



F**ORTINET**

COLOMBIA
& ECUADOR

XPERTS26

FORTINET | COLOMBIA
& ECUADOR
XPERTS26

Anti-Ransomware Protection

Giovanny Iza Gallegos
Systems Engineer - Ecuador

Giovanny Iza Gallegos

Systems Engineer – Ecuador

Enterprise





Disclaimer

Fortinet Confidential

This document contains confidential material proprietary to Fortinet, Inc.

This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside Fortinet, Inc. without prior written consent of Fortinet, Inc.

This information is pre-release and forward looking and therefore is subject to change without notice.

The purpose of this document is to provide a statement of the current direction of Fortinet's product strategy and product marketing efforts.

Please note that this Product Roadmap is neither intended to bind Fortinet to any particular course of product marketing and development nor to constitute a part of the license agreement or any contractual agreement with Fortinet or its subsidiaries or affiliates.



XPERTS26

This content is shared exclusively with the CTO Office and Product Management teams and is considered void if transferred to (or presented by) anyone outside of this group. The contents are for individual use and should not be copied, transferred, uploaded or shared to anyone without written consent. © Fortinet Inc. All Rights Reserved.

CONFIDENTIAL

Access Limited to Authorized Personnel

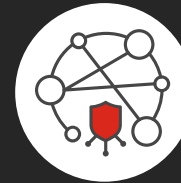
Agenda



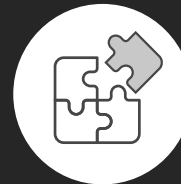
Anti-Ransomware Evolution



Dynamic Containment Architectures



Endpoint & Data Defense



Advanced Mechanics



Hands on Lab

Your Computer Has been Locked

- To unlock the computer , Please pay a fine of \$200

6 : 07 : 02 : 25

DAYS

HOURS

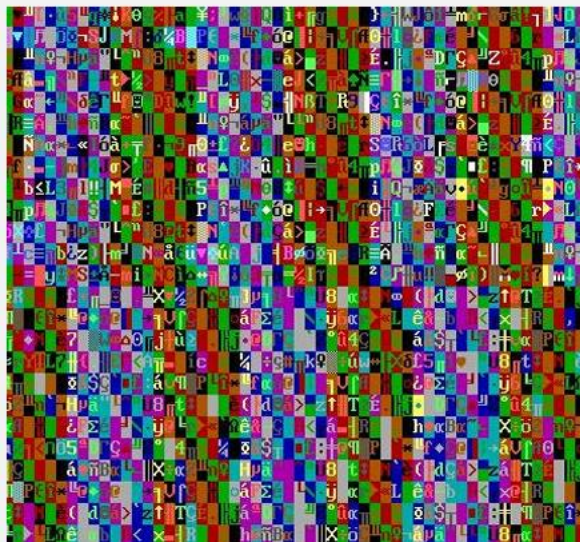
MINUTES

SECONDS

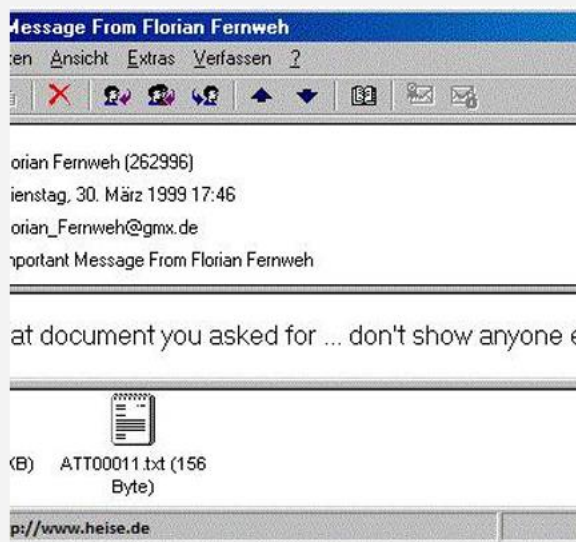




Evolution of Malware across the years



1980s: Nag Screens – Simple pop-ups urging users to register software.
1990s: Macro & Boot Sector Viruses – Spread via floppy disks and documents.



2000s: Worms & Trojans – Internet-enabled self-replicating threats.



2010s: Ransomware Emerges – Encrypts files, demands payment.



2020s+: AI-Driven & Targeted Ransomware – Highly sophisticated, often targeting businesses and infrastructure.

**According to Garner, by 2025
ransomware attacks are
expected to increase by 700%.**





Ransomware continues to be a problem

JLR

Jaguar Land Rover - Global automaker
(United Kingdom)

- ✓ Massive cyberattack in August/September 2025
- ✓ Production paralyzed for over 6 weeks
- Vishing (voice phishing) to the IT help desk was the initial access vector
- ✓ Lack of robust identity verification allowed attackers to obtain valid credentials
- Cost the company £196M (~\$258M) and a total UK economic impact of up to £1.9 billion (~\$2.5 billion)



Industry Knocked down by Cybercrime



Latinoamérica » México | Colombia | Argentina | Venezuela | Perú | Chile | Ecuador | Brasil

Colombia

Sigue la cobertura

COLOMBIA

Activan protocolo de emergencia en Colombia por ciberataque a proveedor de telecomunicaciones

Por José Manuel Álvarez
15:18 ET(19:18 GMT) 14 Septiembre, 2023



Semana Suscribirse Crear cuenta

Ciberataque

Ciberataque: este fue el mensaje de los 'hackers' a IFX tras intervenir páginas del Gobierno colombiano

Fiscalía investiga ataques cibernéticos a páginas web de la SIC, Supersalud y otras entidades del Gobierno.

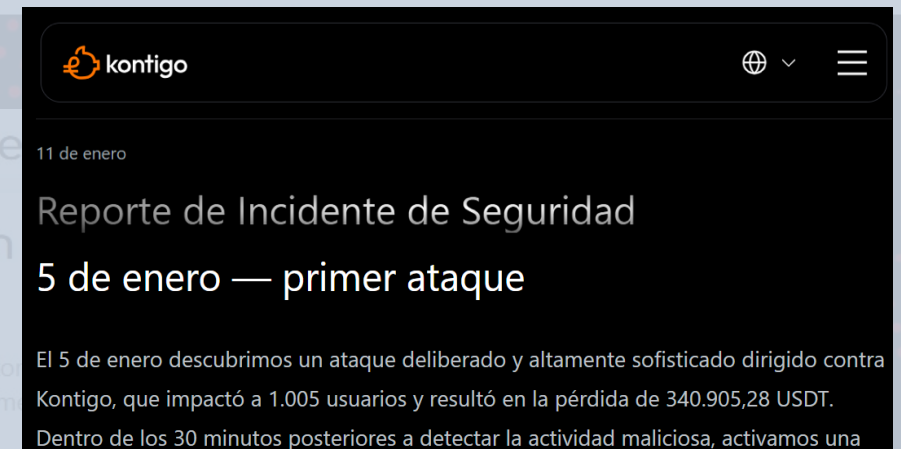
Redacción Semana
14 de septiembre de 2023

Los misterios del ataque que dejó a CNT sumida en la "emergencia"

Expertos entrevistados por PRIMICIAS coinciden que lo ocurrido el 14 de julio fue el último punto de un ataque que, presumiblemente, inició hace meses. CNT pide esperar los resultados de las investigaciones con la Fiscalía

Venezuela sufre una grave ola de hackeos: ¿Qué está pasando?

