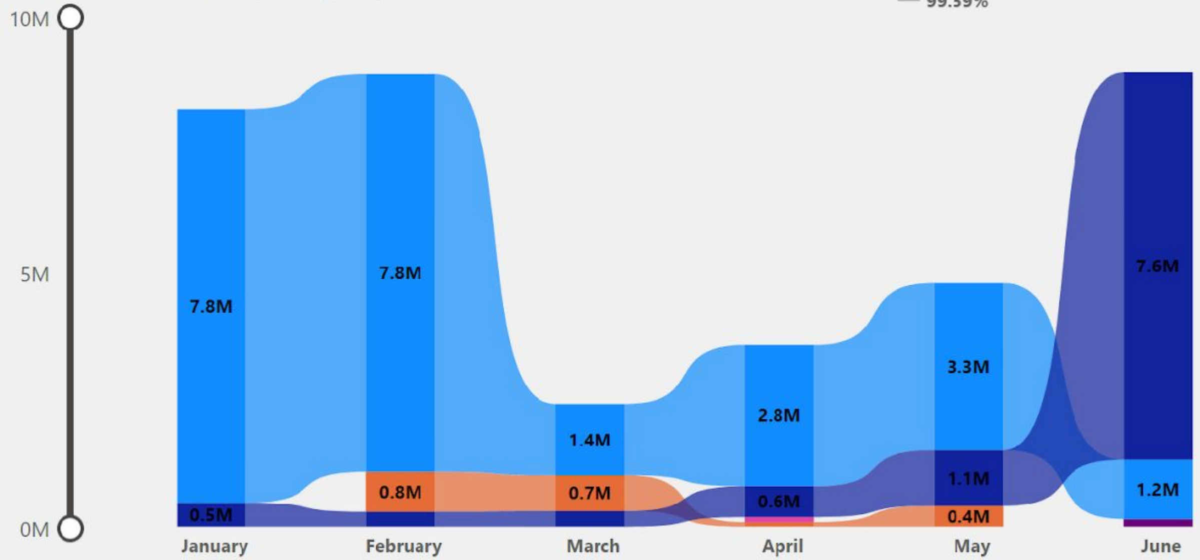
Targeted Applications



Brute Force Attacks Distribution by Signature



Behavioral Trend Analysis by Signature



EMEA Malware Distribution 2025

AV

TLP: GREEN

Limited disclosure, restricted to the community.

NOT For Media Release

Healthcare

ATT&CK®

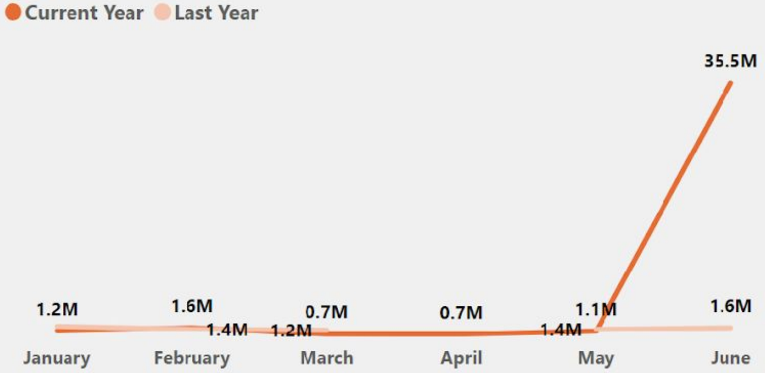
TA0002 - Execution

T1204 - User Execution
- **T1204.001** - Malicious Link
- **T1204.002** - Malicious File

