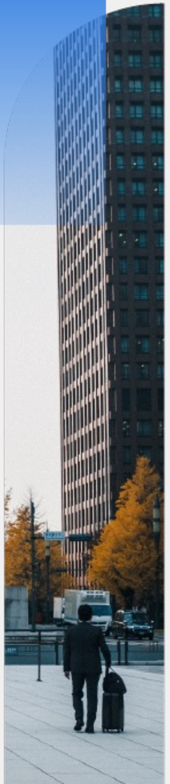
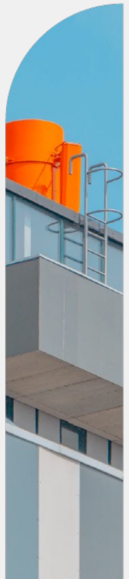
FORTINET



Ochrana koncových zariadení
Fortinet Endpoint Detection and Response / XDR

Juraj Belko, Systems Engineer

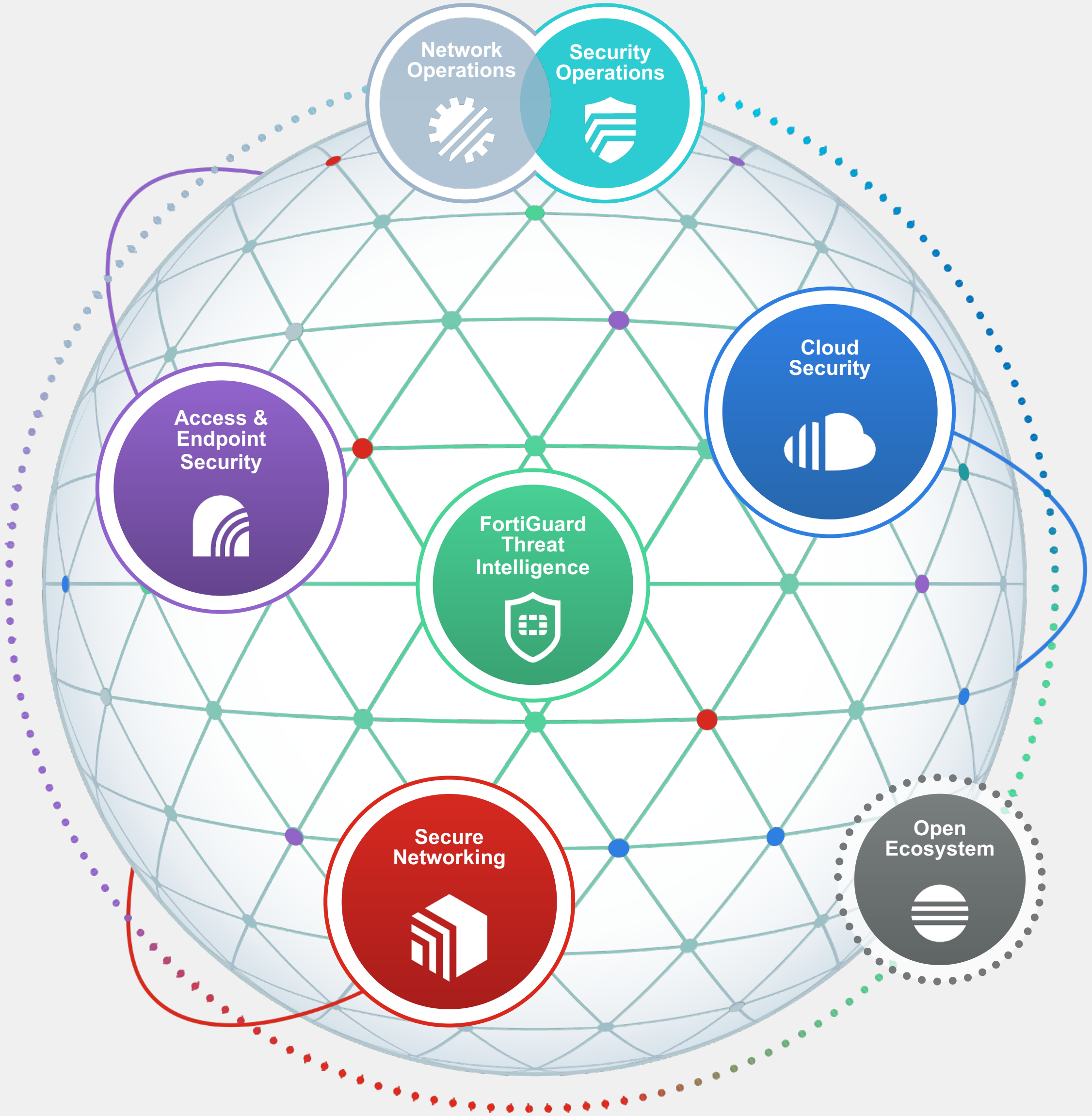


Agenda

01 Modern Endpoint Security

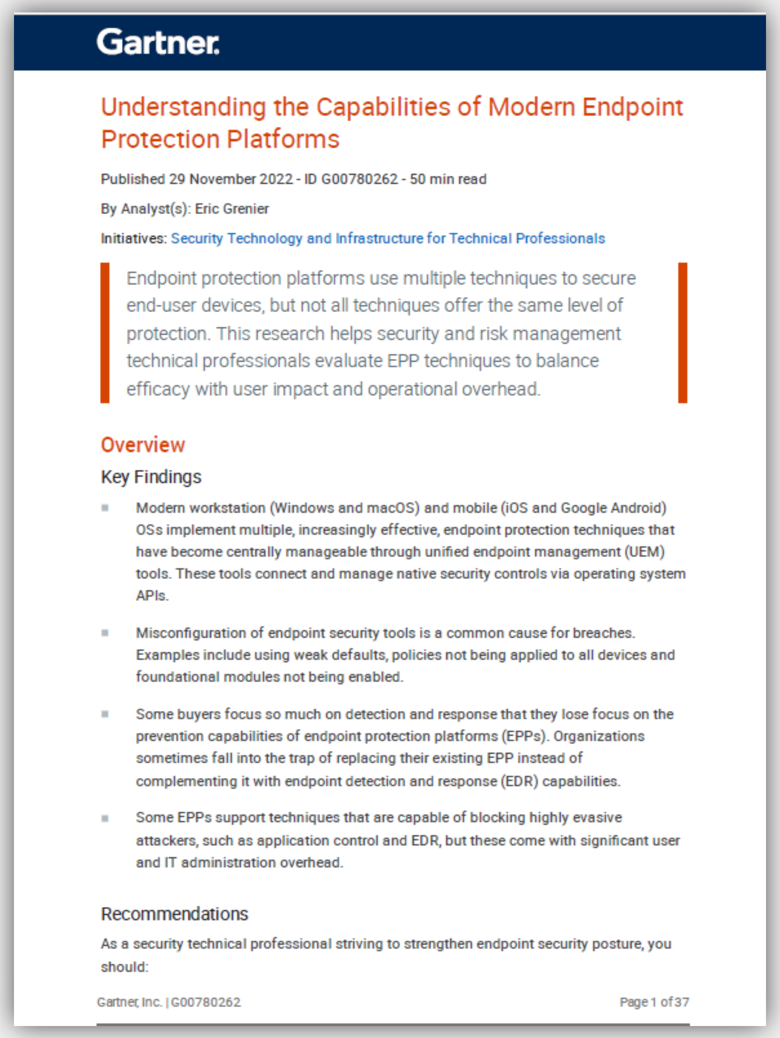
02 Integrations

03 Extended Detection & Response



The Pros and Cons of Various Malware Protections

Strength of protection versus accuracy / ease of use



Gartner.

Understanding the Capabilities of Modern Endpoint Protection Platforms

Published 29 November 2022 - ID G00780262 - 50 min read

By Analyst(s): Eric Grenier

Initiatives: Security Technology and Infrastructure for Technical Professionals

> Endpoint protection platforms use multiple techniques to secure end-user devices, but not all techniques offer the same level of protection. This research helps security and risk management technical professionals evaluate EPP techniques to balance efficacy with user impact and operational overhead.

