PRODUCT CATALOG

SHELT YOUR CYBERSECURITY

AS-A-SERVICE PARTNER



Who Are We?



SHELT is a European Cybersecurity enterprise for the new digital world, with presence in Europe, Middle East and on the African Continent.

A culmination of years of experience from several partners that are all leaders in their respective fields; ranging from Telecommunication Network providers, Managed Services to Cyber Security service providers.





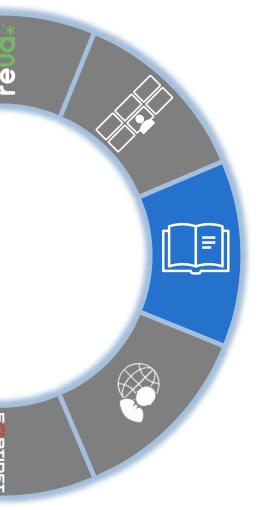








Product Catalog





Managed Next Gen SOC



Brand & VIP Protection



Information Security Services



Unified API Security



EDR & XDR



Fortinet Stack

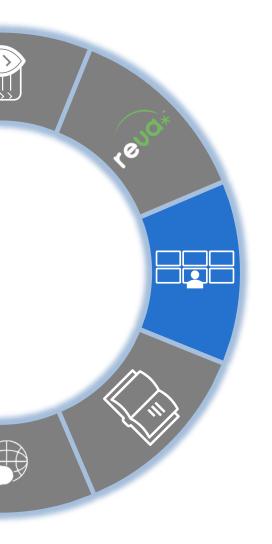
MANAGED SOC

SHELT YOUR CYBERSECURITY AS-A-SERVICE PARTNER

Managed Next Generation SOC

SHELT

SOC Building Blocks

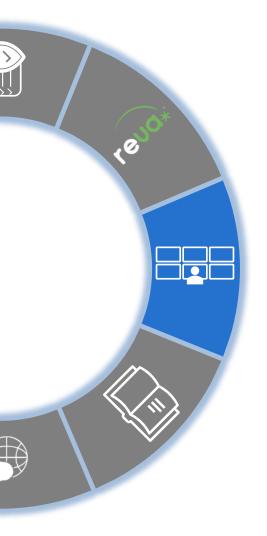




Managed Next Generation SOC

SHELT

People





24/7 Service

- Highly Skilled Professionals With Deep Knowledge In Security & Event Monitoring & Incident Response
- **On-demand Security Experts Available for Critical Investigations**

L1 SUPPORT

Event & Alert Monitoring



- Security Incident & Event Detection
- Event Analysis & Prioritization
- False Positive Reduction
- Notification of Qualified Events to Clients

L2 SUPPORT

Incident Response Support



- Event Advanced Analysis & Verification
- Triage & Investigation Support
- Troubleshoot the Interruptions in Log Collection
- Define Reporting Templates,
 Dashboards, Queries