T1203 - Exploitation for Client Execution

T1059 - Command and Scripting Interpreter

Behavioral Trend Analysis by Month



Current detections

40.76M

Last year detections

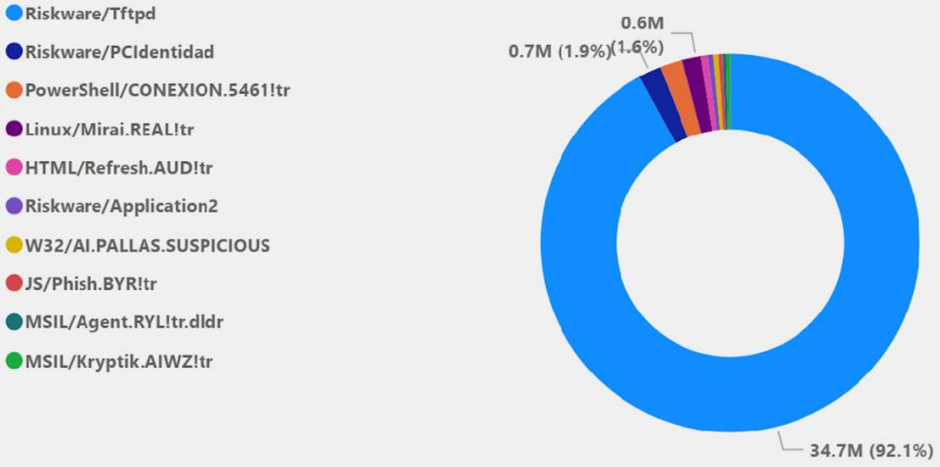
7.38M

Growth YoY

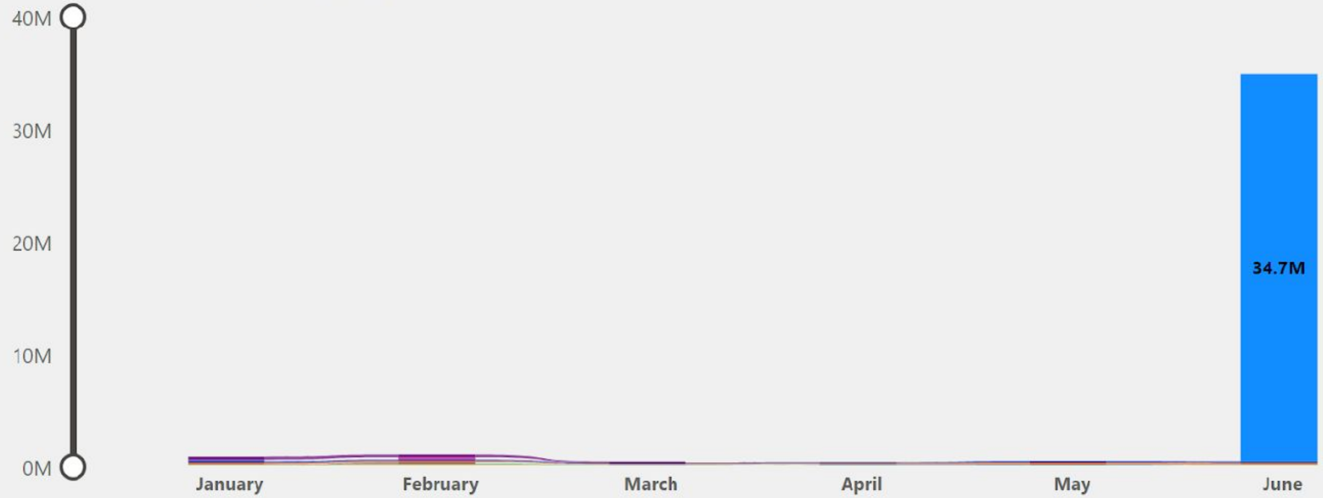
451.96%

AI-based malware detection by Volume

Malware Distribution by Signature



Behavioral Trend Analysis by Signature



EMEA Denial of Service Attacks 2025

IPS

TLP: GREEN
Limited disclosure, restricted to the community.
NOT For Media Release

Healthcare

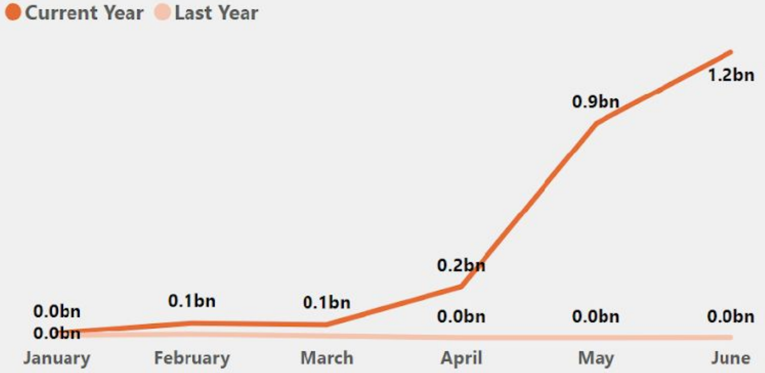
ATT&CK®

TA0040 - Impact

T1498 - Network Denial of Service
- T1498.001 - Direct Network Flood
- T1498.002 - Reflection Amplification

T1499 - Endpoint Denial of Service
- T1499.002 - Service Exhaustion Flood (DNS)

