40Minutes to Grow your Business Focus on FortiEDR

Introducing Fortinet's EDR Solution

Kash Valji
Director Consulting Systems Engineering

Agenda

- Endpoint Market
- Introduction to FortiEDR
- Effective Automated Response
- FortiResponder (Fortinet MDR)
- Licensing (May 2020 Update)
- Fabric Integration

Challenges in Endpoint Security

The Threat Landscape continues to evolve

Vulnerability management remains a challenge

Direct cloud access bypasses network control

Gartner®

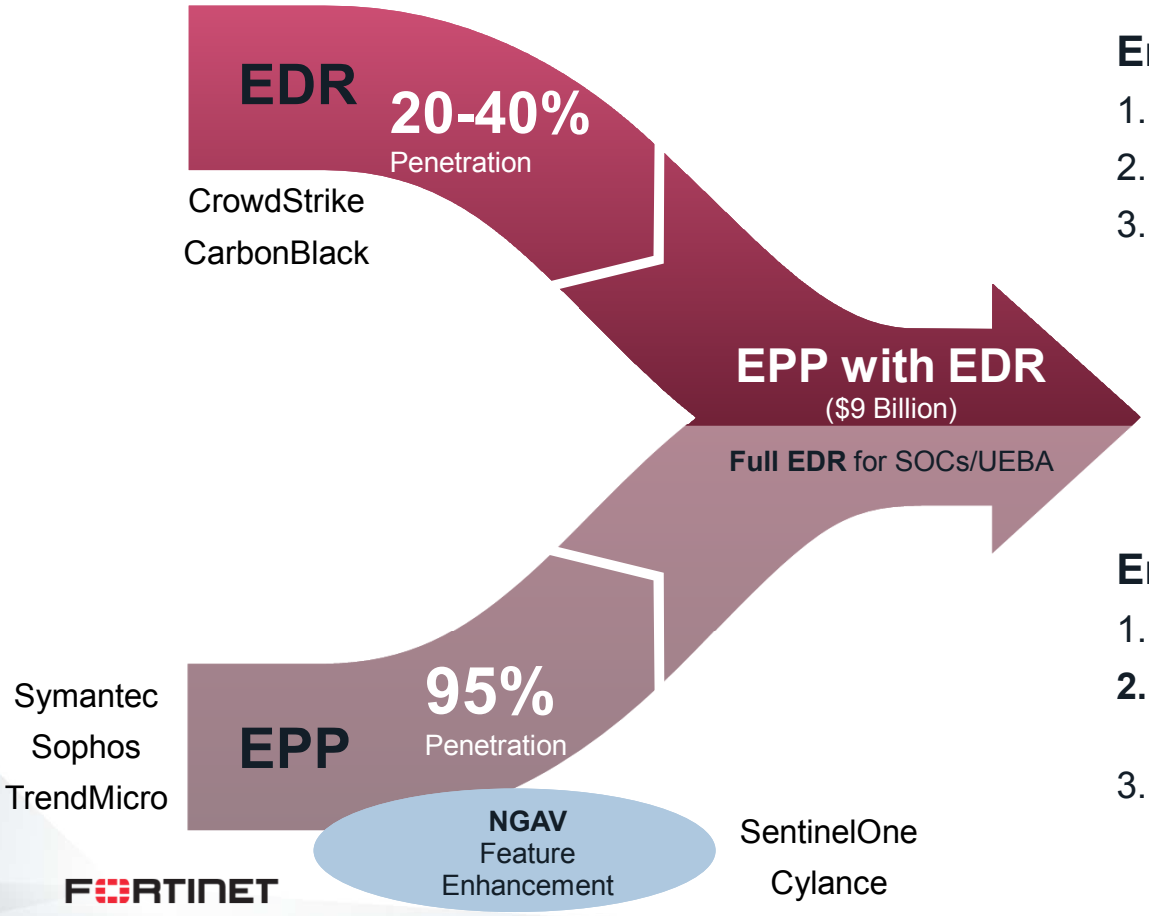
The security mindset has shifted to acknowledge that prevention alone is not enough; security and risk management leaders must be able to more easily harden endpoints and perform more detailed incident response to resolve alerts.