Venezuela lleva tres años acumulando filtraciones masivas de datos: organizaciones, empresas e instituciones del Estado las han sufrido por igual. En medio de incertidumbre, silencio e inexistente regulación, esto es lo que sabemos.



kontigo

11 de enero

Reporte de Incidente de Seguridad

5 de enero — primer ataque

El 5 de enero descubrimos un ataque deliberado y altamente sofisticado dirigido contra Kontigo, que impactó a 1.005 usuarios y resultó en la pérdida de 340.905,28 USDT. Dentro de los 30 minutos posteriores a detectar la actividad maliciosa, activamos una

Allanan oficinas de la ANT en Quito luego de ataque cibernético

Agentes de la Fiscalía y de la Unidad Nacional de Ciberdelitos de la Policía Nacional allanaron la mañana de este viernes las oficinas del departamento de Tecnologías de la Información y Comunicación de la Agencia Nacional de Tránsito, en Quito.

TOP RANSOMWARE ATTACK VECTORS

Attacks on organizations are primarily linked to the compromise of:

- Phishing and Malicious Emails
- Vulnerabilities and Exploitation of Unpatched Software
- Infected USB Devices and Physical Media

- Exploiting Vulnerabilities in Web Applications and Their Code
- Brute Force Attacks and Stolen Credentials
- Supply Chain Engagement

- Social Engineering and Identity Theft
- Untrustworthy Software Downloads
- Attacks via Compromised Websites (Drive-by Downloads)

87%

53%

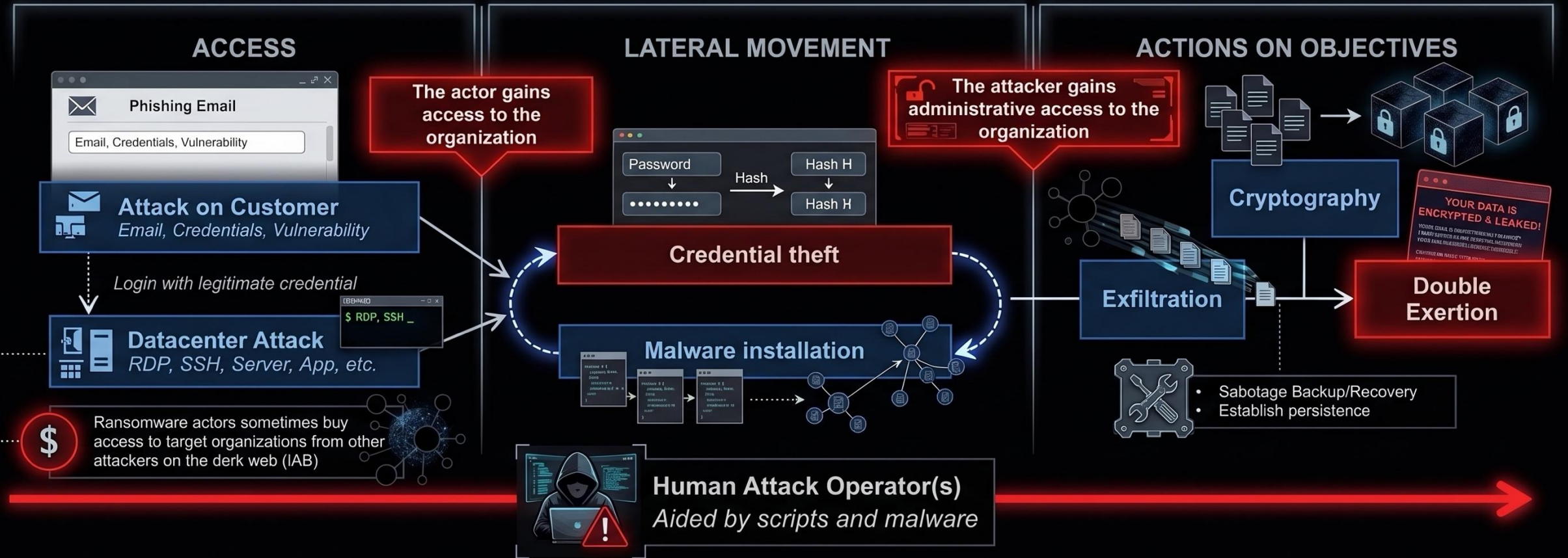
15%

Computers, servers, and
networking equipment

Web Resources

People

Ransomware Workflow





Ransomware as-a-Service (RaaS)

- RaaS is a business model in which cybercriminals purchase ransomware software on the dark web and carry out attacks without any coding.

RaaS Operator
Purchase access
from Initial Access
Broker (IAB)

INITIAL ACCESS BROKER
(IAB) MARKET



Германия / 23 billion / Доступ
By blackdkjackkkk, February 23 in Russia

blackdkjackkkk
byte
Paid registration
4 posts
Joined
02/13/22 (ID: 125595)
Activity
hacking / hacking
Deposit
0.000033

Posted February 23

CEO: Германия
Revenue: \$23 billion
Employees: 62,285
Start: 9000\$
Step: 500\$
BLITZ: 15000\$
Окончание торгиз: 24 часа пиз

Avos
byte
Paid registration
9 posts
Joined
06/27/21 (ID: 117720)
Activity
hacking / hacking
Deposit
0.125014

Posted February 23

https://www.zoominfo.com/j/ades-wj491927

Citrix usa 678\$ Million admin
By BOP, Yesterday at 07:57 AM in Auctions

BOP
byte
Paid registration
4 posts
Joined
05/06/22 (ID: 130039)
Activity
безопасность / security

Posted Yesterday at 07:57 AM

usa
Citrix
Admin
Revenue 678\$ Million
Industry: Business Services
Security Products & Services
3,000 employees
Start: 2k
Step: 500\$
bLITZ: 3k
12H

Avos
byte
Paid registration
12 posts
Joined
06/27/21 (ID: 117720)
Activity
hacking / hacking
Deposit
0.125014