Overview

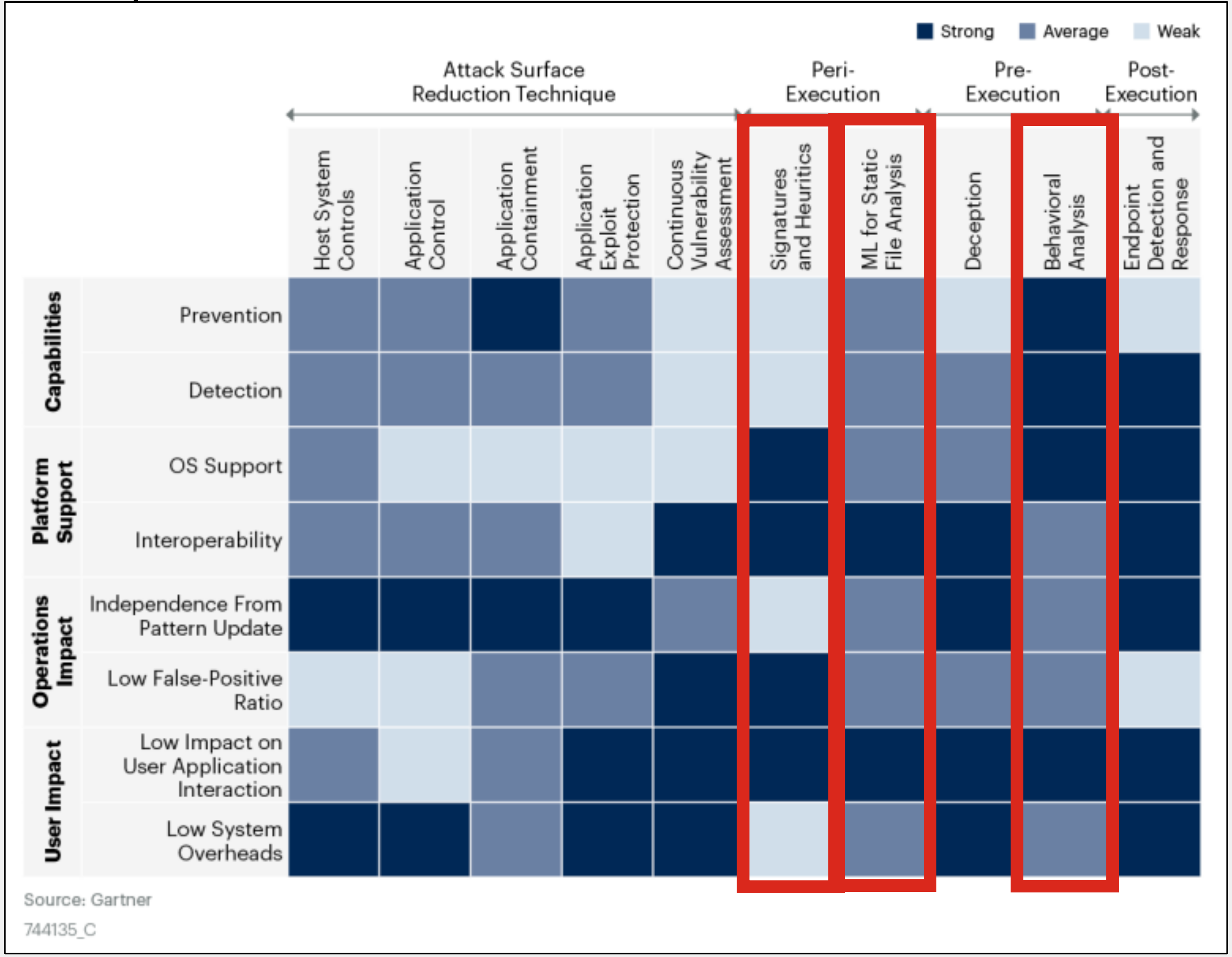
Key Findings

- Modern workstation (Windows and macOS) and mobile (iOS and Google Android) OSs implement multiple, increasingly effective, endpoint protection techniques that have become centrally manageable through unified endpoint management (UEM) tools. These tools connect and manage native security controls via operating system APIs.
- Misconfiguration of endpoint security tools is a common cause for breaches. Examples include using weak defaults, policies not being applied to all devices and foundational modules not being enabled.
- Some buyers focus so much on detection and response that they lose focus on the prevention capabilities of endpoint protection platforms (EPPs). Organizations sometimes fall into the trap of replacing their existing EPP instead of complementing it with endpoint detection and response (EDR) capabilities.
- Some EPPs support techniques that are capable of blocking highly evasive attackers, such as application control and EDR, but these come with significant user and IT administration overhead.

Recommendations

As a security technical professional striving to strengthen endpoint security posture, you should:

Gartner, Inc. | G00780262 Page 1 of 37



■ Strong ▨ Average □ Weak

		Attack Surface Reduction Technique					Peri-Execution		Pre-Execution	Post-Execution	
		Host System Controls	Application Control	Application Containment	Application Exploit Protection	Continuous Vulnerability Assessment	Signatures and Heuritics	ML for Static File Analysis	Deception	Behavioral Analysis	Endpoint Detection and Response
Capabilities	Prevention	▨	▨	■	▨	□	□	▨	□	■	□
	Detection	▨	▨	▨	▨	□	□	▨	▨	■	■
Platform Support	OS Support	▨	□	□	□	□	■	▨	▨	■	■
	Interoperability	▨	▨	▨	□	■	■	■	■	▨	■
Operations Impact	Independence From Pattern Update	■	■	■	■	▨	□	▨	■	▨	■
	Low False-Positive Ratio	□	□	▨	▨	■	■	▨	▨	▨	□
User Impact	Low Impact on User Application Interaction	▨	□	▨	■	■	■	■	■	■	■
	Low System Overheads	■	■	▨	■	■	□	▨	■	▨	■

Source: Gartner

744135_C

How to Break The Attack Sequence

MITRE Pre-ATT&CK

MITRE ATT&CK

	Recon	Weapon	Delivery	Exploit	Installation	C2	Action
Products & Solutions	FortiRecon FortiDeceptor	FortiRecon FortiDeceptor	FortiGate (HW/VM/CN/SASE) FortiProxy FortiClient FortiEDR FortiADC FortiWeb FortiNDR AV+ANN FortiMail FortiCASB FortiCWP	FortiGate (HW/VM/CN/SASE) FortiProxy FortiClient FortiEDR Defuse compromised endpoint FortiADC FortiWeb Web application FortiDeceptor Threat detection, analysis, and response FortiSIEM UEBA	FortiGate (HW/VM/CN/SASE) FortiClient FortiEDR Defuse exploit FortiDeceptor Defuse Lateral Movement FortiCWP FortiSIEM UEBA	FortiGate (HW/VM/CN/SASE) FortiClient FortiEDR Defuse compromised endpoint FortiNDR FortiSIEM UEBA	FortiAnalyzer Event handlers & reports FortiSIEM Rules Engine & Threat Hunting FortiSOAR Playbooks IOC Threat hunting Outbreak Detection ZTNA Auto tagging FortiClient Endpoint search FortiEDR|XDR FortiDeceptor Threat intelligence, & attack isolation
FGD AI-Powered Security		Credential Stuffing Prevention Service	Anti-malware, AV pre-Filter, SBX, Endpoint Vulnerability Protection, App Control, IL CASB, Credentials AV IL SBX IL CASB	IPS, Application, FW, IOT, OT IPS IoT OT	URL, AV URL AV	Botnet, C2, DNS BOT C2 DNS	