L3 SUPPORT

Platform Management

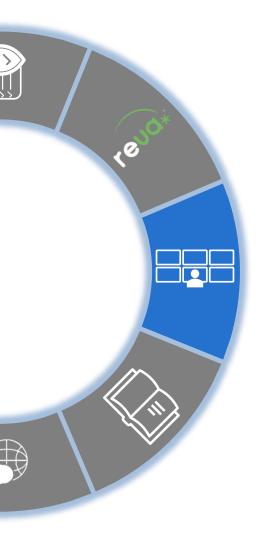


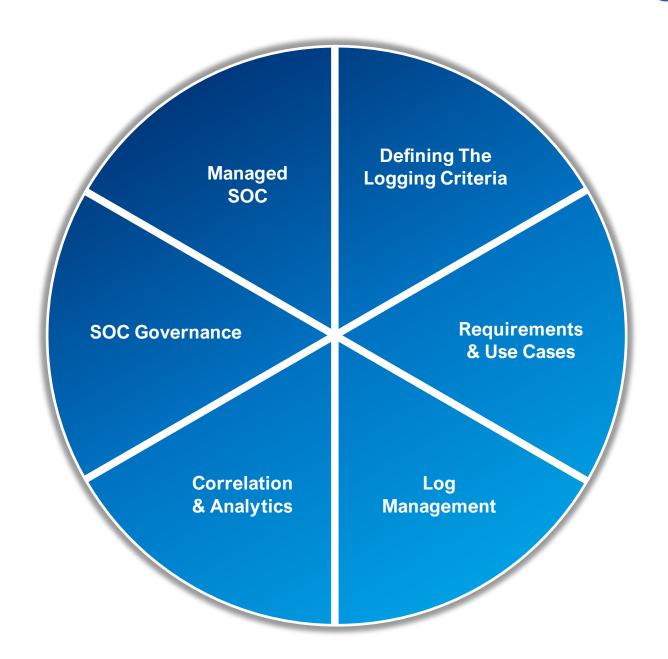
- Health & Performance Monitoring
- Change/Configuration Mgt
- Patch & Content Updates
- User Account & Access Mgt
- Fine Tuning of Existing Rules
- SLA Tracking