Posted Wednesday at 02:58 PM

start

+ Quote

FORTINET | COLOMBIA
XPERTS26 & ECUADOR

Dynamic Containment Architectures

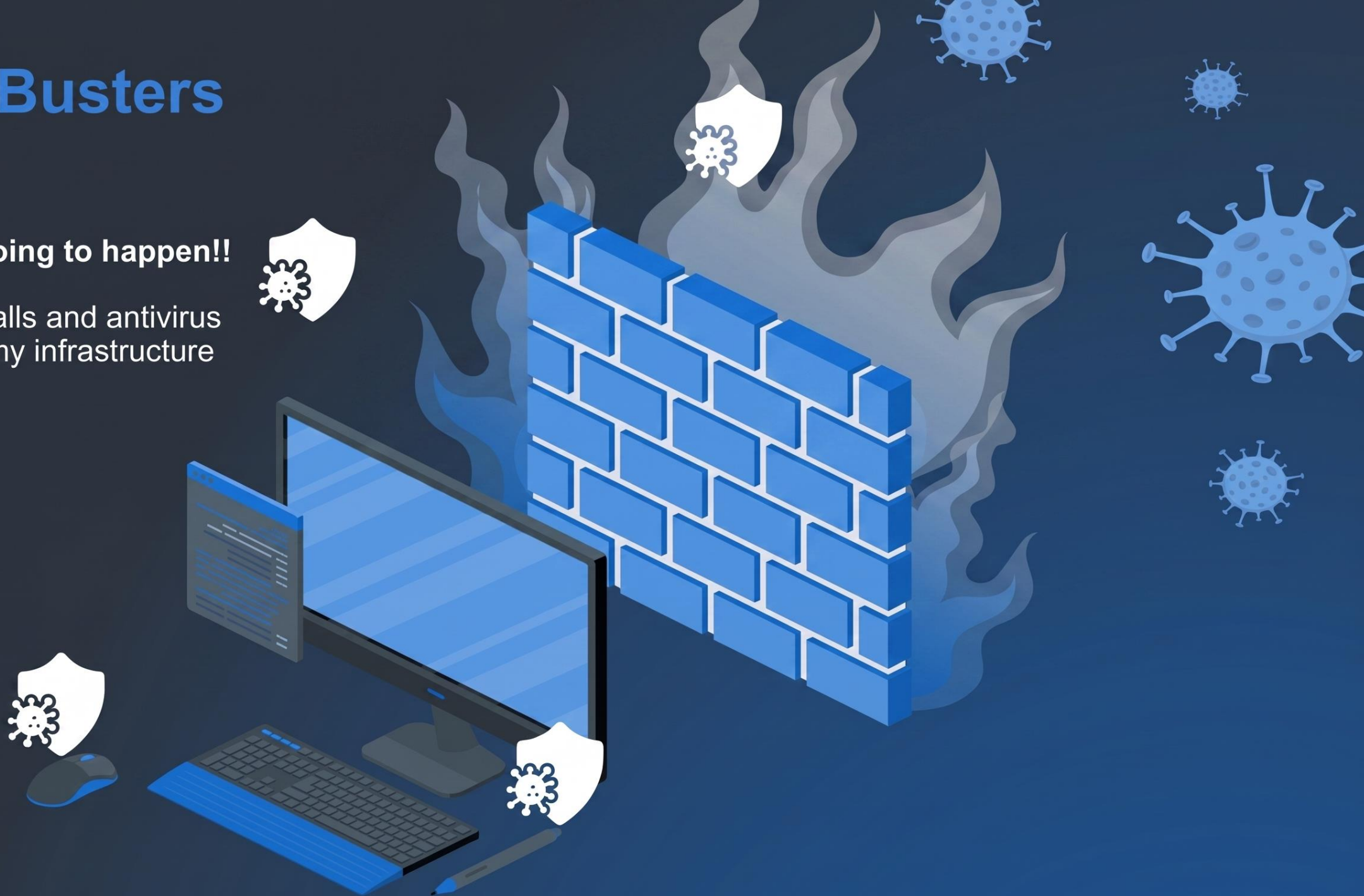
Isolate the Threat. Protect the Business.

Cartagena

MythBusters

Nothing is going to happen!!

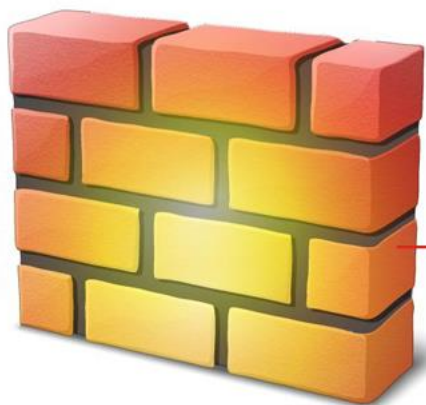
I have firewalls and antivirus
protecting my infrastructure





But.....

Firewall



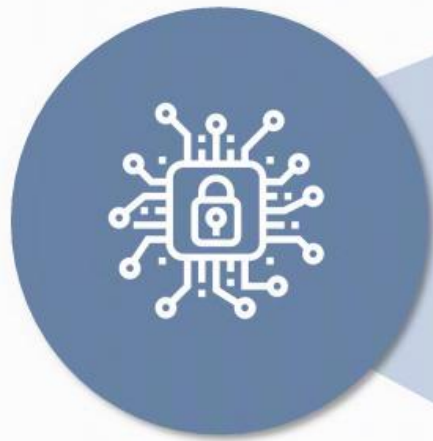
- Increasing Threat Complexity
- Expanding the Attack Surface
- Lack of Full Visibility
- Threat detection is only part of the challenge
- Effective protection requires a layered approach

Antivirus

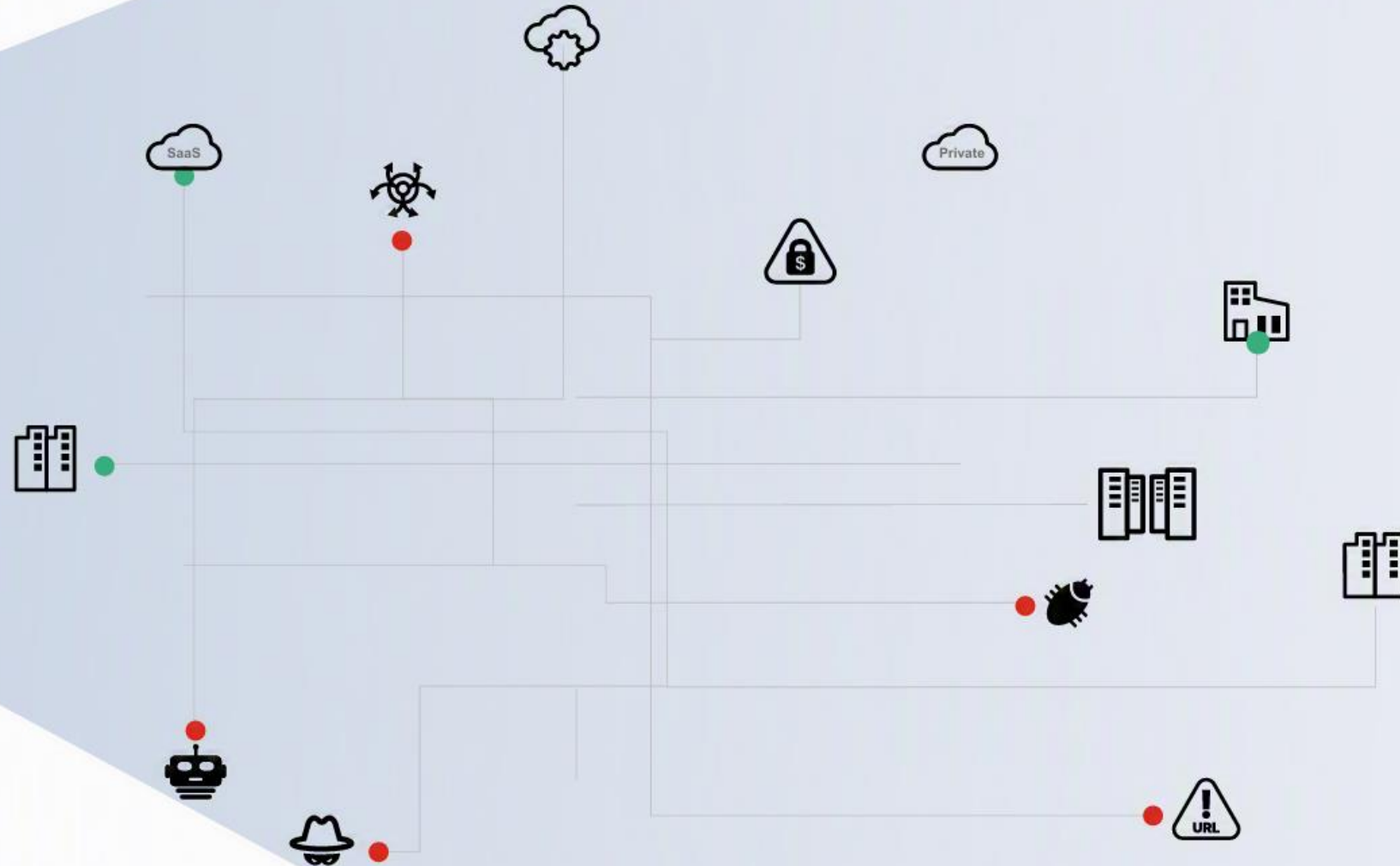


- Focus on detection of known threats.
- Extended Response Inability
- Lack the ability to provide deep visibility
- Lack of integration with the security ecosystem
- Reactive approach