Notes/Sources:

1. Gartner Magic Quadrat for Endpoint Protection Platforms, August 2019.

Evolution of EPP

Advanced Endpoint Protection Platform (EPP) with Automated Detection and Response Capabilities



Endpoint Detection and Response (EDR)

1. Record and store endpoint behaviors and events
2. Detect security incidents
3. Response
    1. Containment and remediate
    2. Forensic—investigate security incidents, root cause analysis

Endpoint Protection Platform (EPP)

1. Prevent file-based malware
2. **Detect** and block malicious activities from *trusted* and untrusted applications
3. Provide the investigation and remediation capabilities to **respond** to security incidents and alerts

FORTINET

Market Opportunity

Worldwide Corporate Endpoint Security Forecast

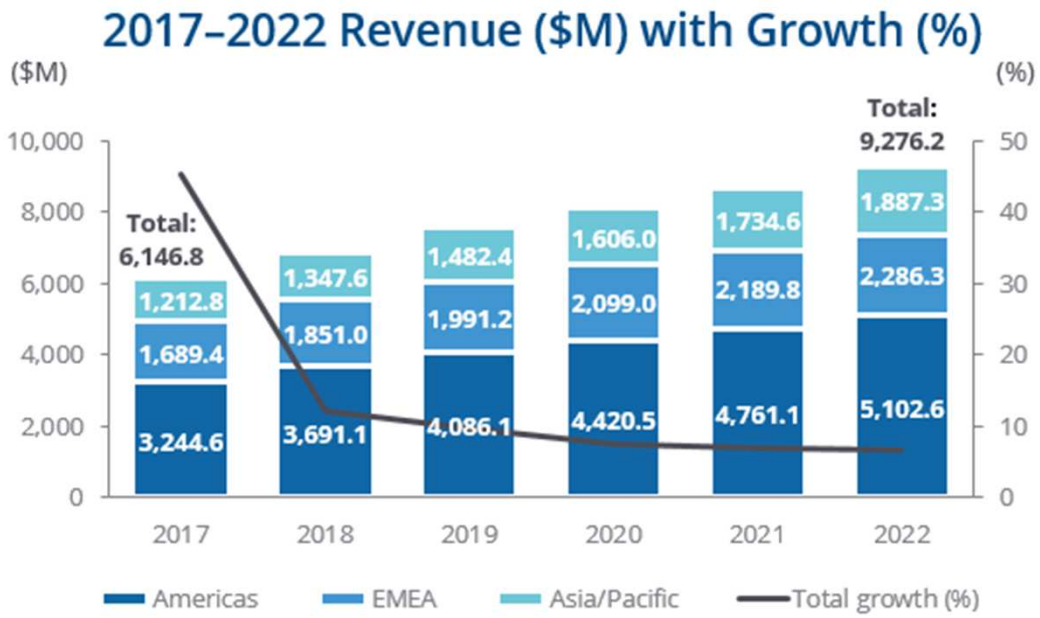
$9.2 billion in 2022

8.6% CAGR

EMEA: 2.28 Billion and CAGR 6.2%

APAC: 1.88 Billion and CAGR 9.2%

Americas: 5.1 Billion and CAGR 9.5%



Endpoint Pain Points

Compromised Endpoints

- There is no 100% prevention
- Threat landscape - Ransomware, data theft, business disruption
- Need better detection. Reduce time to contain, time to remediate

Incident Response – cost, pain and business disruption

- We all want to stop the breach, but at what cost?
- Alert fatigue, false positives
- Blunt tools and Manual response
- Business disruption, machine off-line, lost of productivity, user complaint

Not enough security expertise in house, other resource constrains

- Need to accelerate SOC maturity,
- Need to scale SOC capacity
- Don’t have time to patch, can’t upgrade all machines