Managed Next Generation SOC

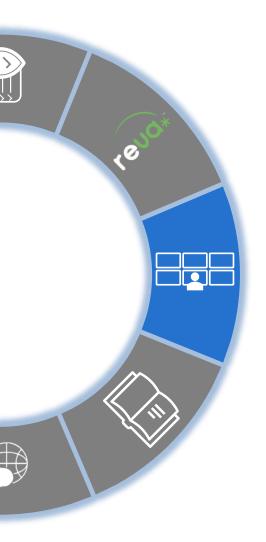
SHELT

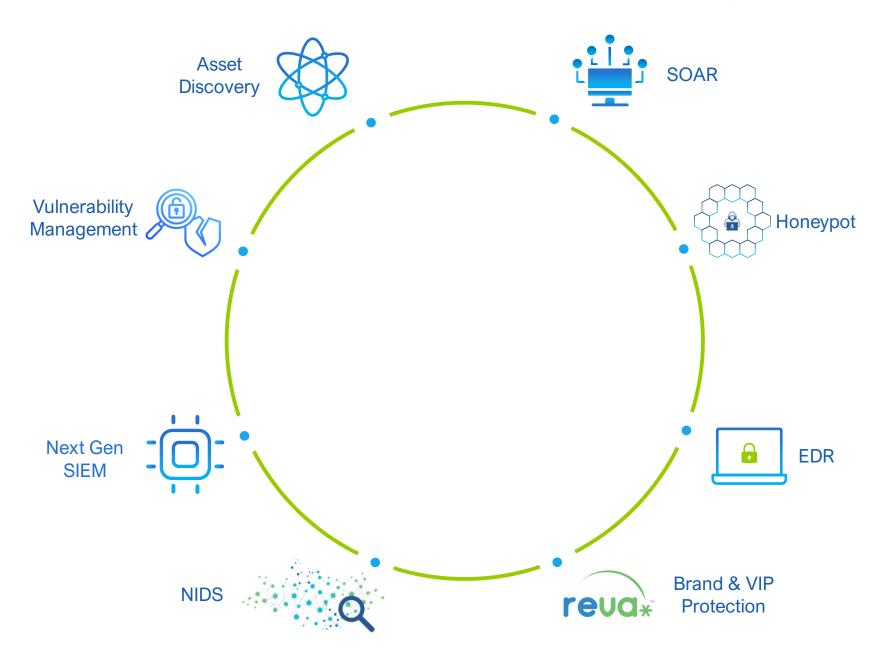
Process



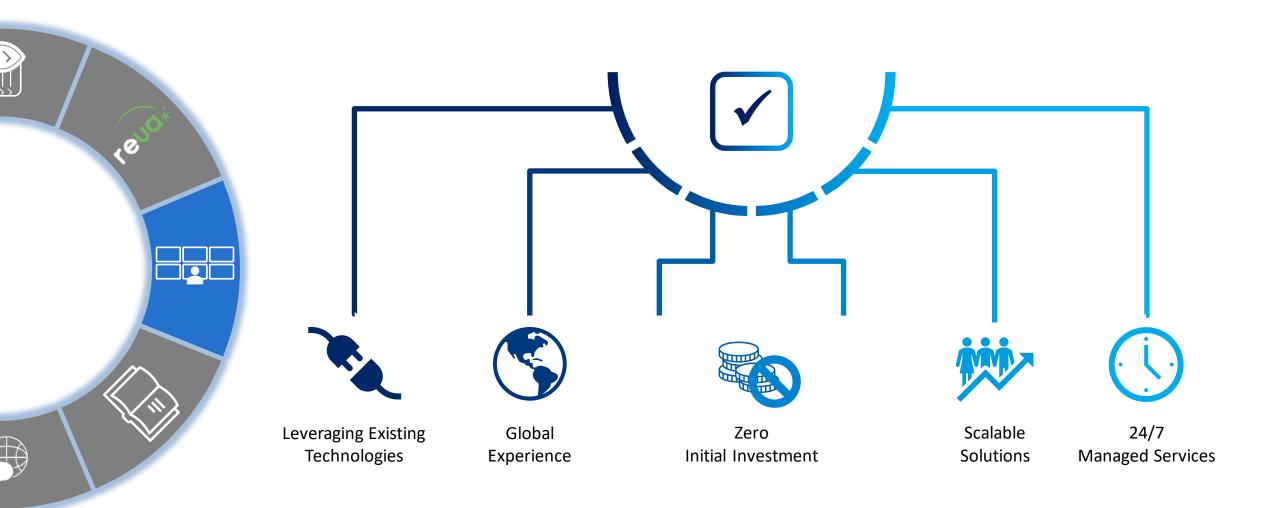


Technology





Advantages



REVA BRAND & VIP PROTECTION

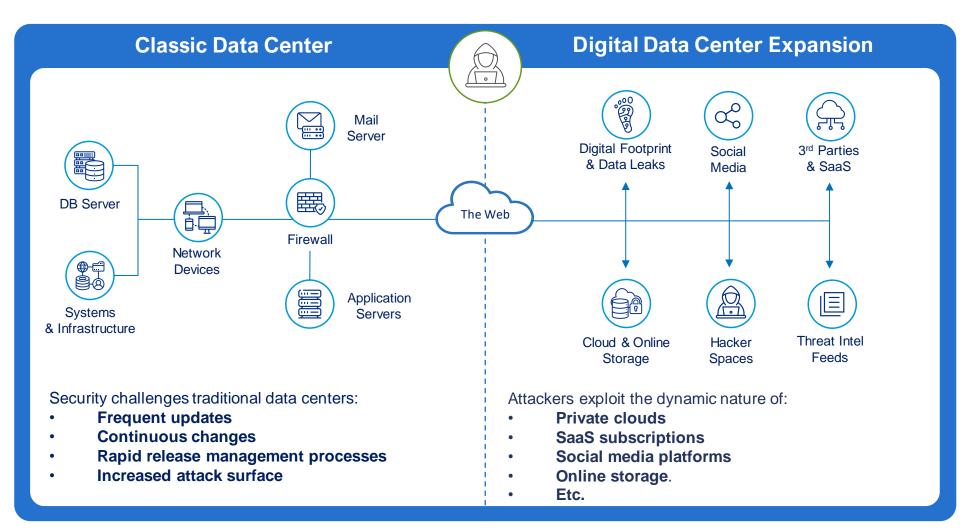
SHELT

YOUR CYBERSECURITY AS-A-SERVICE PARTNER



Data Center Expansion





REVA Modules







Protection

3rd Party & Cloud Security



Attack Surface & Vulnerability Intelligence



Tactical Cyberthreat Intelligence

Digital Risk Protection



REVA Advantages





Hyper Fast Unlimited Takedown



Holistic Social Media Intelligence (SOCMINT) Coverage



Multilingual Threat Detection and Data Scavenging



Granular Deep and Darkweb
Visibility



50+ Commercial, Opensource and CSIRT Threat Feeds



Seamless API Integration for Security Orchestration



Machine Learning and Analyst Curated Results



PII Exposure Protection

INFORMATION SECURITY SERVICES

SHELT YOUR CYBERSECURITY

AS-A-SERVICE PARTNER



VAPT, Compliance, and Best Practice



Technical & Advisory Services



Penetration Testing



Source Code Review



Digital Forensics



Business Continuity



Maturity Assessment



Technical Reviews



Governance, Risk & Compliance Services



GRC Services













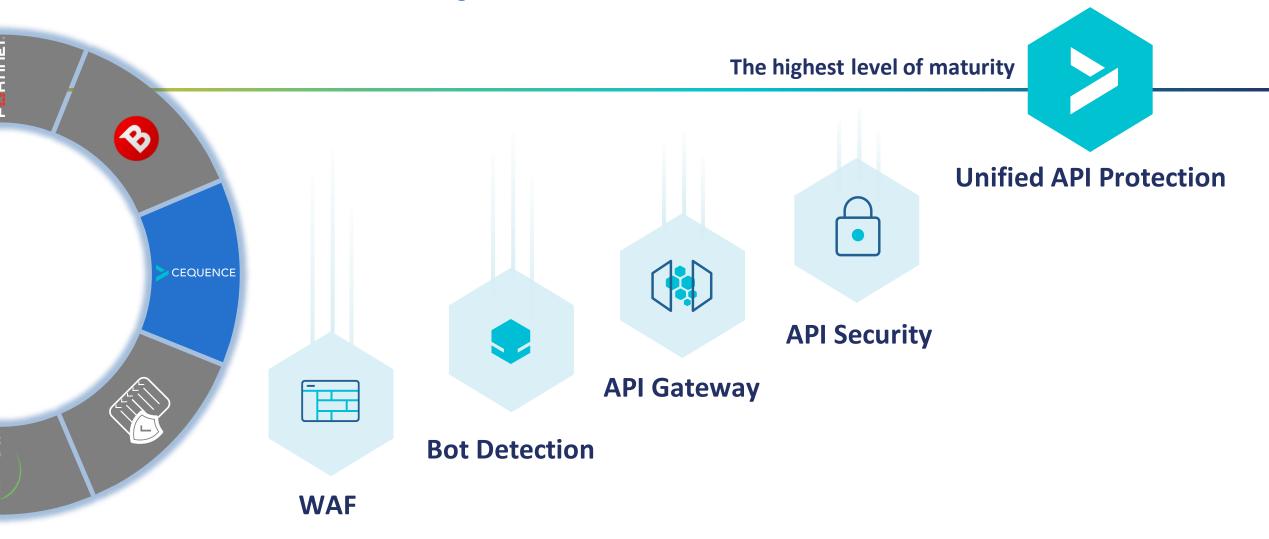
CEQUENCE API SECURITY

SHIELT

YOUR CYBERSECURITY AS-A-SERVICE PARTNER



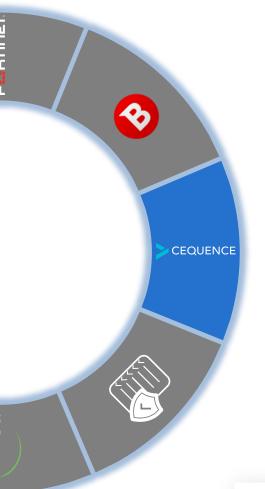