Behavioral Trend Analysis by Month



Current detections

2.46bn

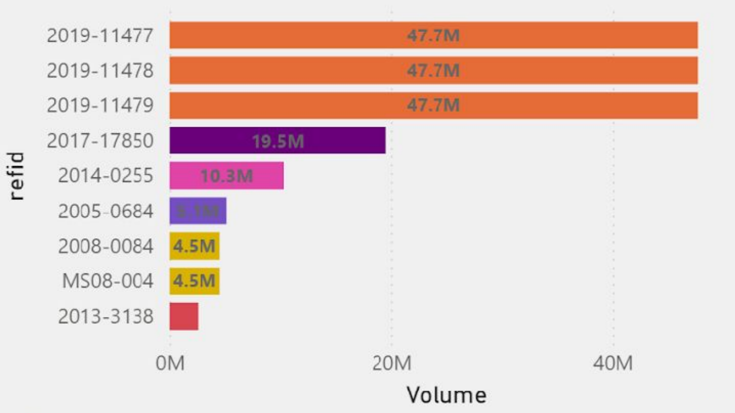
Last year detections

61.37M

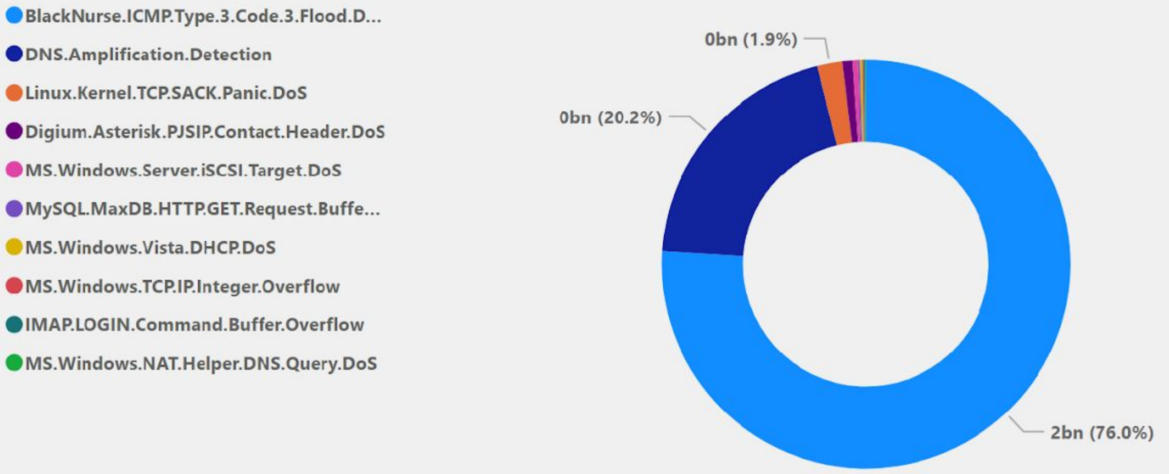
Growth YoY

3909.59%

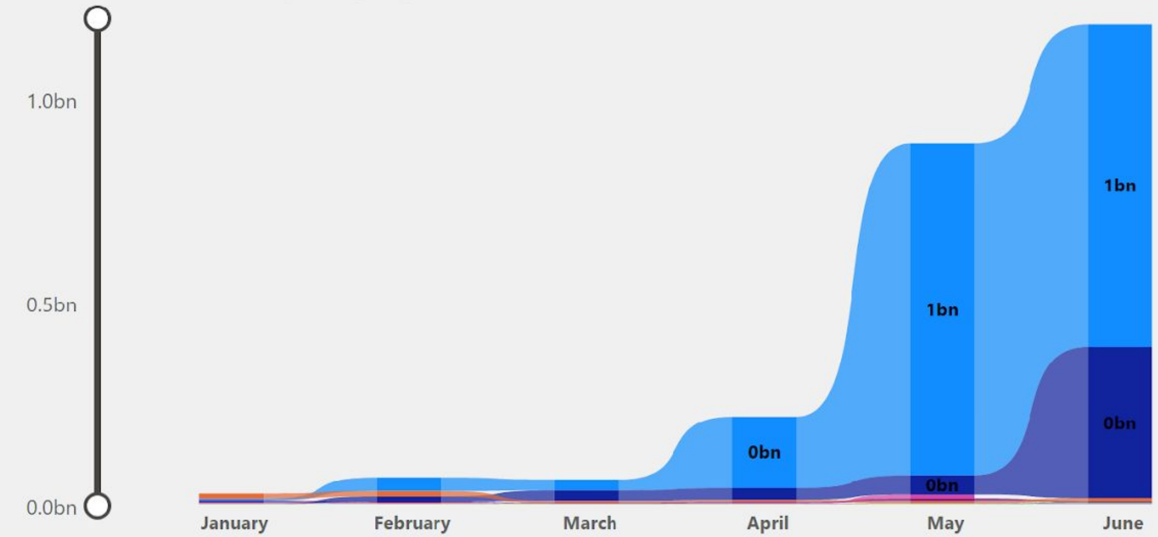
Targeted Vulnerabilities



Scan Attempts Distribution by Signature



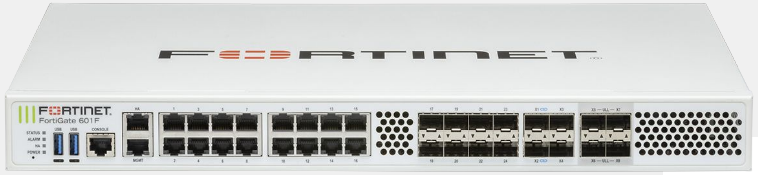
Behavioral Trend Analysis by Signature



Safeguarded by AI-powered Security