Complex security eco system, too many point solutions

- Need Integrated solution

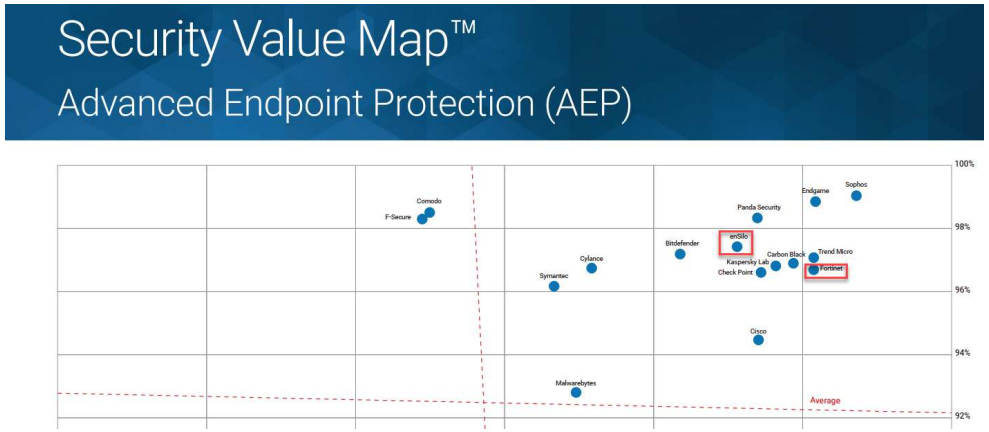
Introducing FortiEDR

FEDR provides host-based next generation AV along with endpoint detection and response (EDR), including automated orchestration

- **Top-rated Next Gen Endpoint Protection**
  Multiple machine learning-based engines provide NSS Labs recommend advanced endpoint protection
- **Behaviour-based EDR**
  Host-based code tracing and other techniques assess runtime operation, detect suspicious activity
- **Automated Orchestration Framework**
  Cloud-based analytics provide incident classification and predefined playbooks enable automated response

NSS Labs AEP

2019 Report



Impressive Results from the last NSS Labs report:
~97.9% on NGAV (pre-execution) engine,
~99.8% with pre- and post-infection policies
~99.9989 with pre- post-infection and playbooks applied

2020 Report

“Comprehensive, robust management. Overall protection impressive; low false positive rate; excellent resistance to evasion. Excellent malware protection; strong exploit protection.”

FortiEDR – Real-time Endpoint Protection at Pre- and Post-Infection

Pre-Infection

Discover & Predict

Proactive risk mitigation

- Discover rogue devices & IoT
- Application and reputation
- Vulnerabilities
- Risk-based policies reduces attack surface
- Virtual patching

Prevent

Pre-execution protection

- Kernel-level
- Machine learning & Signature-less
- Application communication control
- Eliminate data tempering and exfiltration

Post-Infection

Detect

Detect threats in real time

- No alert fatigue
- Provide malware classification
- Display IOC's
- Deliver full attack chain

Defuse

Stop Breach and data loss

- First and only real-time post infection blocking
- Block outbound communication
- Prevent data exfiltration
- Prevent data tempering and ransomware encryption

Respond & Investigate

Full attack visibility

- Customizable incident response playbooks
- Eliminate dwell time
- Capturing forensic data
- Memory snapshot for file less attack
- Conduct threat hunting in your time

Remediate & Roll back

Dis-infection

- Rollback malicious changes
- Remove bad files
- Clean up persistency
- Eliminate re-image/rebuild
- Ensure business continuity
- REST API output for external remediation tools

Fortinet EPP and EDR

FortiClient

- Endpoint Protection
  - **Vulnerability scanning/ patching**
  - CPRL – **AV**
  - Anti-Exploit
  - Web filtering
  - Application firewall (SaaS Control)
- Fabric Agent Connectivity
  - Endpoint telemetry
  - **Application inventory**
  - Dynamic Access control
- Secure Remote Access
  - VPN Agent
  - SSO

FortiEDR

- Endpoint Protection
  - ML-based **AV**
  - **Application discovery**
  - **Vulnerability scanning / Virtual patching**
- Ransomware Protection
  - Data protection
  - File-less attack detection/protection
- Endpoint Detection and Response
  - Attack surface reduction – Virtual patching
  - Post-execution detection (behavioral-based)
  - Automatic Threat containment, remediation/roll back
- Forensic Investigation
- Threat hunting
- MDR (Managed Detection and Response) Service