API Protection Maturity Model

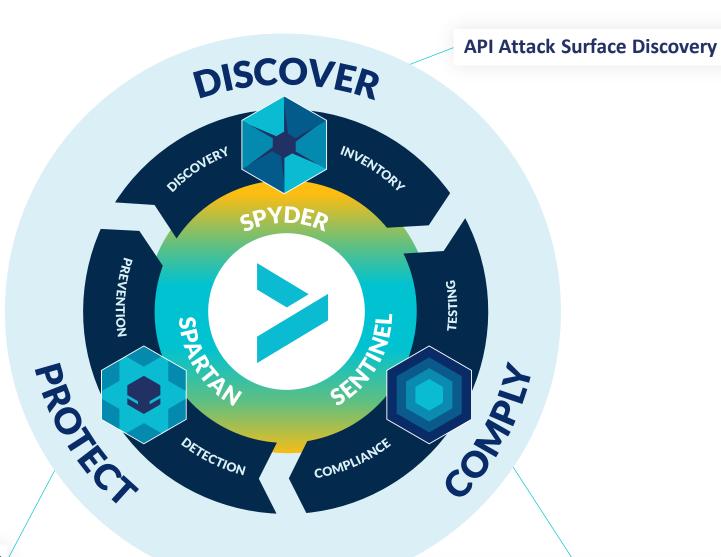


Cequence AI – Unified API Security

SHELT

API Security Pillars





API Threat Detection & Response



Cequence Deployment Options

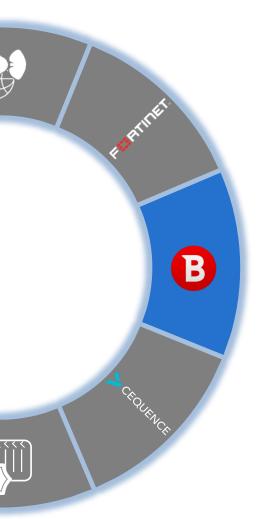
	SaaS	On-Premises	Hybrid
Deployed as	Dedicated single tenant	Microservices application	Microservices application + Network sensors or proxy
Hosted in	Cequence hosted	Customer's environment	Cequence hosted + Customer's environment
Time to deploy	15 mins	1-2 hours	1-2 hours
Data security/ privacy	PCI, SOC2, ISO certified	100% privacy Data remains in customer's environment	PCI, SOC2, ISO certified
Latency	Avg ~25 ms	0 - 5 ms	0-5 ms
Inline / passive	X Passive	✓ Passive ✓ Inline	✓ Passive ✓ Inline

BITDEFENDER

SHELT YOUR CYBERSECURITY AS-A-SERVICE PARTNER

Bitdefender – EDR

GravityZone







5. MDR Services

Expert 24x7 managed hunting and threat intelligence services



1. Prevention

Proactively reduce the attack surface at the endpoint, network & human



Automated response and actionable insights that enable remediation without system overloading



Bitdefender

GravityZone



2. PROTECTION

Stop attacks with active security technologies



3. DETECTION

Fast and intuitive detection with visibility across endpoint, network, clouds, productivity apps, and identities



GravityZone



MITIGATION

EXPLOIT

PROCECTION

DEFENSE