Simple FortiGate Bundles

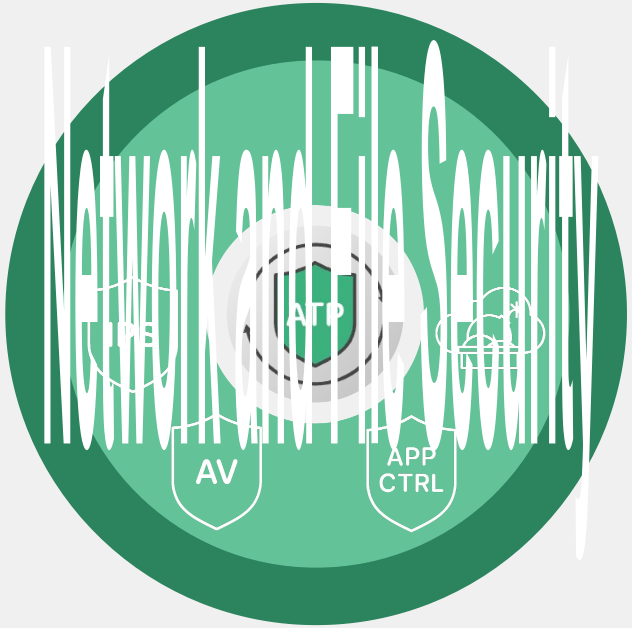
Each bundle, builds on the other

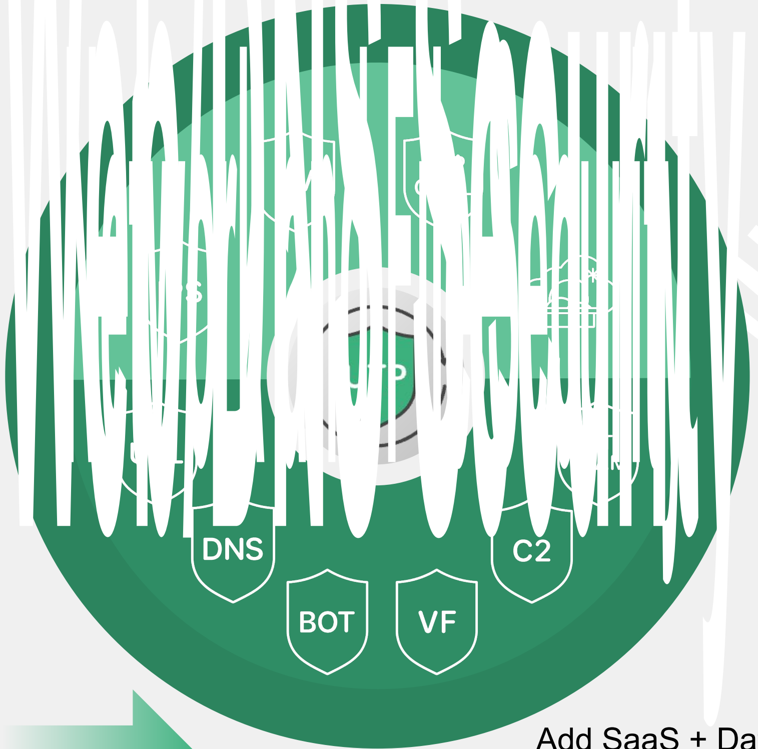


Comprehensive security across your entire attack surface - Networks, Files, Web, SaaS, Data and Devices. Includes ATP and UTP.

Advanced protection across network and web., Includes ATP. Blocks more threat vectors.

Essential First Line of Defense. Protects against known network intrusions and malware.