Minimal Overlap

Elements of AV – pre-execution protection

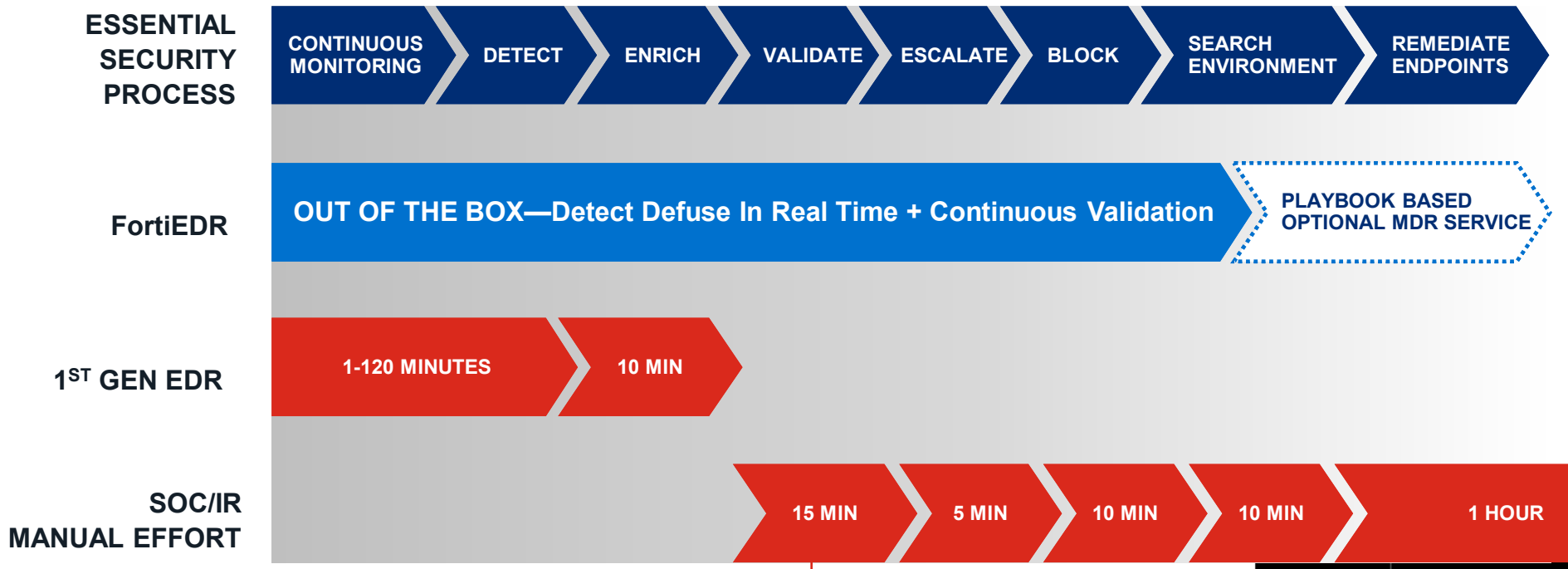
Attack surface reduction - Vulnerability scanning

Fortinet Endpoint Solutions

Quick Snapshot

- FortiInsight – User and entity behaviour analytics (UEBA)
- FortiNAC – Fortinet Network Access Control
- FortiClient – Next-Generation Endpoint Protection
- FortiEDR - Fortinet EDR Solution (aka enSilo)
- FortiSIEM