FILELESS ATTACK DEFENSE

TUNABLE MACHINE



SECURITY FOR **EMAIL**

SECURITY FOR

MOBIL F





INCIDENT VISUALIZATION

INCIDENT **ADVISOR**

GUIDED

RESPONSE





MANAGED DETECTION AND RESPONSE



PREMIUM SUPPORT



SERVICES



EXTENDED

RESPONSE

DETECTION AND



DEPLOYMENT SERVICES



RANSOMWARE



SANDBOX **ANALYSIS**

LEARNING



SECURITY FOR **CONTAINERS**



LIVE SEARCH



INTEGRITY



ADVISORY AND



APPLICATION CONTROL

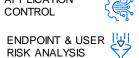
RISK ANALYSIS



FULL DISK ENCRYPTION

MANAGEMENT

PATCH



PREVENTION

WEB AND CONTENT **CONTROL & FILTERING**



NETWORK ATTACK DEFENSE



ATTACK FORENSICS



SECURITY FOR STORAGE



ANOMALY **DEFENSE**



MONITORING

PROTECTION DETECTION AND RESPONSE



DATA ANALYTICS & RETENTION



LOCAL & CLOUD MACHINE LEARNING



MALWARE DETECTION



ANOMALY DETECTIONS



THREAT INTELLIGENCE



CONFIGURATION MANAGEMENT



VULNERABILITY IDENTIFICATION



AUTOMATION & ORCHESTRATION



DASHBOARDS & INTEGRATION REPORTING APIs

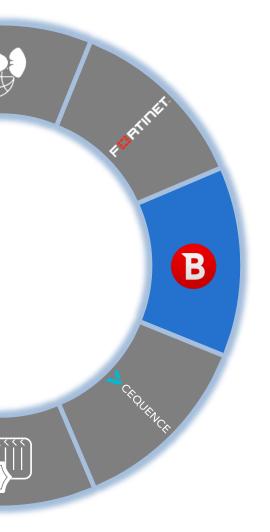
GRAVITYZONE PLATFORM

ENDPOINT | CLOUD | NETWORK | MOBILE | IDENTITY | PRODUCTIVITY | IOT DEVICES





GravityZone XDR Sensors





Identity Sensor

- Monitor, analyze, respond to events from AD, Azure AD
- Detects compromised accounts, Kerberos attacks, Brute Force and others. XDR responses include password reset or disabling accounts involved in suspicious activity