UTP
IPS
AV
APP CTRL
DNS
C2
ANTI-SPAM

Add Web Security

Add SaaS + Data + Device Security and Zero-day Protection

FortiSwitch Secure Ethernet Switching

A secure approach to Ethernet

Secure

NGFW security visibility and control to Ethernet networking

Simple

Zero touch deployment

Easy to manage whether integrated or standalone

Scalable

Deployments from the smallest branch to largest campus

FortiAP Secure Wireless LAN

A secure approach to Wi-Fi networking

Secure

SSIDs directly controlled and secured by FortiOS

Flexible

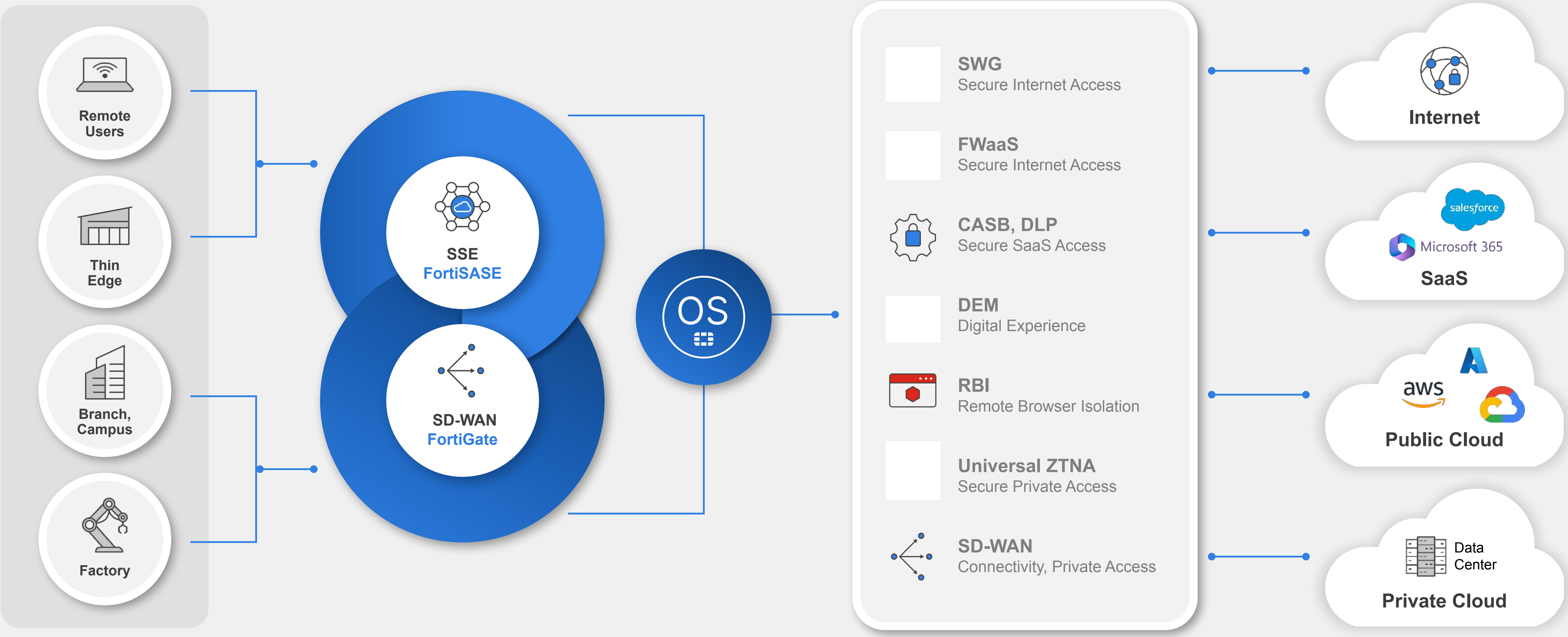
Manageable via FortiGate, Cloud, or SASE, on-prem, hardware or VM

Resilient

Quad radio design for access + troubleshooting

Intelligence at all levels for peak connectivity

Fortinet's Unified SASE Solution for Secure Access



Unified Console, Agent, Data-lake

Flexible Enforcement, Connectivity

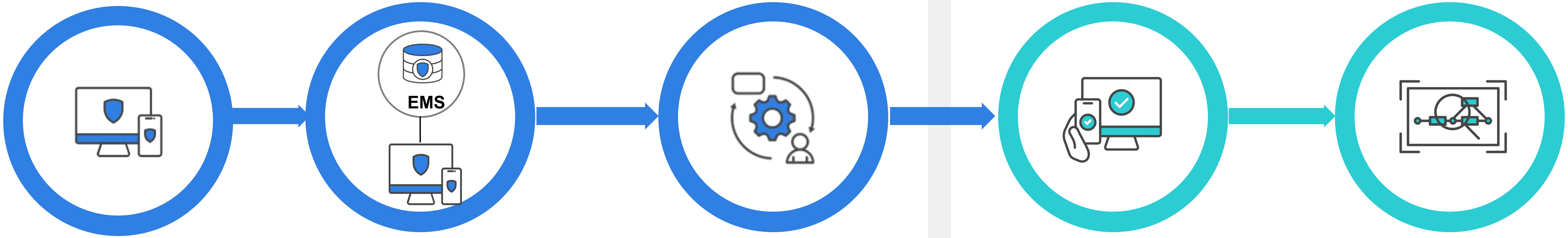
AI-Powered Intelligence

Fortinet Unified Agent Evolution

Continuous Innovation, Wide adoption with over 20M endpoints deployed

Evolution of Secure Access

Integrated Endpoint Security



VPN Only

- Remote Access VPN only

Endpoint Management (SaaS / On-prem)