Real Time Vs. Manual Response

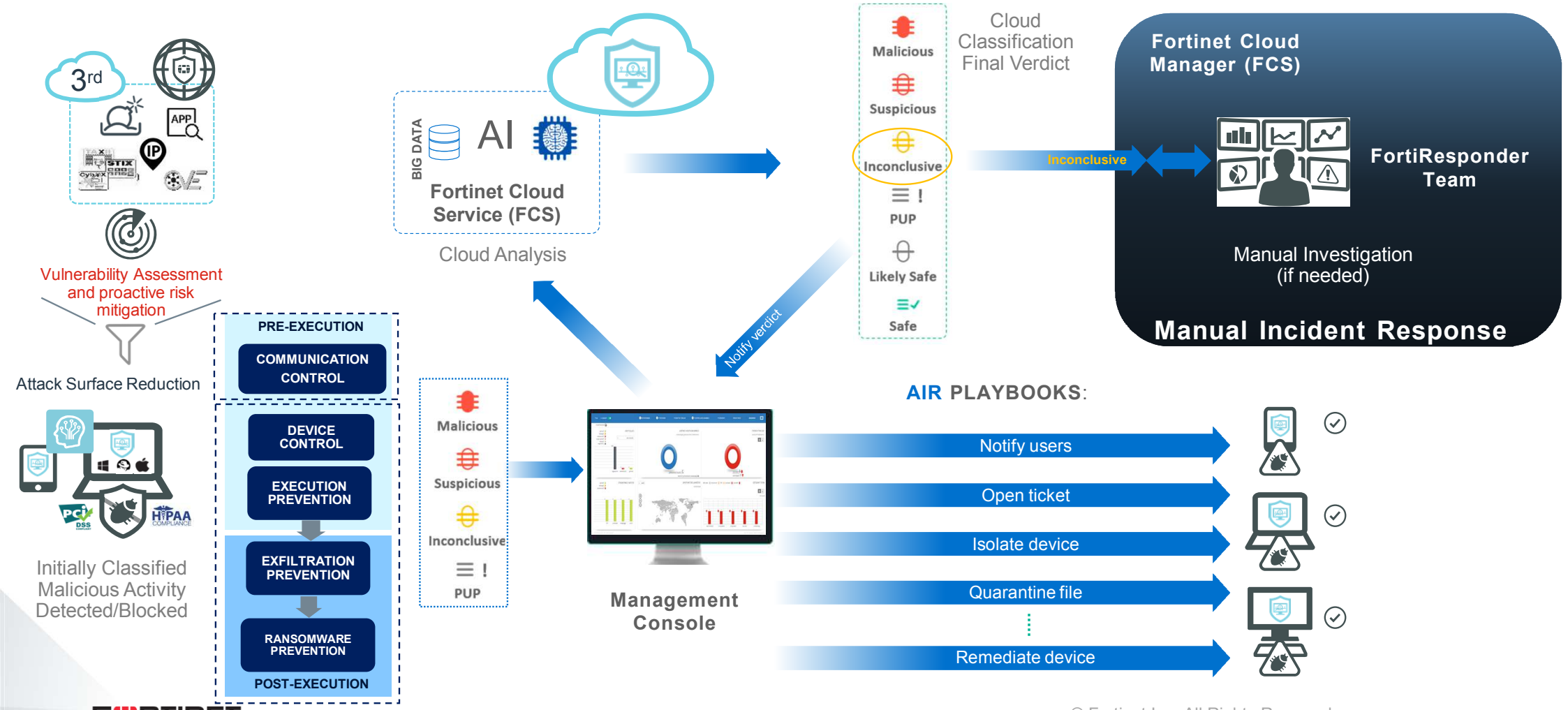


FUNCTION	MANUAL EDRs	FortiEDR Automation
L1 SOC Analyst		AUTOMATED VIA SOFTWARE
L2 SOC Analyst		
Security Engineer		
Incident Handler		
Forensic Investigator		
Hunt Analyst		IF REQUIRED
Managers		

"EDR tools are not very useful for organizations not prepared to handle alerts." - Gartner

FORTINET

FortiEDR – High Level Workflow



FortiEDR Competitive Advantages

Protection Efficacy

Attack Surface Reduction

- Discovery: vulnerability, applications, rogue devices
- Virtual patching

Real Time Protection

- Pre- and post-infection with automated containment
- Stop breach and ransomware destruction
- Offline Protection

Automated Detection and Response

- Behavioral-based detection
- Orchestrated, automated remediation (with playbooks)
- No business disruptions

Forensic Investigation and Threat Hunting

- 6 months of data retention
- Retrieve memory snapshot for File-less malware investigation
- Patented Code-Tracing technology – attack story drill down

Operational Efficiency

Light and Fast

- 60-120 MB RAM
- Less than 1% CPU
- Minimal network traffics (1.5 kb per host)

Minimise Post Infection Disruption

- Containment and remediation without taking machines off-line
- Remediate and roll back malicious changes
- Eliminate the need to re-image

Platform Coverage

- Windows XP SP2/SP3, 7,8,8.1 and 10
- Windows Server 2003 R2 SP2, 2008 R2 SP2, 2012, 2012 R2, 2016 and 2019
- MacOS Versions – Yosemithe (10.10), El Captain (10.11), Sierra (10.12), High Sierra (10.13) and Mojave (10.14)
- Linux Versions – Redhat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7, and Ubuntu LTS 16.04.5, 16.04.6, 18.04.2 server, 64-bit only
- VDI Environments – VMWare Horizons 6 and 7 and Citrix Desktop 7

Deployment Options

- Cloud, on-prem, and hybrid
- Supports Air-gapped systems
- Supports multitenancy for MSSP/MDR providers

So, what does this mean for Fortinet, Channel and Customers?