SOC Augmentation By FortiGuard

Know Your Risks & vulnerabilities
Security Assessments

Train your SOC
IRR, Playbooks, Training

Managed Detection & Response
MDR

Augment your SOC
SOC as a Service

Respond Faster and More Effectively
Incident Response

FortiEDR

Patented Behavior-based Approach

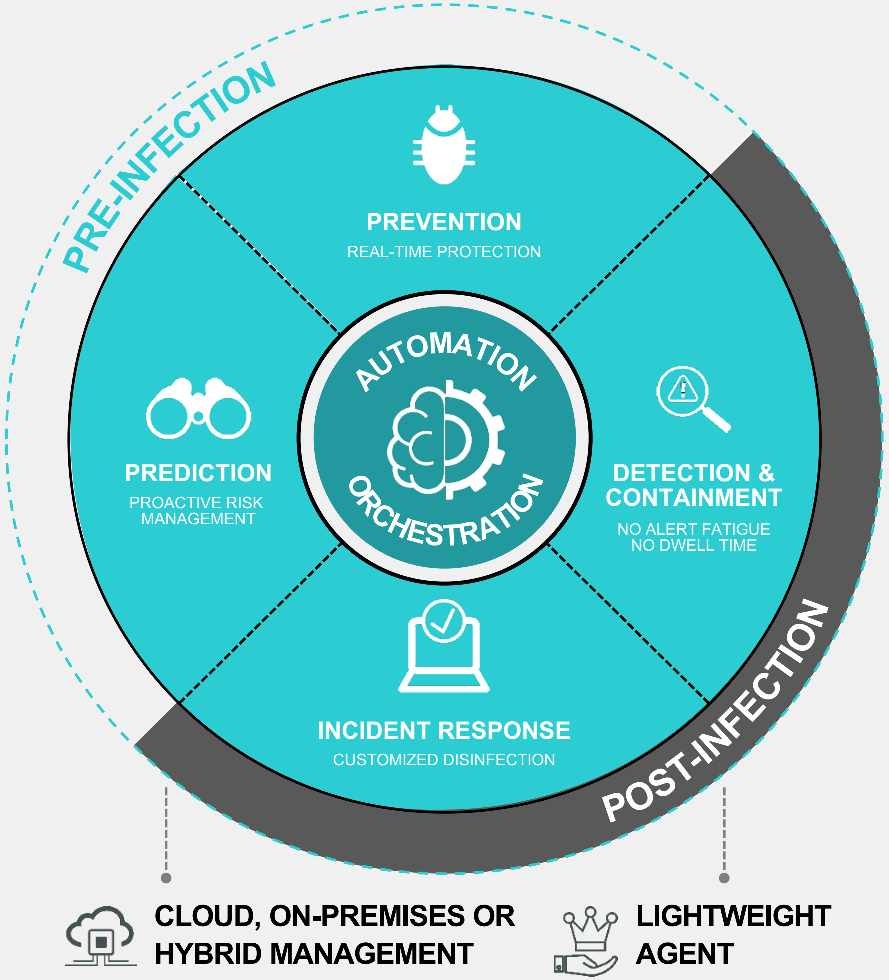
Automated or Augmented Response

Endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malwere

FortiEDR Design Principles

Cloud-native Endpoint Protection, Detection & Response

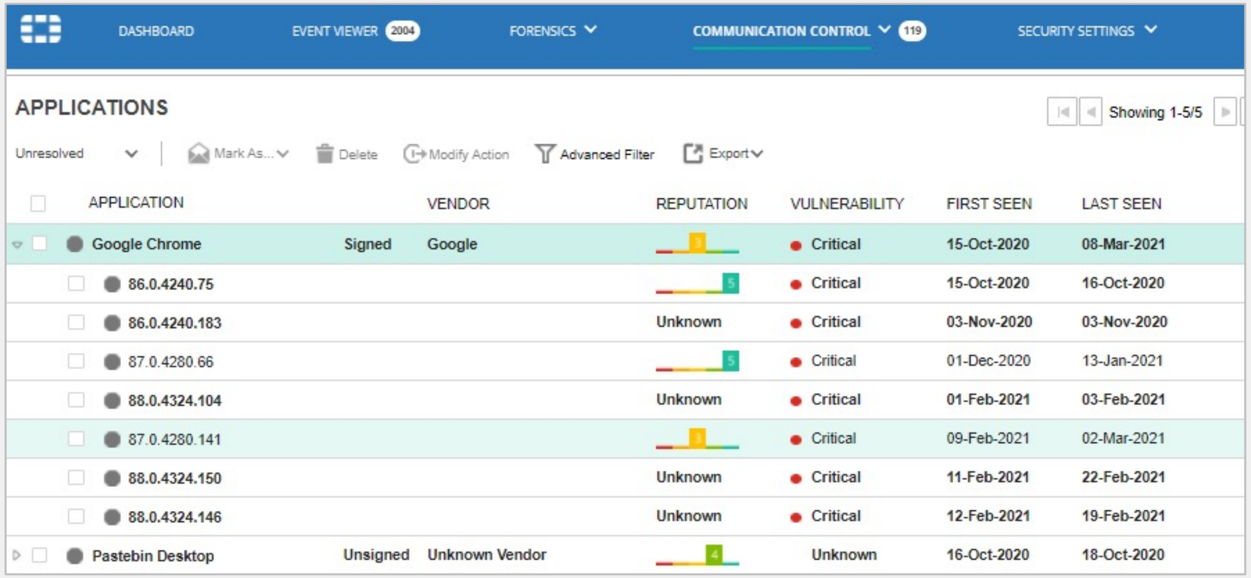
- Unified agent by design
- ML and Behavior-based protection
- Continuous classification by cloud-based AI
- Support for legacy OSes and hybrid environments
- Low TCO
- Lightweight agent
- Secure remote remediation
- Tamper-proof & evasion resistent
- Strong third-party results
- Managed options available



Proactive Attack Surface Reduction

DISCOVER, ENRICH AND (V)PATCH

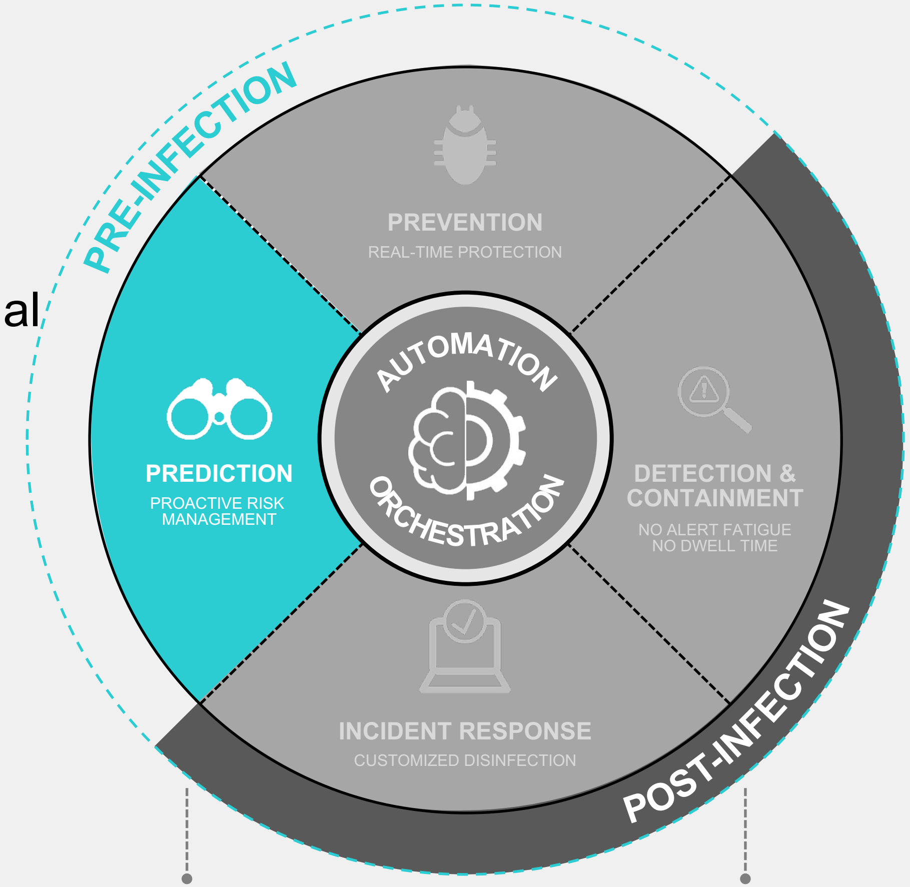
- Rogue and IoT devices
- Applications, vulnerabilities, CVE and application rating data enrichment
- Attack surface reduction with risk-based proactive policies (virtual patching)
- Application Control policies



APPLICATIONS

Showing 1-5/5

☐ APPLICATION		VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
☐ Google Chrome	Signed	Google	3	● Critical	15-Oct-2020	08-Mar-2021
☐ 86.0.4240.75			5	● Critical	15-Oct-2020	16-Oct-2020
☐ 86.0.4240.183			Unknown	● Critical	03-Nov-2020	03-Nov-2020
☐ 87.0.4280.66			5	● Critical	01-Dec-2020	13-Jan-2021
☐ 88.0.4324.104			Unknown	● Critical	01-Feb-2021	03-Feb-2021
☐ 87.0.4280.141			3	● Critical	09-Feb-2021	02-Mar-2021
☐ 88.0.4324.150			Unknown	● Critical	11-Feb-2021	22-Feb-2021
☐ 88.0.4324.146			Unknown	● Critical	12-Feb-2021	19-Feb-2021
☐ Pastebin Desktop	Unsigned	Unknown Vendor	4	Unknown	16-Oct-2020	18-Oct-2020