- Centralized Endpoint Management
- Endpoint Telemetry and Visibility

Universal ZTNA (with IT Hygiene)

- Continuous Posture Validation
- Vulnerability Scanning and Patching Policy
- Web Filtering

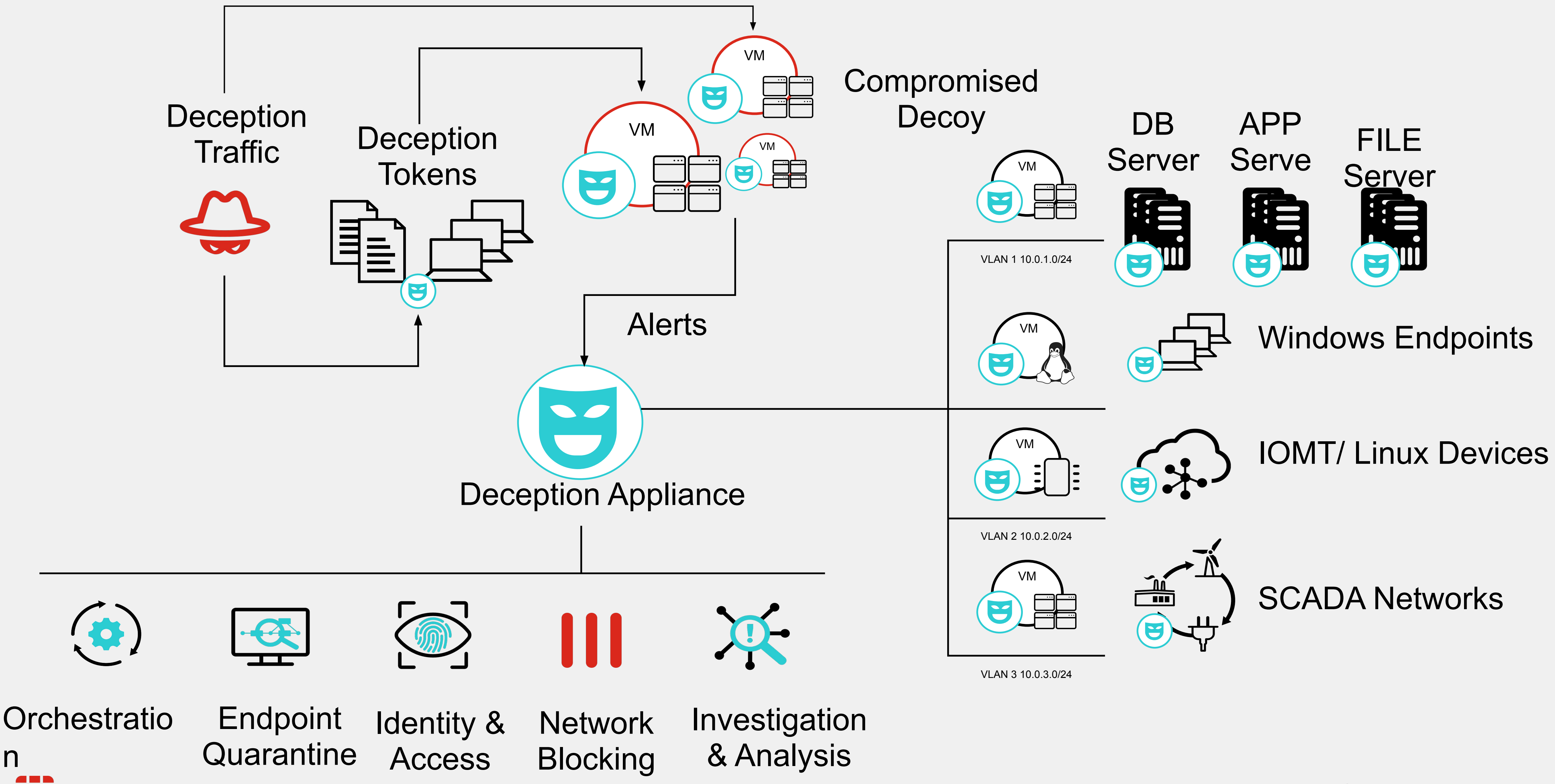
Endpoint Protection (EPP)