- What this adds to Fortinet's offerings:
  - Fortinet Security Fabric Customers – additional integrated solution for security efficacy and SOC optimisation
  - Enterprise customers (non-Fortinet) that looking for advanced / automated EDR, can consider FEDR with confidence

- Key business benefits for Enterprise Customers:
  - Real-time detection, containment and response to cyber threats
  - Maintain business continuity, availability, without disrupting user productivity – top ask in in OT environments
  - Cap OpEx Incident Response (IR) expenses & Address cyber security skill shortage
  - Multi-tenancy Cloud infrastructure for MSSP
  - Integrated platform that reduces complexity, optimise SOC operations

FortiResponder Services

Managed Detection and Response

Incident Response Services

FortiResponder Team

24x7 Security Operations Center

The Team is comprised of individuals with expert knowledge in:

- Malware Hunting/Analysis
  Reverse Engineering
- Multiple Scripting Languages
- Forensics
- Incident Response
  Processes
- Threat Actors TTPs
- Multi-National Analysts

FORTIGUARD LABS

FortiResponder Managed Detection and Response

24x7 Monitoring and Response

Continuous
Monitoring

FortiResponder MDR provides organizations with 24x7 continuous threat monitoring, alert triage, and incident handling by experienced analysts and the FortiEDR platform

Available as an add-on subscription

FortiResponder - Incident Response Service

Remote Services Only

Per Incident

Forensics and Incident Response

SOW-based (hourly = $500) remote forensic analysis and incident response

Assists clients with the analysis, response, containment and remediation of security incidents leveraging **FortiEDR** to decrease the time to resolution limiting the overall impact to an organization.

The team may also perform additional analytics, including analysis of available and relevant logs from **firewall/NetFlow, VPN, web proxy, IDS/IPS, SIEM**, and additional forensics artifacts as well as detailed **analysis of files and memory for discovery of malicious payloads**.

FortiEDR
FortiGate
FortiAnalyzer
FortiNAC
3rd Party
XD

FortiSOAR

FortiGate
FortiNAC
3rd Party
Active Directory
FortiSIEM
XR

FortiResponder Mission

Ensure all events are handled

Threat Detection and Analysis

- Analyzing malware both static and dynamic
- Analyzing memory for malicious processes
- Identifying potential vulnerable and unwanted programs
- Environment tuning - Setting micro exceptions for clean applications
- Retrieval and analysis of additional forensic artifacts

Containment and Remediation

- Tactical containment options
  - Stop process, Block comms
- Guided Remediation/Recommendations options (Short and Longer Term)
  - Terminate process, Removal of file, Remove persistency

Reporting and Alerting

- Alerts addressed within 24 hours – Notifications
- Annual reporting
- Escalation Requests – Threat Analysis, Guided Recommendations

Training

Benefits

FortiResponder Managed Detection and Response

Accelerate SOC Maturity

24/7 - Scale the Existing SOC

Reduce Analyst Burnout

Licensing

Licensing from May 2020

May Pricelist – Revised SKUs

- Bundle Prices are Endpoint based (per seat)
- Bundles are sold in packs - 25, 500 and 10,000 seat packs
- Rules regarding Seat count
  - < 250 = is for customers found by MSSP certified FortiEDR partners only (can not be done via referral)
  - 250 – 500 = direct but only the most expensive SKU (Complete + FortiResponder)
  - > 500 = standard

Licensing from May 2020

Ordering/SKU Terminology

PREDICT - Asset Discovery and Attack Surface Reduction

- Application Discovery, Communication Control and Vulnerability Management

PROTECT - Pre-infection and post-infection real-time protection

- NGAV Pre-infection, Device Control, Ransomware and Exfiltration post-infection protection