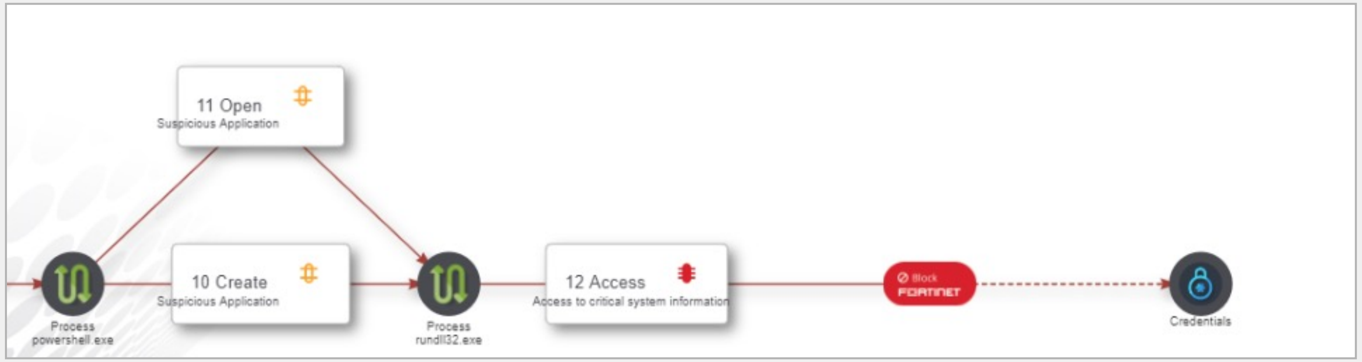
CLOUD, ON-PREMISES OR HYBRID MANAGEMENT

LIGHTWEIGHT AGENT

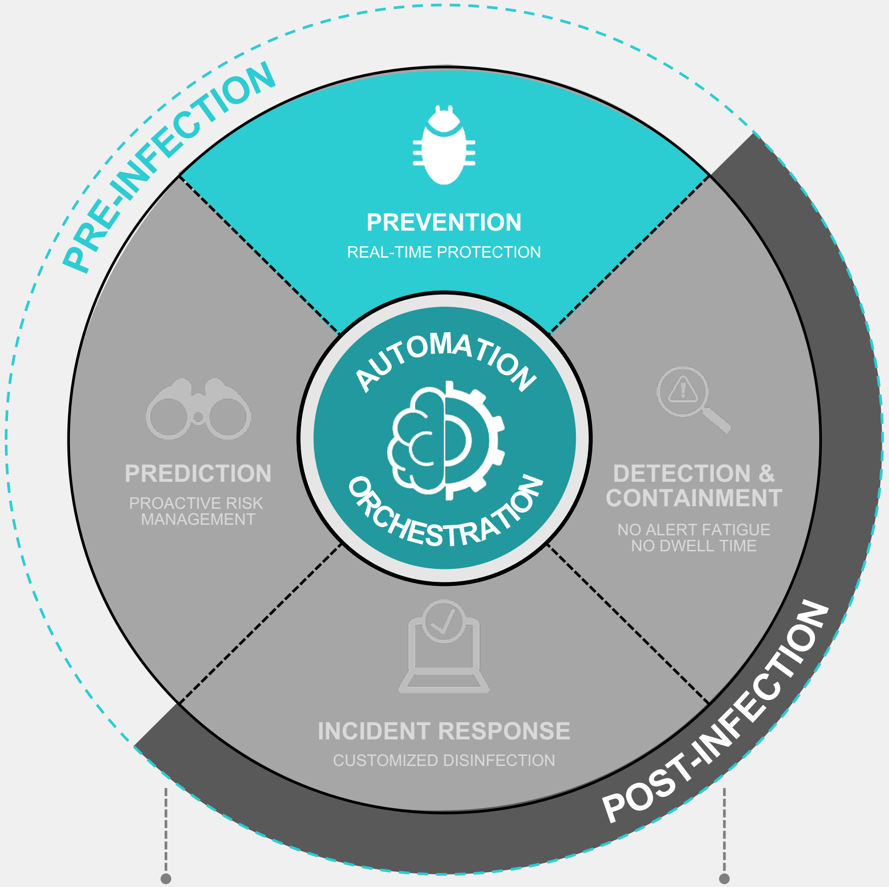
Prevention

✓ **REAL-TIME PREVENTION**

- Machine learning, kernel-based Next Generation AV
- Feeds from a continuously updated FortiGuard cloud database
- Real-time automated protection and rollback of ransomware encryption
- Sandbox Integration



https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard



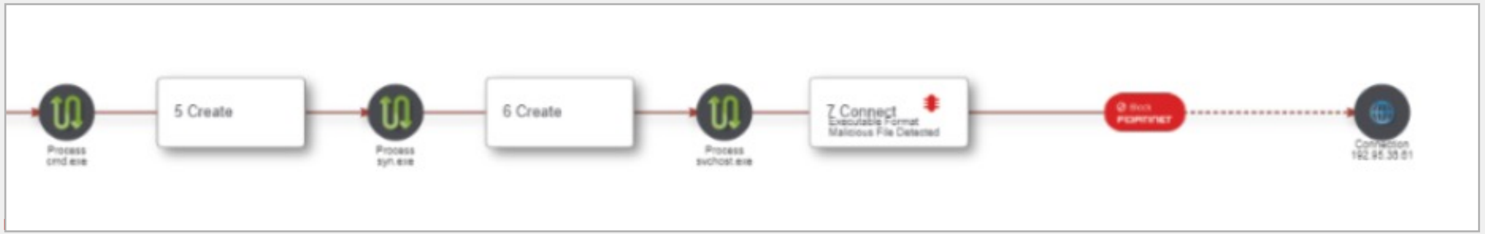
CLOUD, ON-PREMISES OR HYBRID MANAGEMENT

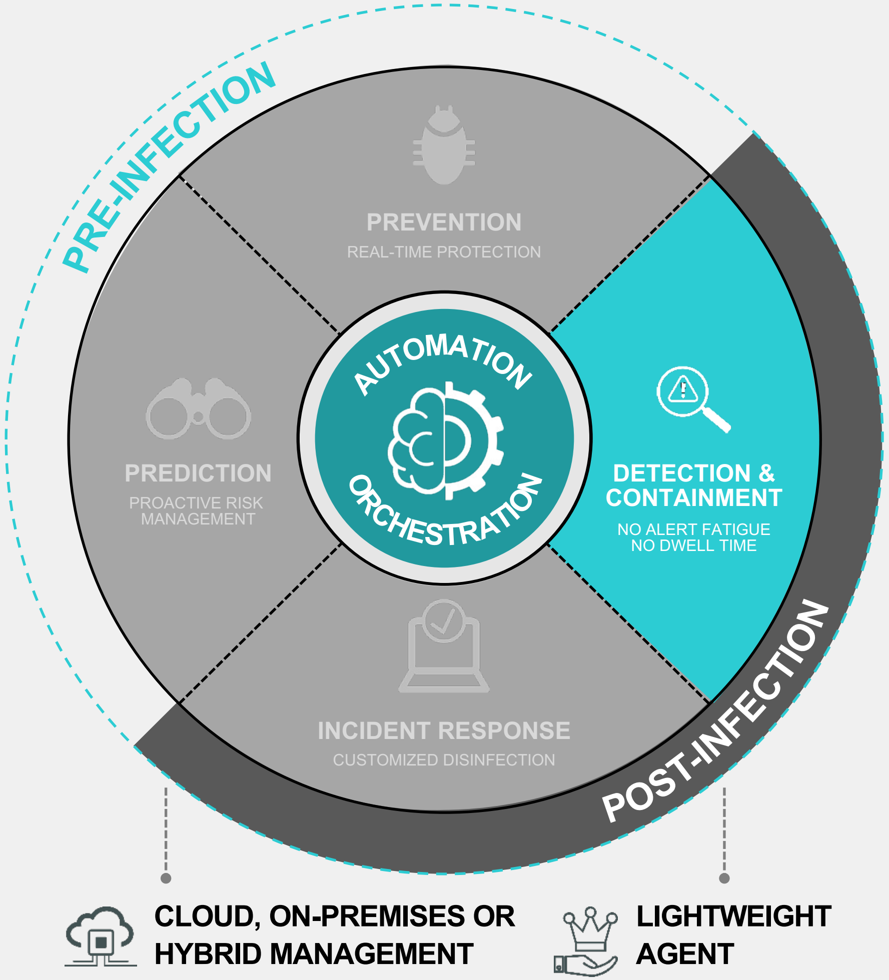
LIGHTWEIGHT AGENT

Detection & Containment

DETECT, DEFUSE AND AUDIT
Patent Number US2016149887A1

- Stop the breach in real-time even upon successful infiltration
- Block communication—data exfiltration, lateral movement, C2
- Deny access to file systems—prevent ransomware encryption, registry tampering
- Behavior-based analysis of entire activity log history
- Cross-Fabric “Search & Destroy”




PRE-INFECTION

PREVENTION
REAL-TIME PROTECTION

PREDICTION
PROACTIVE RISK MANAGEMENT

AUTOMATION
ORCHESTRATION

DETECTION & CONTAINMENT
NO ALERT FATIGUE
NO DWELL TIME

INCIDENT RESPONSE
CUSTOMIZED DISINFECTION

POST-INFECTION

CLOUD, ON-PREMISES OR HYBRID MANAGEMENT

LIGHTWEIGHT AGENT

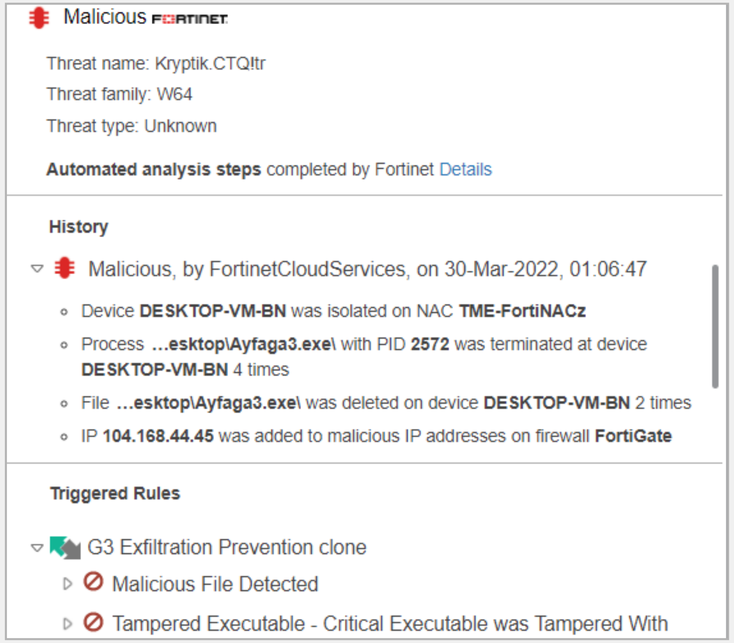
https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits

Automated Response Framework

ORCHESTRATED INCIDENT RESPONSE

Fortinet Ref.: 19154; FORT-035200

- Customizable playbooks based on device group and threat classification
- eXtended Automated response and remediation
- Supports Fabric and 3rd party tools



Malicious FORTINET

Threat name: Kryptik.CTQ!tr

Threat family: W64

Threat type: Unknown

Automated analysis steps completed by Fortinet Details

History

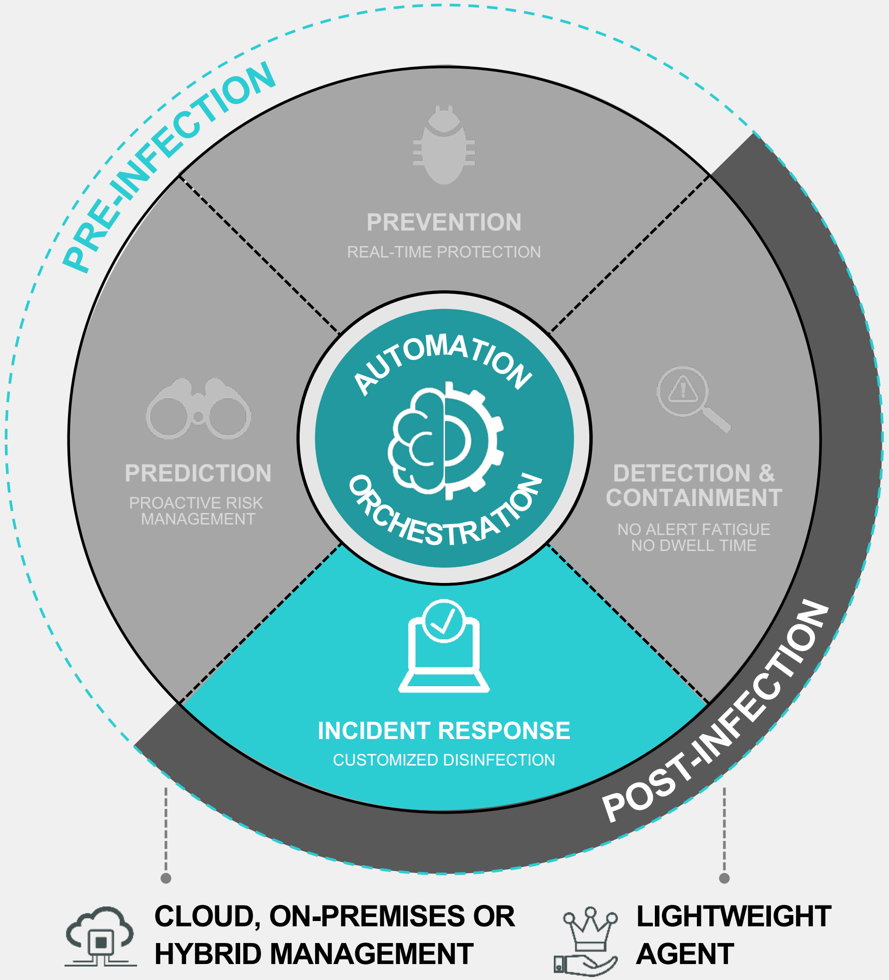
Malicious, by FortinetCloudServices, on 30-Mar-2022, 01:06:47

- Device **DESKTOP-VM-BN** was isolated on NAC **TME-FortiNACz**
- Process **...esktop\Ayfaga3.exe\** with PID **2572** was terminated at device **DESKTOP-VM-BN** 4 times
- File **...esktop\Ayfaga3.exe\** was deleted on device **DESKTOP-VM-BN** 2 times
- IP **104.168.44.45** was added to malicious IP addresses on firewall **FortiGate**

Triggered Rules

G3 Exfiltration Prevention clone

- Malicious File Detected
- Tampered Executable - Critical Executable was Tampered With