- AI Powered Anti-Virus
- Application firewall
- Ransomware protection

Endpoint Detection and Response (EDR)

- Behavior-based Protection
- Extended automated responses
- Threat hunting

Fortinet Deception Solution



Deception Traffic

Deception Tokens

VM

VM

VM

Compromised Decoy

Alerts

Deception Appliance

VM

VLAN 1 10.0.1.0/24

VM

VM

VLAN 2 10.0.2.0/24

VM

VLAN 3 10.0.3.0/24

DB Server

APP Serve

FILE Server

Windows Endpoints

IOMT/ Linux Devices

SCADA Networks

Orchestratio n

Endpoint Quarantine

Identity & Access

Network Blocking

Investigation & Analysis

Appliance Virtual Machine Cloud Big Data

FortiAnalyzer Turnkey SOC

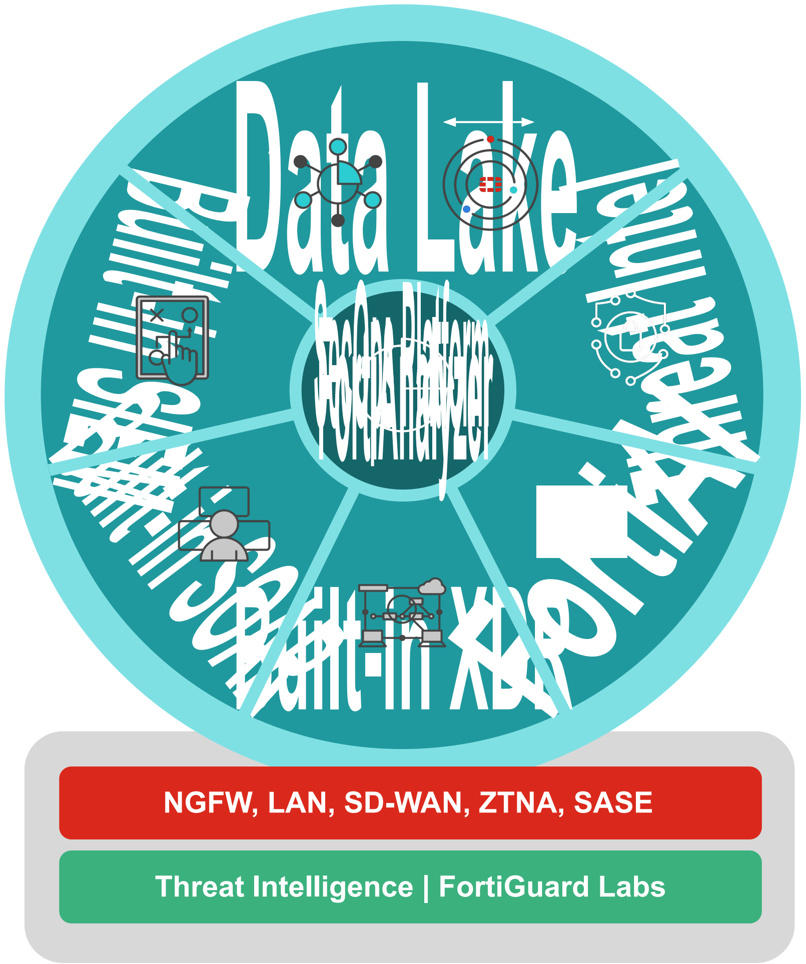
Essential turnkey capabilities for the lean security team

Solution Specs

FortiAnalyzer

Turnkey SOC

- Purpose-built for teams managing both IT and security
- Delivers speed, structure, and visibility in a single platform
- Reduces operational burden—no stitching, scripting, or standing up extra tools



NGFW, LAN, SD-WAN, ZTNA, SASE

Threat Intelligence | FortiGuard Labs

Unified Data Lake

Close security gaps through centralized log collection and analysis, providing a unified single source of truth view

Native Threat Intelligence

Stay ahead of emerging attacks with real-time FortiGuard Labs threat intel, outbreak detection and IoC tracking

Built-in SOC Automation

Streamline processes with ready-to-deploy SIEM, SOAR, and XDR capabilities, featuring prebuilt content.