For that reason, we need to build an Anti-Ransomware Architecture



Protection of the
main attack
vectors beyond
frontline protection



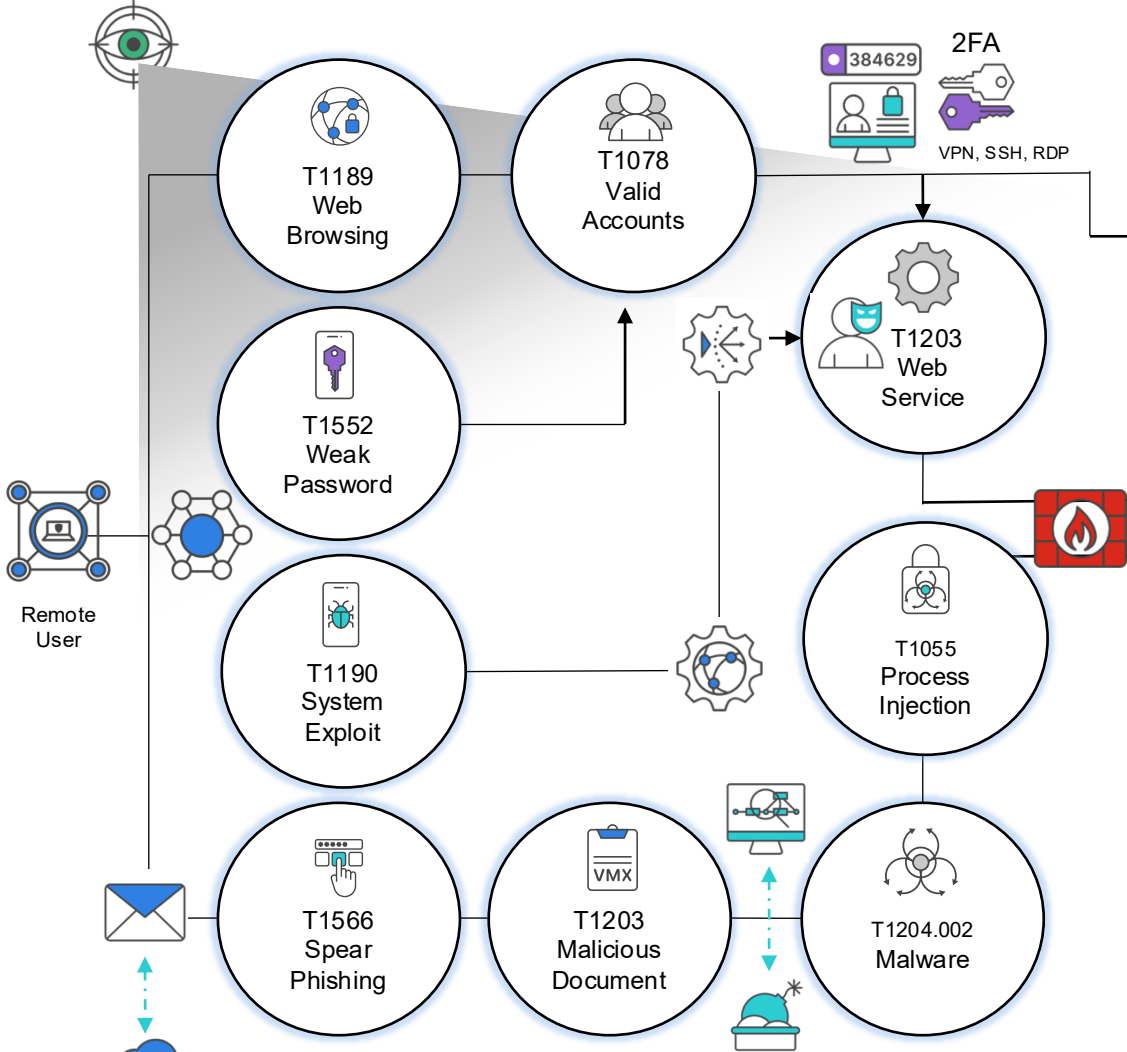
Why do we need a Ransomware Architecture

- No single product can protect against every attack vectors leaves gaps in security
- Multiple consoles independent of each others add complexity
- Lack of visibility across the full network and endpoints
- Little or no integration between solutions
- Time loss due to slow manual incident response



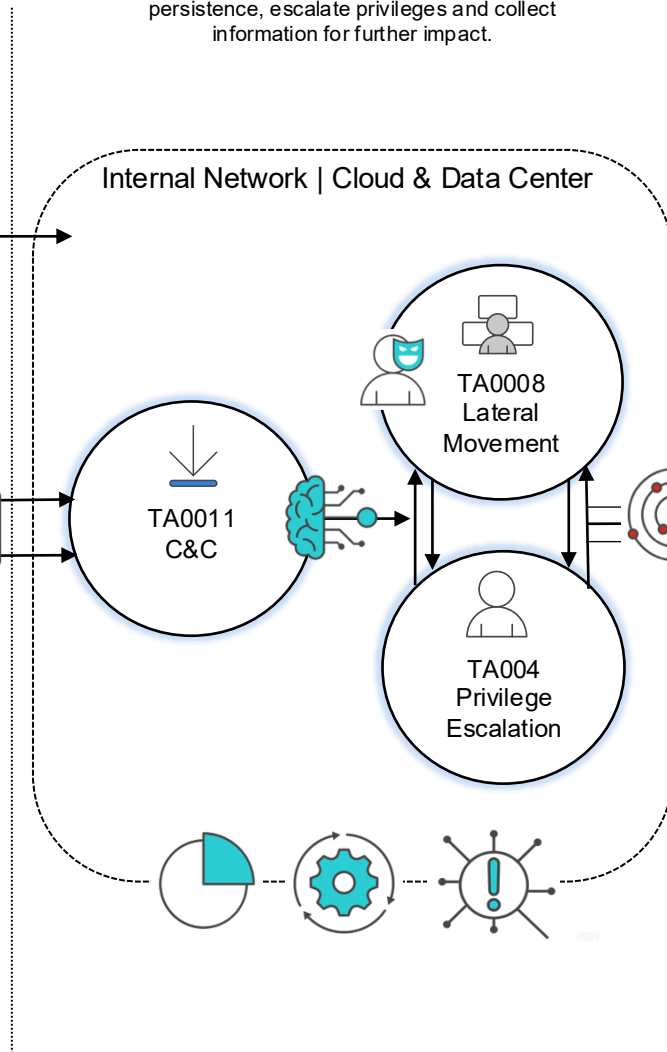
TA0001 - INITIAL ACCESS

Consists of techniques that use various entry vectors to gain their initial foothold within a network