CLOUD, ON-PREMISES OR HYBRID MANAGEMENT

LIGHTWEIGHT AGENT

Integrations

FortiEDR Fabric Integration

FortiGate
- Telemetry sharing, automatic blocking of malicious destination IP

FortiNAC

•Extended response - move endpoints to remediation VLAN

FortiSandbox

•Threat intelligence sharing

FortiAnalyzer / FortiSIEM

•Alerts and logs

FortiSOAR

•Extended workflow automation

FortiClient/EMS

Ingesting endpoint status from EDR for ZTNA posture check

3rd Party Firewall
- Palo Alto, Check Point

3rd Party Identity
- Active Directory

3rd Party Mail Security
- ProofPoint

3rd Party SIEM
- Splunk App

3rd Party Event Management
- ServiceNow

3rd Party Access Management
- Microsoft AD, Azure

Third-Party Results

High marks in performance across 3rd party testers

Gartner®

4.6/5.0

Garner Peer Insights

95% Recommend the solution

4.28/5.0

For Type A Organizations

in Critical Capabilities

Visionary

Endpoint Protection

Magic Quadrant

MITRE ENGENUITY™

MITRE ENGENUITY ATT&CK® EVALUATIONS
Enterprise
WIZARD SPIDER & SANDWORM
PARTICIPANT
2022

100%

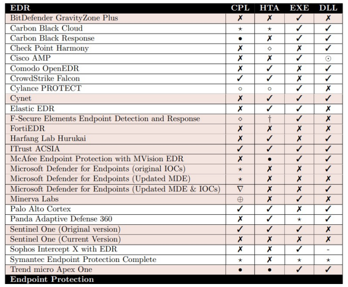
Attacks Blocked
Two Years in a Row

97%

Overall Sub-Technique Detection

94%

Analytic Detection Rate

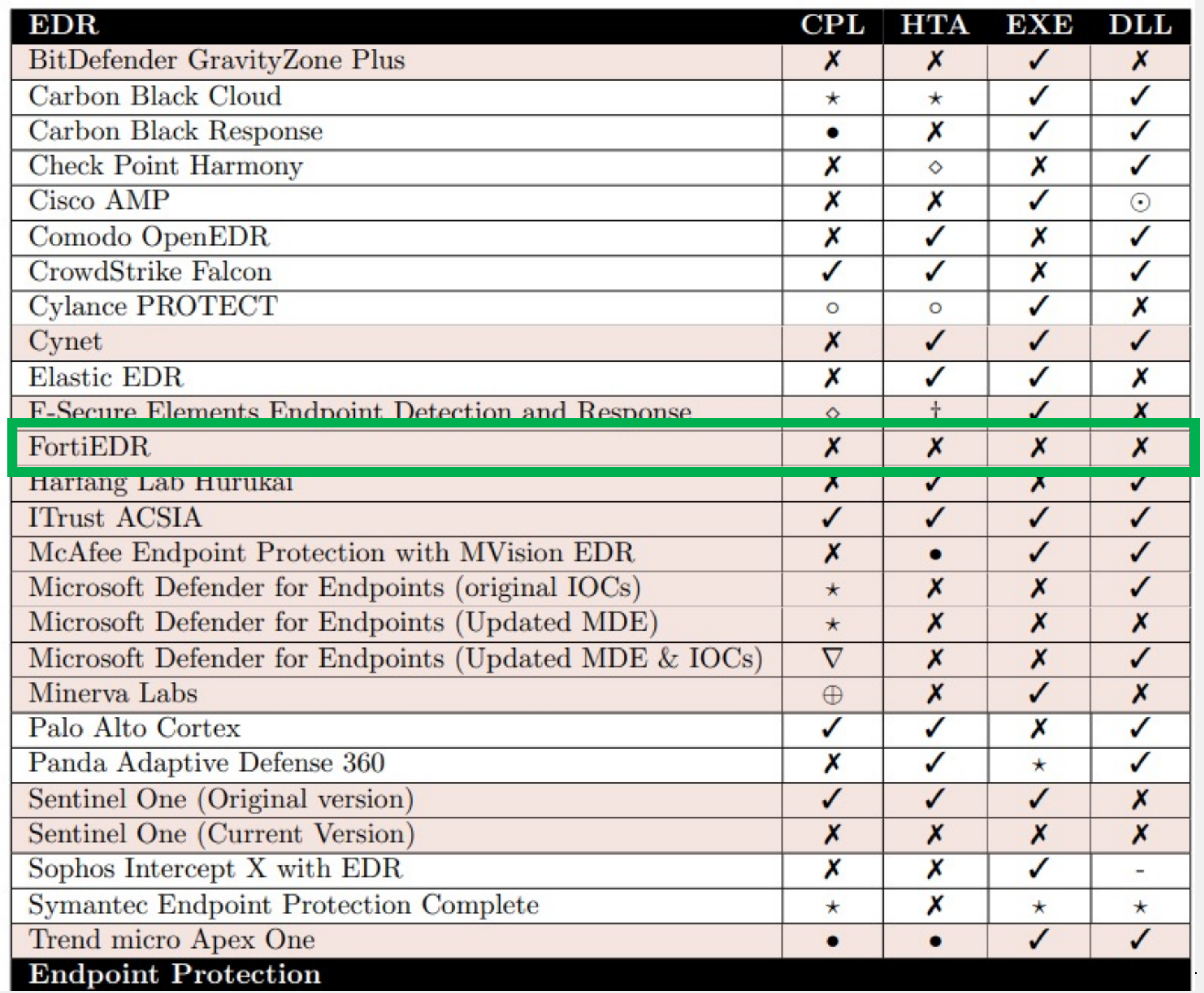


EDR	CPL	HTA	EXE	DLL
BitDefender GravityZone Plus	✗	✗	✓	✗
Carbon Black Cloud	⋆	⋆	✓	✓
Carbon Black Response	●	✗	✓	✓
Check Point Harmony	✗	◇	✗	✓
Cisco AMP	✗	✗	✓	⊙
Comodo OpenEDR	✗	✓	✗	✓
CrowdStrike Falcon	✓	✓	✗	✓
Cylance PROTECT	○	○	✓	✗
Cynet	✗	✓	✓	✓
Elastic EDR	✗	✓	✓	✗
F-Secure Elements Endpoint Detection and Response	◇	†	✓	✗
FortiEDR	✗	✗	✗	✗
Harfang Lab Hurukai	✗	✓	✗	✓
ITrust ACSIA	✓	✓	✓	✓
McAfee Endpoint Protection with MVision EDR	✗	●	✓	✓
Microsoft Defender for Endpoints (original IOCs)	⋆	✗	✗	✓
Microsoft Defender for Endpoints (Updated MDE)	⋆	✗	✗	✗
Microsoft Defender for Endpoints (Updated MDE & IOCs)	∇	✗	✗	✓
Minerva Labs	⊕	✗	✓	✗
Palo Alto Cortex	✓	✓	✗	✓
Panda Adaptive Defense 360	✗	✓	⋆	✓
Sentinel One (Original version)	✓	✓	✓	✗
Sentinel One (Current Version)	✗	✗	✗	✗
Sophos Intercept X with EDR	✗	✗	✓	-
Symantec Endpoint Protection Complete	⋆	✗	⋆	⋆
Trend micro Apex One	●	●	✓	✓
Endpoint Protection				

1st

Out of the Box Solution to
Stop All Attacks

Independent Academic Study (Jan. 2022)



EDR	CPL	HTA	EXE	DLL
BitDefender GravityZone Plus	✗	✗	✓	✗
Carbon Black Cloud	⋆	⋆	✓	✓
Carbon Black Response	•	✗	✓	✓
Check Point Harmony	✗	⋄	✗	✓
Cisco AMP	✗	✗	✓	⊙
Comodo OpenEDR	✗	✓	✗	✓
CrowdStrike Falcon	✓	✓	✗	✓
Cylance PROTECT	○	○	✓	✗
Cynet	✗	✓	✓	✓
Elastic EDR	✗	✓	✓	✗
F-Secure Elements Endpoint Detection and Response	⋄	†	✓	✗
FortiEDR	✗	✗	✗	✗
Harfang Lab Hurukai	✗	✓	✗	✓
ITrust ACSIA	✓	✓	✓	✓
McAfee Endpoint Protection with MVision EDR	✗	•	✓	✓
Microsoft Defender for Endpoints (original IOCs)	⋆	✗	✗	✓
Microsoft Defender for Endpoints (Updated MDE)	⋆	✗	✗	✗
Microsoft Defender for Endpoints (Updated MDE & IOCs)	∇	✗	✗	✓
Minerva Labs	⊕	✗	✓	✗
Palo Alto Cortex	✓	✓	✗	✓
Panda Adaptive Defense 360	✗	✓	⋆	✓
Sentinel One (Original version)	✓	✓	✓	✗
Sentinel One (Current Version)	✗	✗	✗	✗
Sophos Intercept X with EDR	✗	✗	✓	-
Symantec Endpoint Protection Complete	⋆	✗	⋆	⋆
Trend micro Apex One	•	•	✓	✓
Endpoint Protection				

Legend:

√ = Successful Attack

◊ = Successful Attack, Medium Alert

• = Successful Attack, Minor Alert

★ = Successful Attack, Alert raised

Χ = Failed Attack

† & ◉ = Mixed results

2022 ATT&CK Evaluation Overview—FortiEDR

The 2022 test used Wizard Spider and Sandworm ransomware samples

1.a.1 (user execution)	**FortiEDR** detected **87 out of 90** (97%) in scope sub-steps (19 Linux excluded)
Technique	**Technique**—84/90 (94%)
Tactic	**Tactic**—1/90 (1%)
General	**General**—0/90
Telemetry	**Telemetry**—2/90 (2%)
None	**None**—3/90 (3%)
Block (Suspicious Macro)	**FortiEDR** blocked **100%** of attacks