Embedded AI-Assistance

Speed response and enhance efficiency with AI-assistance for augmented operations

Flexible Deployments

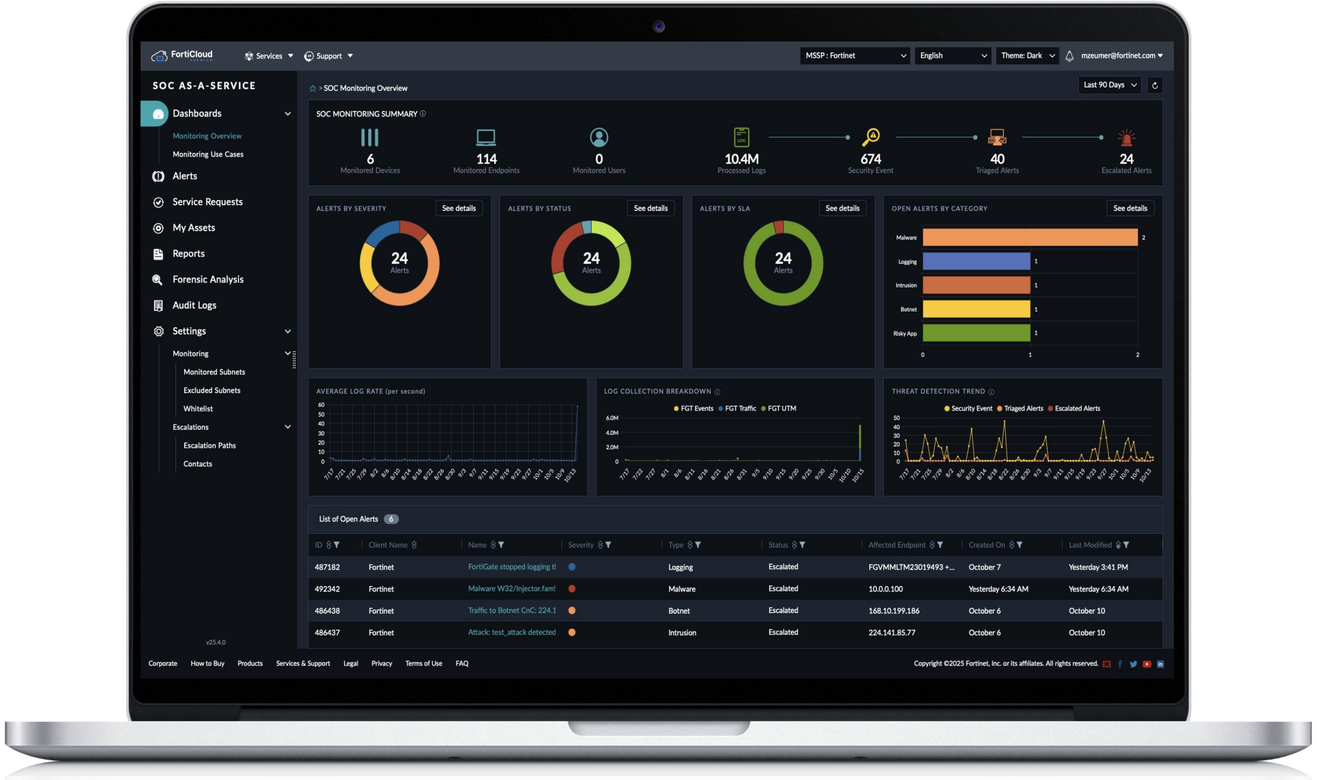
Lightweight deployment options through horizontal big data scale with appliance, VM, or cloud deployment

24/7 Security Monitoring with FortiGuard SOCaaS

Solution Specs

FortiGuard SOCaaS

- Ensures threats are acted on—not just detected
- Maintains full coverage during off-hours, holidays, and staffing gaps
- Accelerates maturity without building a full in-house SOC



SOC MONITORING SUMMARY

6	114	0	10.4M	674	40	24
Monitored Devices	Monitored Endpoints	Monitored Users	Processed Logs	Security Event	Triaged Alerts	Escalated Alerts

List of Open Alerts 6

ID	Client Name	Name	Severity	Type	Status	Affected Endpoint	Created On	Last Modified
487182	Fortinet	FortiGate stopped logging tl	●	Logging	Escalated	FGVMMLTM23019493 +...	October 7	Yesterday 3:41 PM
492342	Fortinet	Malware W32/Injector.fam!	●	Malware	Escalated	10.0.0.100	Yesterday 6:34 AM	Yesterday 6:34 AM
486438	Fortinet	Traffic to Botnet CnC: 224.1	●	Botnet	Escalated	168.10.199.186	October 6	October 10
486437	Fortinet	Attack: test_attack detected	●	Intrusion	Escalated	224.141.85.77	October 6	October 10

Copyright ©2025 Fortinet, Inc. or its affiliates. All rights reserved.

Detect

Let Fortinet monitor and investigate alerts 24/7, notifying you when something is important and needs attention.

Respond

Fortinet experts will alert teams in 15 minutes and provide insights on the incident and remediation steps.

Improve

Cloud portal with intuitive dashboards, on-demand reports, and quarterly meetings with Fortinet Experts

*FortiGuard SOCaaS is a simple FortiGate on subscription

FORTINET