Network Sensor

- Monitor, analyze network traffic for signs of an attack
- Identifies lateral movement across the network, exfiltration, port scanning techniques, network originated Brute Force attacks



Productivity App Sensor

- Monitor, analyze, respond to O365, G Workspace events
- Detects disabled phishing protection, user creation, suspicious macros, spear phishing, exfiltration, Brute Force.
- Responses: delete suspicious emails, suspend accounts



Cloud Sensor

- Monitor, analyze security events from AWS, Azure, GCP
- Builds behavior baselines, reveals anomalies, use of Lambda function, encryption removal, monitoring services removal, reconnaissance, login failures, etc.

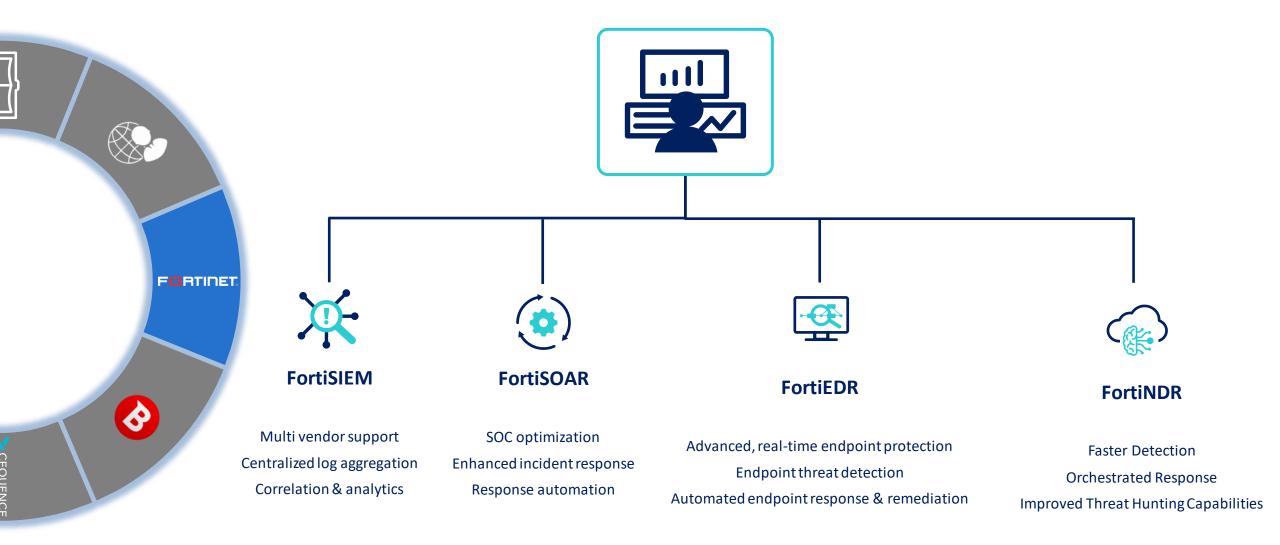
FORTINET

SHELT YOUR CYBERSECURITY

AS-A-SERVICE PARTNER



SOC Toolkit





FortiSIEM

Performance & Availability

- Discovery Driven
- Configuration Change Detection
- Custom Monitoring
- Synthetic Transaction Monitoring
- Business Service SLA

Next-Generation SIEM

- Cross-Domain Event Correlation
- Discovery Driven Event Context
- File Integrity Monitoring
- Dynamic Identity & Location

Infrastructure Discovery

- Relationships Discovery
- Comprehensive Physical, Virtual, Cloud
- Automatic CMDB
- Ping, L2, Range, Smart, AWS Scan