2022 ATT&CK Evaluation Overview—FortiEDR

The 2022 test used Wizard Spider and Sandworm ransomware samples

100% Protection

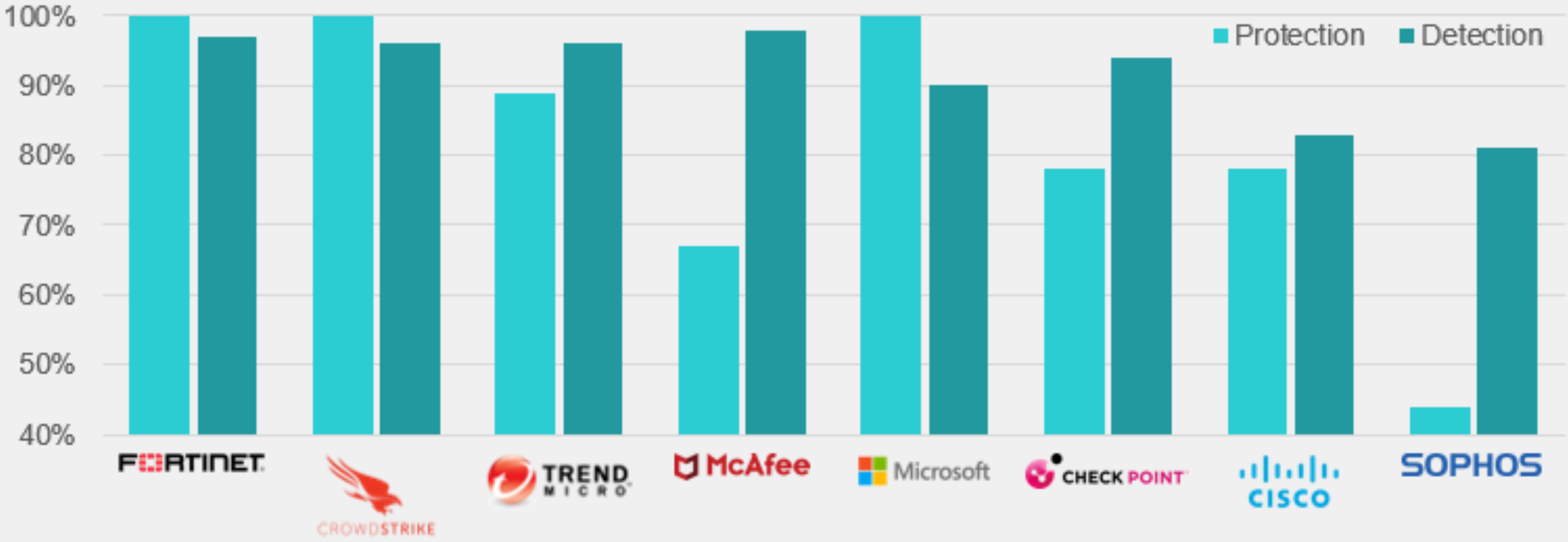
2 Years Running

97% Visibility

One of the Best at Detection

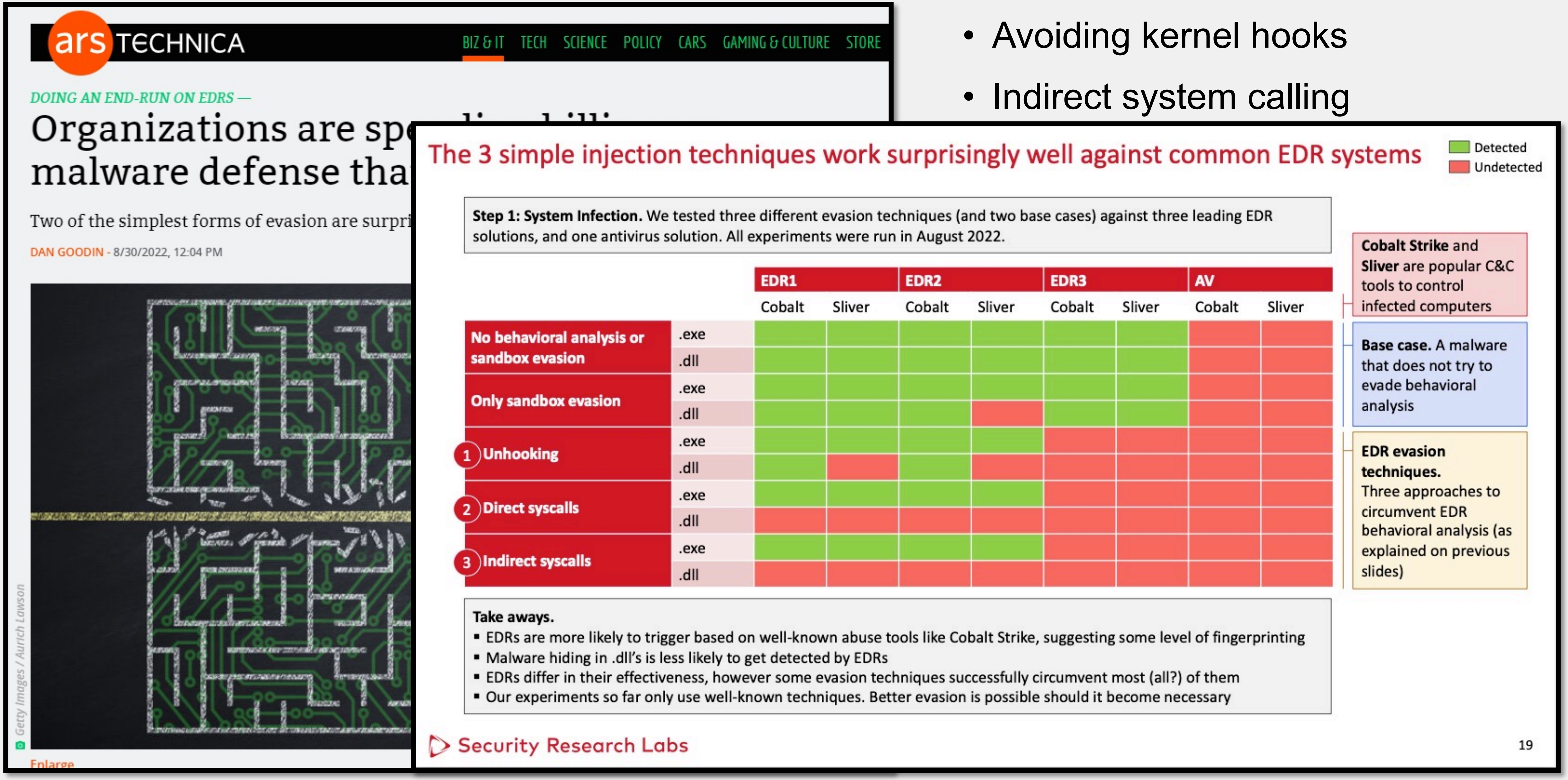
94% Technique Coverage

Best Possible Outcome



How resistant is your EDR?

- Streamlining EDR evasion
- Avoiding kernel hooks
- Indirect system calling



ars TECHNICA

DOING AN END-RUN ON EDRS —

Organizations are spe
malware defense tha

Two of the simplest forms of evasion are surpri

DAN GOODIN - 8/30/2022, 12:04 PM

Getty Images / Aurich Lawson

Enlarge

The 3 simple injection techniques work surprisingly well against common EDR systems

🟩 Detected
🟥 Undetected

Step 1: System Infection. We tested three different evasion techniques (and two base cases) against three leading EDR solutions, and one antivirus solution. All experiments were run in August 2022.

		EDR1		EDR2		EDR3		AV	
		Cobalt	Sliver	Cobalt	Sliver	Cobalt	Sliver	Cobalt	Sliver
No behavioral analysis or sandbox evasion	.exe	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥
	.dll	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥
Only sandbox evasion	.exe	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥
	.dll	🟩	🟩	🟩	🟥	🟩	🟩	🟥	🟥
1 Unhooking	.exe	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥
	.dll	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟥
2 Direct syscalls	.exe	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥
	.dll	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
3 Indirect syscalls	.exe	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥
	.dll	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

Cobalt Strike and **Sliver** are popular C&C tools to control infected computers

Base case. A malware that does not try to evade behavioral analysis

EDR evasion techniques. Three approaches to circumvent EDR behavioral analysis (as explained on previous slides)

Take aways.
- EDRs are more likely to trigger based on well-known abuse tools like Cobalt Strike, suggesting some level of fingerprinting
- Malware hiding in .dll's is less likely to get detected by EDRs
- EDRs differ in their effectiveness, however some evasion techniques successfully circumvent most (all?) of them
- Our experiments so far only use well-known techniques. Better evasion is possible should it become necessary

Security Research Labs

19

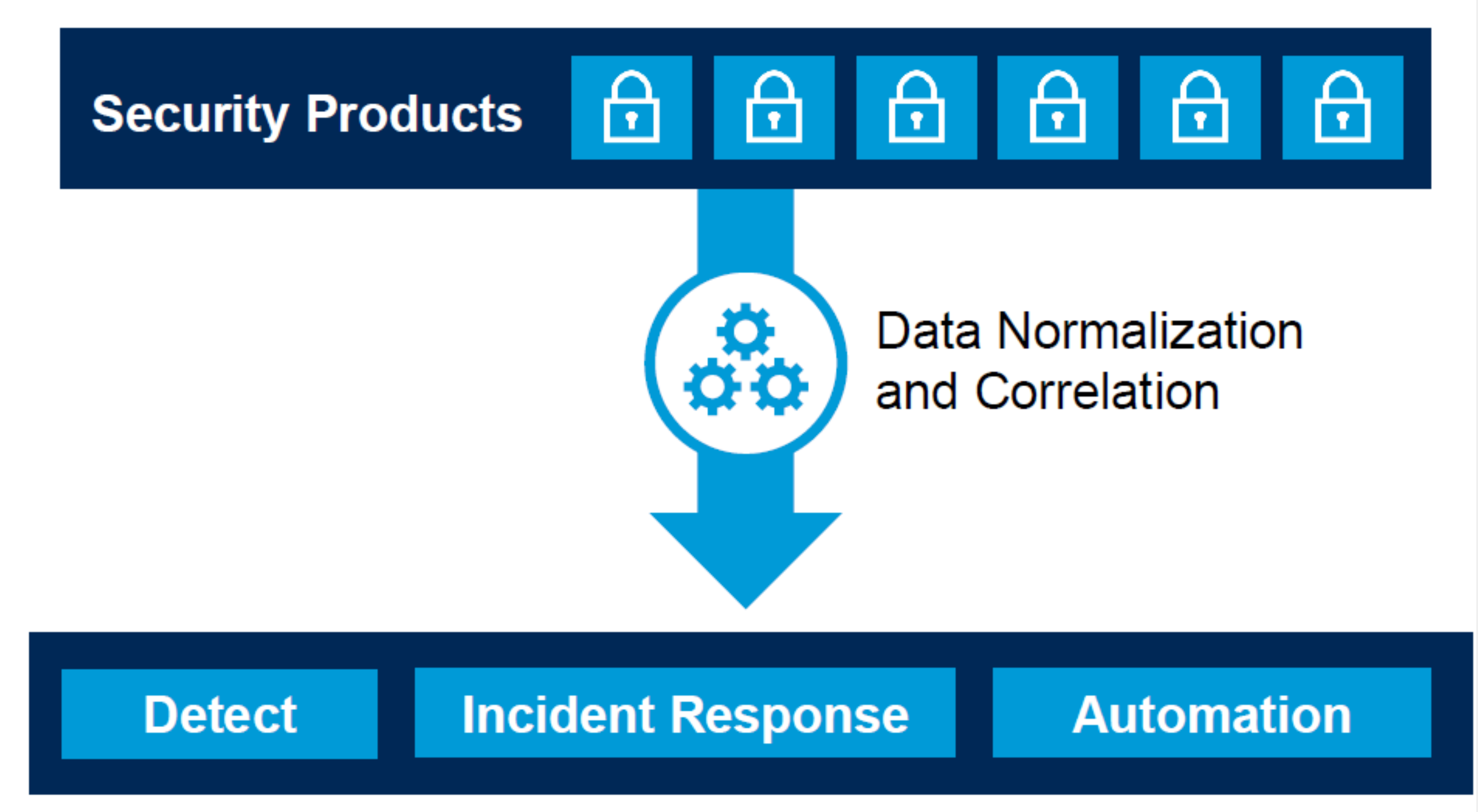
FortiXDR

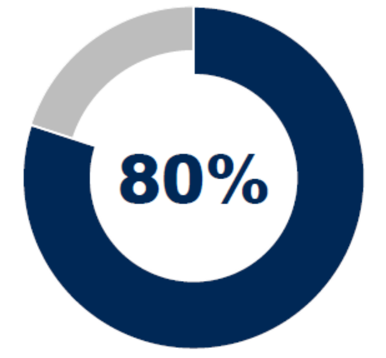
Automated Detection, Investigation and Response across the Security Fabric