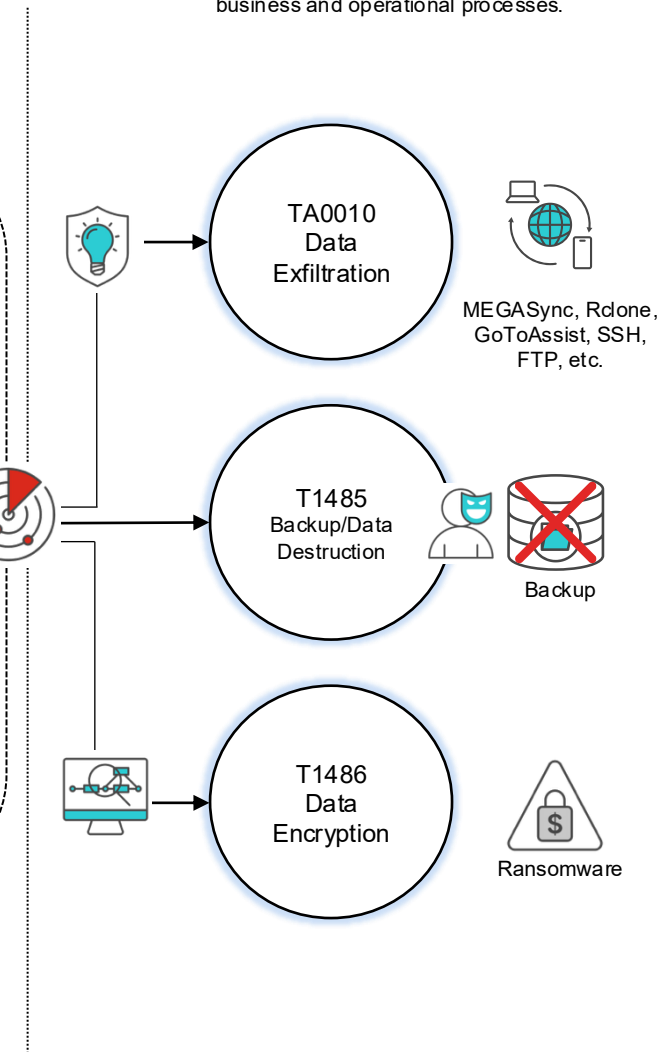
CONSOLIDATION AND PREPARATION

Consists of multiple tactics in order to stablish persistence, escalate privileges and collect information for further impact.



TA0040 - IMPACT ON TARGET

consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.



FortiSandbox

FortiRecon

FortiClient

FortiSASE

FortiToken

FortiADC WAF

FortiSOAR

FortiNDR

FortiAnalyzer

FortiDeceptor

FortiMail

FortiPhish

FortiEDR

FortiPAM

FortiGate

FortiSIEM

FortiNAC

FortiDLP

Fortinet Maturity Reports



		Methods					
		Detect	Deny	Disrupt	Degrade	Deceive	Contain
Phases	Reconnaissance & Discovery	- Web analytics - Threat analytics - NIDS - EASM	- Edge FW - WAAP	- Info Sharing Policy	- Traffic Encryption	- Honeypot	- Secure Recurte Access
	Weaponization	- NIDS - Threat intelligence	- NIPS				
	Delivery	- EPP / ATP	- Web filtering - App whitelisting - Mail Security - EDR / XDR	- NGAV - NAC	- Queuing - Change mgmnt - Web filtering		- FW - App aware FW - Trust Zones - NIPS
	Social Engineering	- Phishing detection - Brand protection	- Anti phishing - Mail Security	- Training			- Anti phishing - Mail Security
	Exploitation & Execution	- EPP / ATP - NDR - Threat analytics	- Secure Password - Patch management	- Execution prevention	- Domain Controller - Incident Readiness	- Honeypot	- App aware FW - Trust Zones - NIPS - ISFW
	Persistence & Defense Evasion	- SIEM - NDR - Threat analytics	- PAM - Secure Password - MFK - WAAP	- Password Policy - Network Segmentation			- App aware FW - Trust Zones - EDR / SDR - ISFW
	Command and Control	- NDR	- FW - Network Segmentation	- EDR / XDR	- Sandbox	- DNS Redirect	- Trust Zones - DNS Shikholes
	Pivoting & Lateral Movement	- NDR	- ISFW - Network Segmentation		- Sandbox		- Trust Zones - NAC - EDR / XDR
	Privilege Escalation & Credential access	- Threat analytics - NDR	- PAM - MFA	- IAM	- Password Policy		- ISFW - Secure Remote Access
	Collection & Exfiltration	- NDR	- EDR / XDR	- Traffic Encryption	- Backup and Recovery		- DLP
	Impact	- NDR	- EDR / XDR		- EPP / ATP		- EDR / XDR
Objectives		- Anti phishing - Mail Security		- Training - Incident Readiness			
		Security Controls					



The logo for Fortinet Xperts 26. It features the word "FORTINET" in white with a red square icon containing a white grid pattern. To its right is a vertical line, followed by "COLOMBIA & ECUADOR" in white. Below "FORTINET" is the word "XPERTS26" in a large, bold font, with "XPERTS" in white and "26" in red.

FORTINET | COLOMBIA
& ECUADOR
XPERTS26

Endpoint & Data Defense

Securing access, stopping execution, and
preventing data exfiltration.

The background of the slide is a blue-tinted aerial photograph of the city of Cartagena, Colombia. A large, glowing white 'X' is superimposed over the image. The word "Cartagena" is written in a large, light blue, sans-serif font across the middle of the image, partially obscured by the 'X' and the city's architecture.