RESPONSE – EDR

- Data retention for Threat hunting event - 6 months, Deep Forensics Overview and Control, Attack Graph with Code Tracing

ALERT MONITORING SERVICE – MDR

- 24x7 threat monitoring and incident triage Email notifications, Quarterly and Annual threat intelligence reports, Guided remote remediation, Orchestrated response playbook setup

FortiEDR Licensing and Bundles

- Price Per endpoint, sold in packs
  - No distinctions between Servers and Workstations
  - 25, 500 and 10,000 packs
  - Most have a minimum of 500 endpoints
- Deployment service is **mandatory** for new customers
- 24x7 Managed Detection and Response (MDR) service –
  - **Should be included** in quote
  - Price per endpoint
  - Quantity must **match** the totally number of endpoints ordered

	PREDICT AND PROTECT	PROTECT AND RESPONSE	COMPLETE (PREDICT, PROTECT AND RESPONSE)	COMPLETE + MDR	COMPLETE FOR AIR-GAPPED
Target Use Case	AV Replacement	EPP/EDR full Suite Price Sensitive	Mature Org, not as price sensitive	Require Managed Detection and Response Service	Critical, air-gapped infrastructure
Discovery	√		√	√	√
Pre and Post Infection Protection	√	√	√	√	√
Forensic and Threat Hunting		√	√	√	√
MDR Service	Optional Add On	Optional Add On	Optional Add On	√	
On-prem or cloud	Cloud and Hybrid	Cloud and Hybrid	Cloud and Hybrid	Cloud and Hybrid	On-Premise
Deployment service	Mandatory	Mandatory	Mandatory	Mandatory	Optional

FORTINET

FortiEDR Licensing and Bundles

- Default deployment options
  - Cloud or Hybrid
  - On-prem – requires the air-gapped SKU
- Use combination of the packs to achieve the quantity
  - i.e. 600 endpoint = 600 endpoints – 1x 500pack + 4x25 pack
  - 1200 endpoints = 2x500 pack + 8x 25
- Most SKU has **minimum** order Quantity **500** endpoints

	PREDICT AND PROTECT	PROTECT AND RESPONSE	COMPLETE (PREDICT, PROTECT AND RESPONSE)	COMPLETE + MDR	COMPLETE FOR AIR-GAPPED
Target Use Case	AV Replacement	EPP/EDR full Suite Price Sensitive	Mature Org, not as price sensitive	Require Managed Detection and Response Service	Critical, air-gapped infrastructure
Discovery	√		√	√	√
Pre and Post Infection Protection	√	√	√	√	√
Forensic and Threat Hunting		√	√	√	√
MDR Service	Optional Add On	Optional Add On	Optional Add On	√	
On-prem or cloud	Cloud and Hybrid	Cloud and Hybrid	Cloud and Hybrid	Cloud and Hybrid	On-Premise
Deployment service	Mandatory	Mandatory	Mandatory	Mandatory	Optional

FORTINET

Fortinet Fabric Integration

FortiEDR Fabric Integration

Overview

FortiEDR leverages the Fortinet Security Fabric architecture and integrates with many Security Fabric components including

- FortiGate
- FortiSIEM
- FortiNAC
- FortiSandbox
- FortiGuard Labs

Existing Integration

- FortiGate
  - Threat intelligence sharing
  - Triggering enhanced response actions - such as suspending or blocking an IP address following an infiltration attack
- FortiSIEM – Two Way integration
  - Endpoint Alerts → FortiSIEM
  - Alert triage/ verification SIEM → interrogate endpoint hosts
- FortiSandbox
  - Threat Intelligence sharing
  - Analyse malicious objects
- FortiNAC
  - FortiEDR shares endpoint threat intelligence and discovered assets with FortiNAC
  - Triggering enhanced response actions - such as isolating a device
- FortiGuard Labs
  - Up-to-date Intelligence, supporting real-time incident classification to enable accurate incident response playbook activation.

Training resources

Available Resources

- Available resources – on Fortinet partner portal and Fortinet website
- NSE training
- Fast Track
- Local Channel Team for Demo’s, Proof of Concepts, RFP Assistance etc etc


FORTINET