- Compliance Management Dashboard
- Compliance Reports-SOX, HIPAA, PCI, etc.
- Built-in compliance rules & widgets



- Baseline & Trend Analysis
- Outlier/Anomaly Detection
- Flow Analysis
- Statistical Anomaly Based
- UEBA

Security & Operational Intelligence

- Visual Analytics
- Dynamic Dashboards
- Inline Reporting
- Mobile Ready

Superior Architecture

- Univfied, HW and VM, single data lake
- Multi-Tenant (Service Provider Ready)
- Scale Out Architecture
- Role-Based Access Control

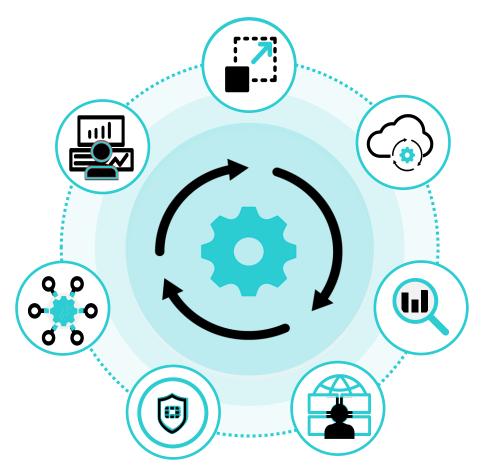








FortiSOAR



Centralize, standardize & automate IT/OT security operations

Connect anything – automate everything

500+ integrations, 800+ playbooks, robust use-case solutions for SOC/NOC/OT

Security incident response

Automated triage, enrichment, investigation, case mgmt, collaboration, and response actions

Threat Intelligence management

Powered by FortiGuard Labs and any public source

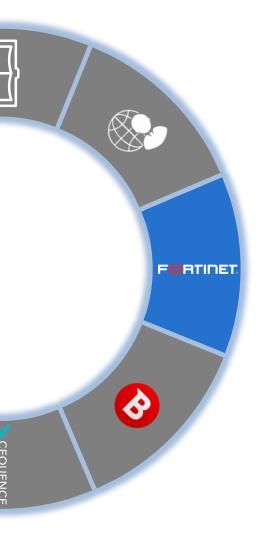
Asset and vulnerability mgmt

IT/OT risk-based tracking and remediation playbooks

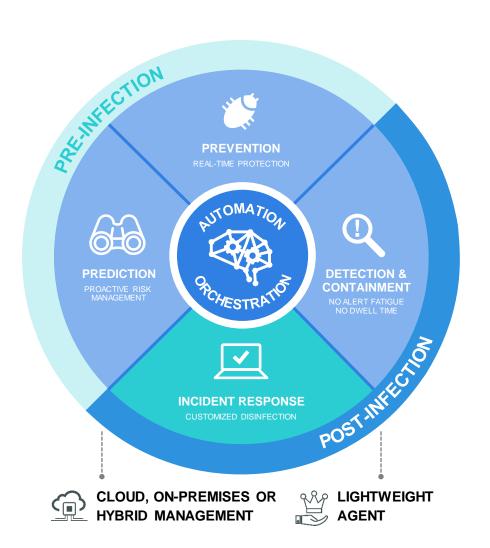
No/low-code playbook creation

Patented development modes for any user and workflow

FortiEDR



- Unified agent by design
- ML and Behavior-based protection
- Continuous classification by cloud-based AI
- Support for legacy OSes and hybrid environments
- Low TCO
- Lightweight agent
- Secure remote remediation
- Tamper-proof & evasion resistent
- Strong third-party results
- Managed options available





FortiNDR







Faster Detection

- Al / ML models designed to detect anomalous and malicious activity
- Virtual, human, and behavioral analysis reduces false positives
- Detections mapped to MITRE ATT&CK framework



Orchestrated Response

Integrates with Fortinet Security Fabric and SOAR, SIEM and XDR tools to automate response



Improved Threat Hunting Capabilities

- 365-day network metadata retention
- Proactive investigation tools
- Guided playbooks for hunting efficiency

THANK YOU

SHELT YOUR CYBERSECURITY AS-A-SERVICE PARTNER