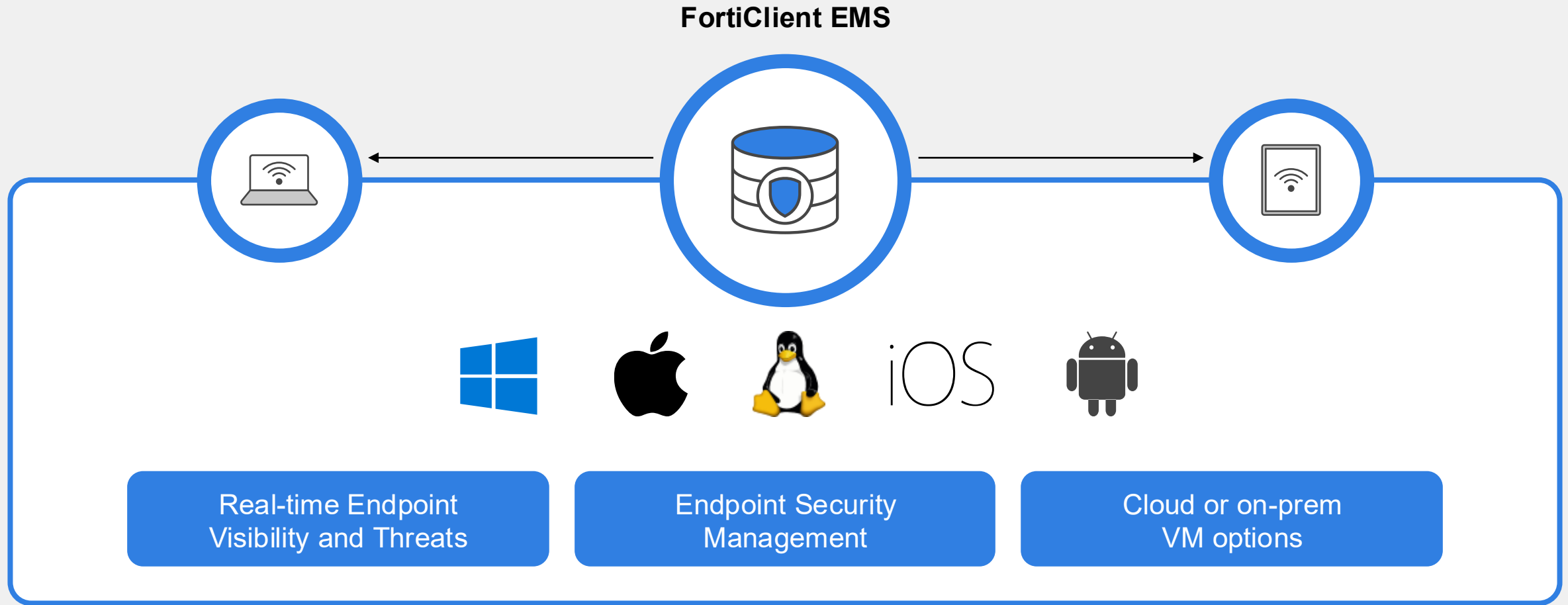
Cartagena

FortiClient: Endpoint Agent



Centralized Endpoint Management

FortiClient Endpoint Management Server (EMS)



FortiClient Use Cases



**Endpoint Visibility
and Control**



Secure Access



**Endpoint Protection
(EPP)**

Endpoint Protection (EPP)

AI-powered Anti-Virus, Malware and Ransomware Protection



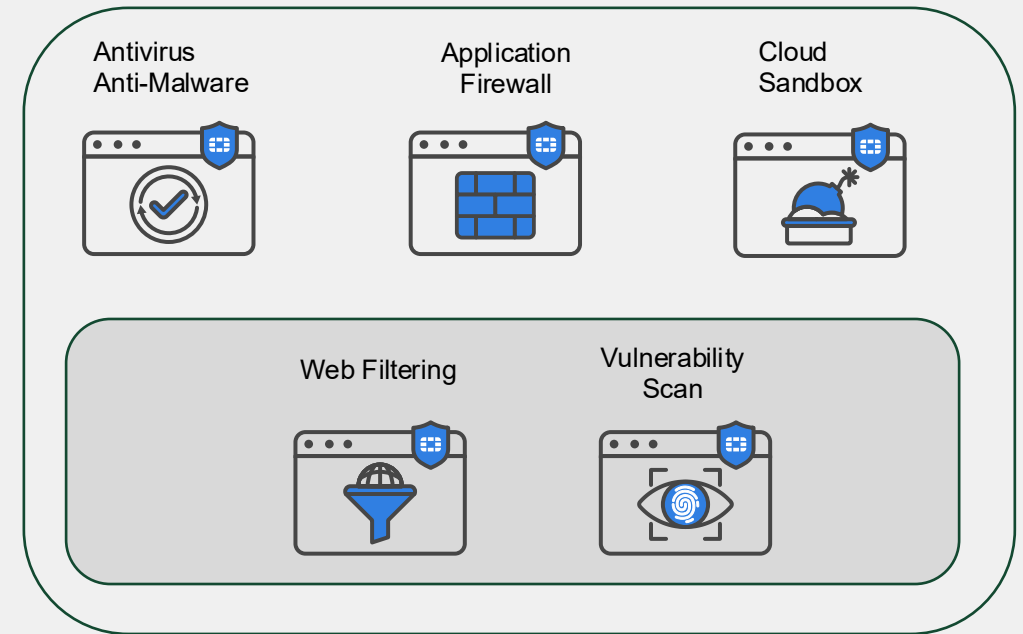
FortiClient Endpoint Protection (EPP)

- **Key Benefits**

- Malware and Exploit Prevention
- Ransomware Protection

- **Key Features**

- AI-powered Anti-Virus
- Anti-Malware
- Application Firewall
- Anti-exploit and Anti-ransomware
- Cloud Sandbox
- Removable media control



Endpoint Protection and Reducing Attack Surface



Vulnerability Scan

Manage application vulnerabilities



Device Control

Removable media access control and device authorization



Application Firewall

Block unauthorized application communications



Anti-Malware

Real-time malware protection, Next-Gen AV



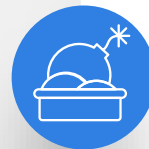
Anti-Ransomware

Protects files and folders from unauthorized changes and protect from exploits



Web Filter

Block malicious, phishing websites



Cloud Sandbox

Behaviour based file analysis and threat detection

FortiClient Services

Best Practices (BPS), Managed Services, Forensics Services



FortiClient Managed Service

Offloading the Monitoring and Analysis of Endpoint

- Fortinet professionals actively assisting with deployment, configuration, management, and analysis of FortiClient deployments
- Cloud-provisioning of:
 - ZTNA and/or VPN
 - Endpoint Security
 - Vulnerability management
 - Posture Check tools
- Endpoint onboarding (putting FortiClient onto customer devices)
- Vulnerability monitoring & reporting (with recommendations)
- Requires FortiClient Cloud



FortiClient Forensic Service

Post-event review, analysis and reporting

- Helps customers respond and recover from incidents
- Fortinet professionals will collect info, analyze, and report
 - Accelerates response time to an event
 - Offloads customer teams
- For FortiClient Cloud & on-prem
- Annual subscription (not per-incident)
 - No restriction on number of incidents