Consolidation of tools and data that provides extended visibility, analysis, and response across endpoint, workloads, users, networks

Extended Detection and Response

A Perfect Principle for Vendor Consolidation





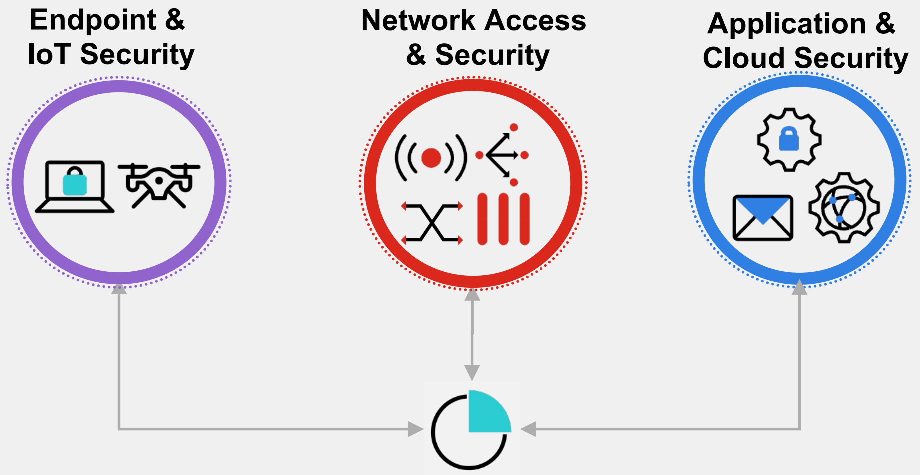
of IT organizations plan to pursue a vendor consolidation strategy in the next three years.

Sources:
Gartner. Innovation Insight for Extended Detection and Response. March 19, 2020. Firstbrook and Lawson.
Gartner. Gartner Security Summit Presentation- Top Trends in Security and Risk Management. September 17, 2020. Peter Firstbrook.

FortiXDR

Fully-automatable extended detection and response

- Leverages the Security Fabric
  - Reduces the complexity of too many vendors

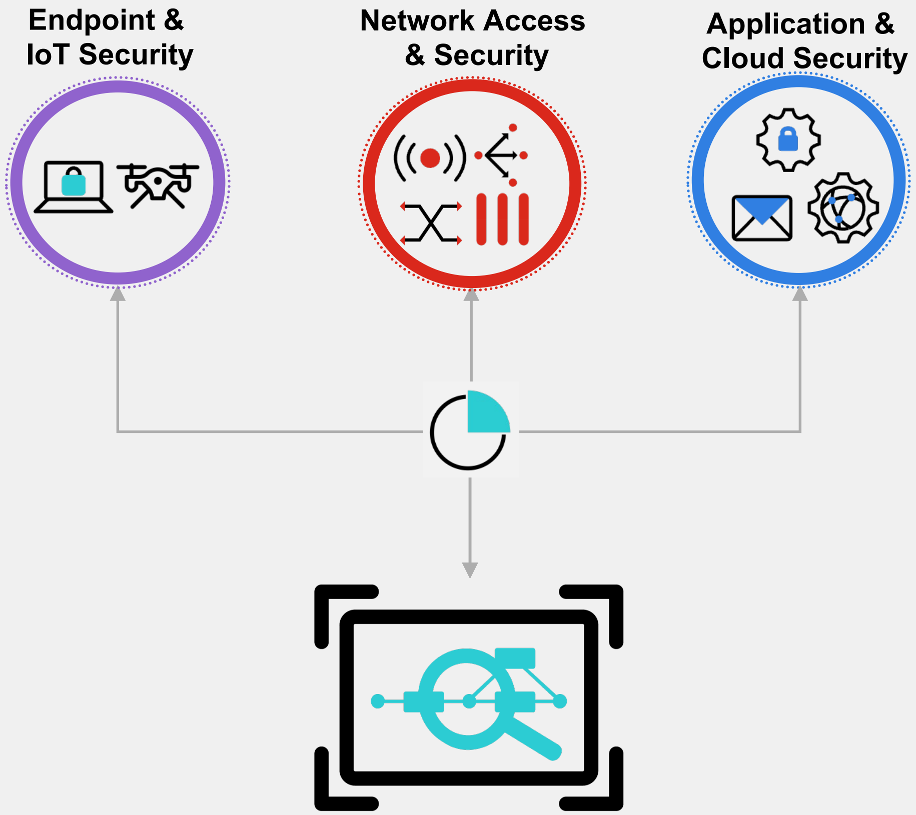


FortiXDR

Fully-automatable extended detection and response

- Leverages the Security Fabric
  - Reduces the complexity of too many vendors

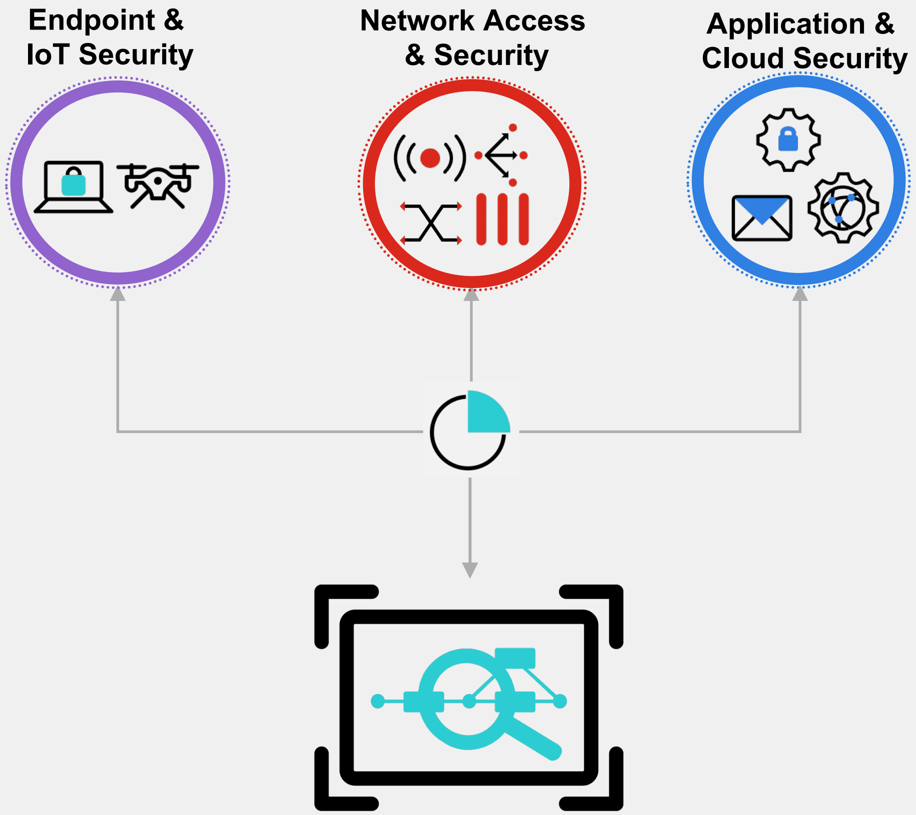
- Adds automated detection, investigation and response
  - Fortinet curated analytics convert alerts to incidents
  - Uses AI to investigate incidents just like a security pro, but faster
  - Can pre-define response to block attacks faster



FortiXDR

Fully-automatable extended detection and response

- Leverages the Security Fabric
  - Reduces the complexity of too many vendors
- Adds automated detection, investigation and response
  - Fortinet curated analytics convert alerts to incidents
  - Uses AI to investigate incidents just like a security pro, but faster
  - Can pre-define response to block attacks faster
- Improved operational efficiency
  - ¾ reduction in alerts
  - Incident investigation in seconds
  - Automatable response



FORTINET®