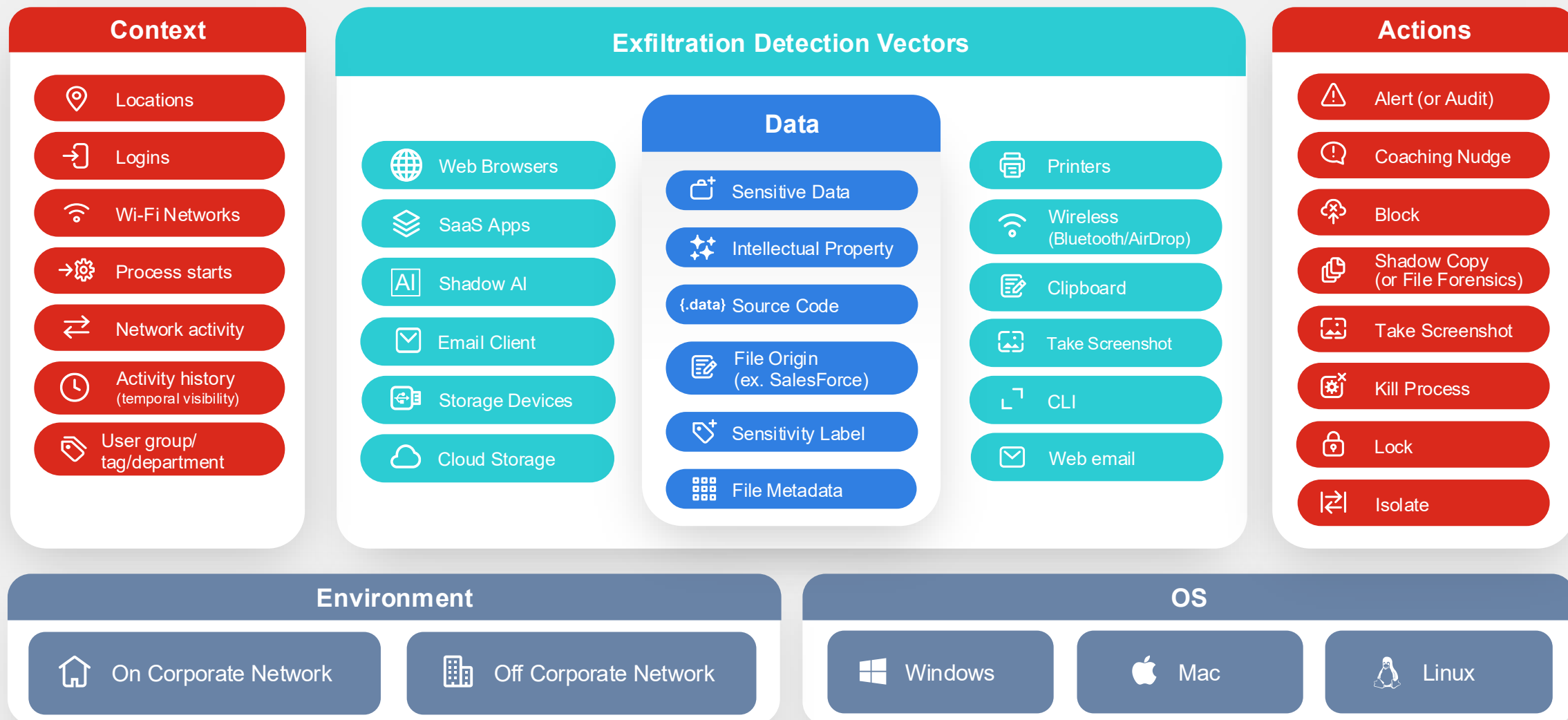


Anticipate and Prevent Data Theft

FortiDLP



Deep and Broad Contextual Visibility is Required to Protect Data



How FortiDLP Works: Overview

SIEM



splunk>
a CISCO company



panther

IAM



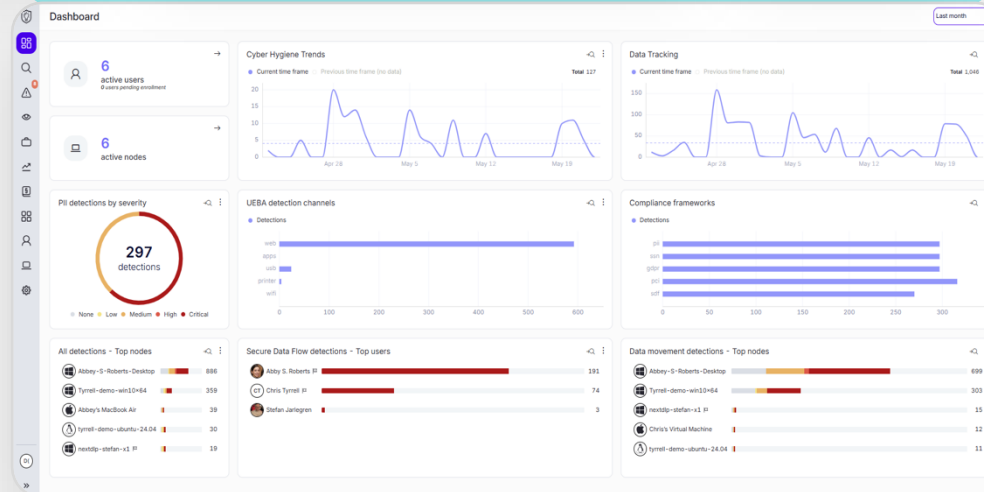
okta

XDR



Evidence Store

aws



OS Integrations



Connectors



XPERTS26

FortiDLP Insider Risk Management

Detecting High-Risk Behavior Before Data Loss Occurs

1 Normal User Behavior

- Normal Logins
- Standard File Access
- Approved Applications
- Trusted Network Activity
- Regular SaaS Usage

Behavior Baseline

2 Anomalous Activity Detected



3 Attack Sequence Detection

Behavior Analytics & Risk Scoring



4 Risk Analysis



5 Data Protection Targets

- | | | |
|-------------------|-----------------------|-----------------------|
| Web Browsers | Sensitive Data | Clipboard |
| SaaS Applications | Intellectual Property | Screen Capture |
| Cloud Storage | Source Code | SSH Sessions |
| Email | Financial Records | Downloads |
| GenAI Tools | Customer Information | File Transfers |
| Removable Media | Security Credentials | Command Line Activity |

6 Automated Response

Action

- Alert
- User Coaching
- Block
- Screenshot Capture
- Shadow Copy
- Kill Process
- Lock Endpoint
- Isolate Device

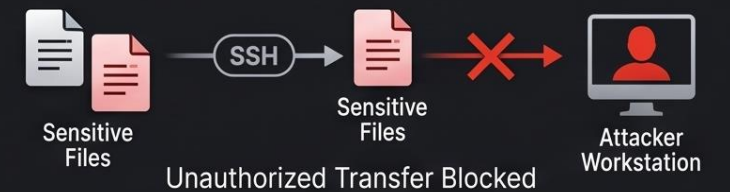
7 Ransomware Prevention Visual

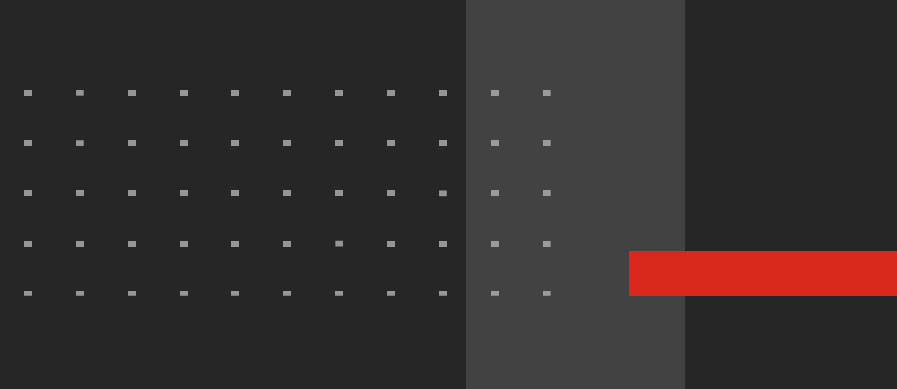


Complete Protection

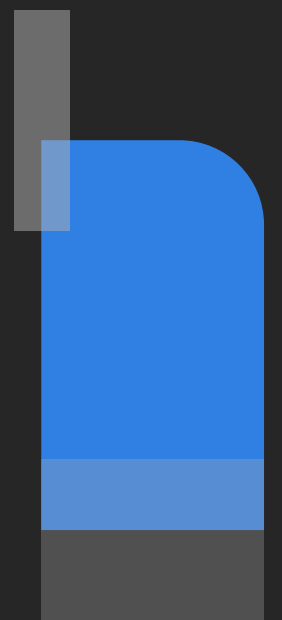
FortiDLP combines Data Loss Prevention and Insider Risk Management to identify abnormal behavior, correlate attack sequences, stop ransomware-related activity, detect credential theft, prevent privilege abuse, and block data exfiltration before critical information leaves the organization.

8 Data Exfiltration Prevention Visual



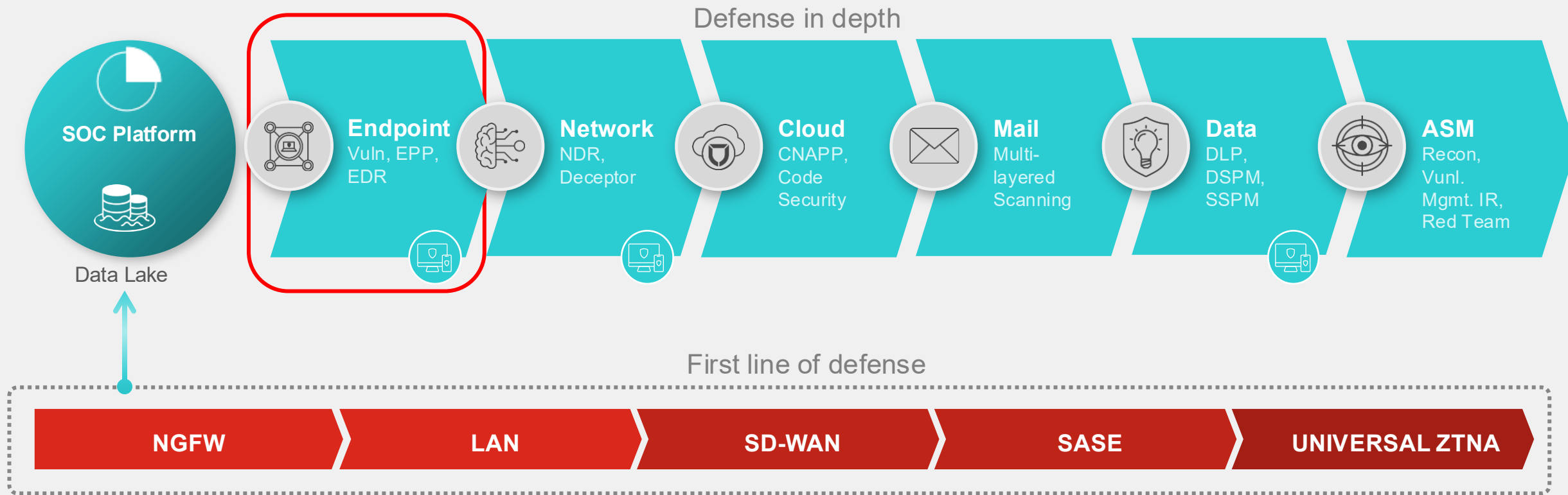


Fortinet Endpoint Detection and Response (FortiEDR)



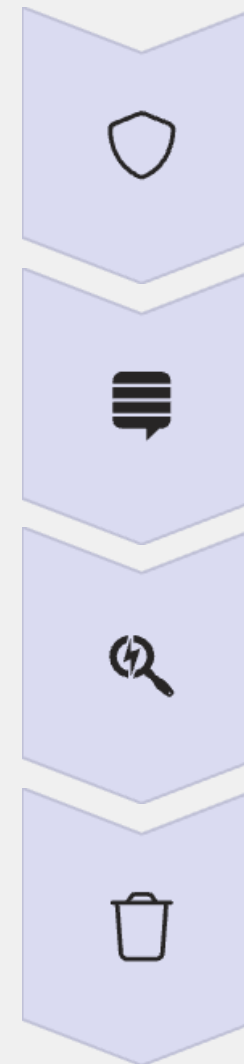
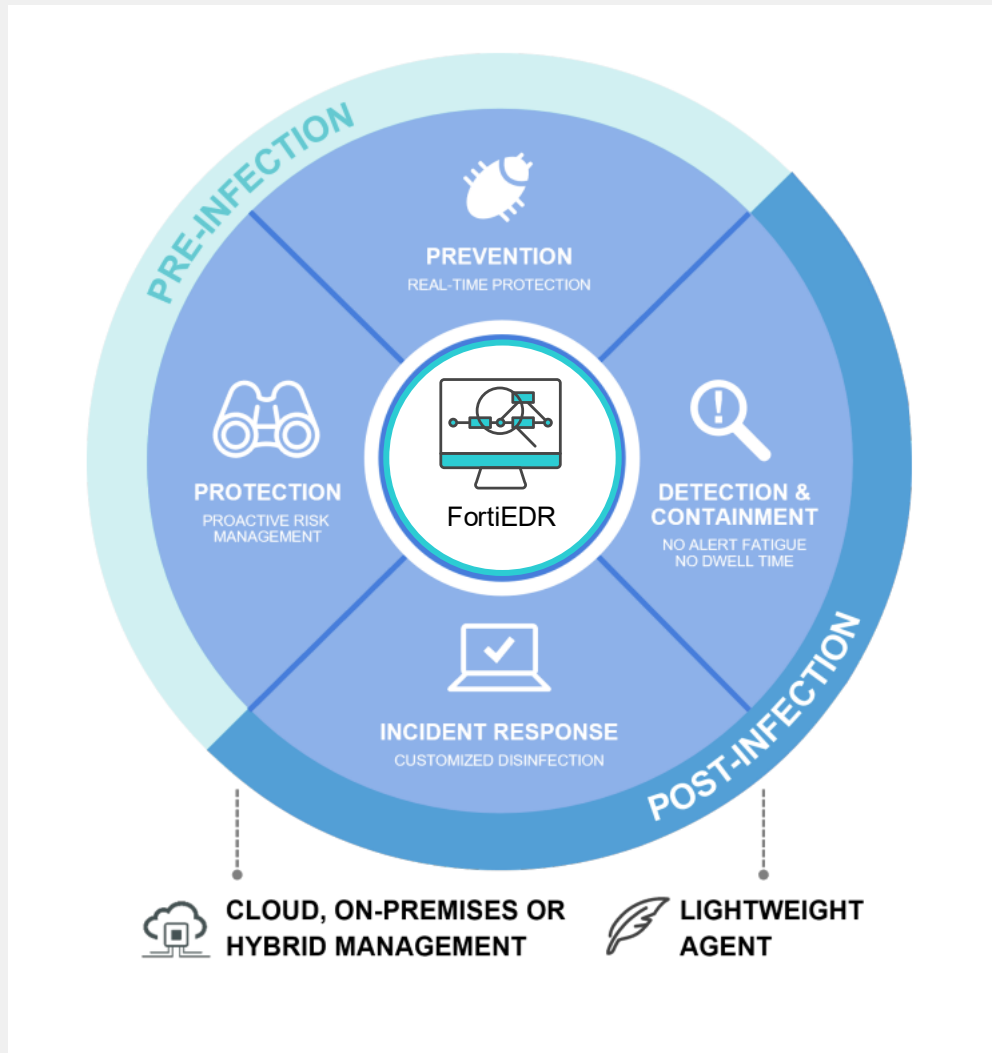
Fortinet AI-Driven SecOps

Integrated end-to-end security for the modern enterprise



The Fortinet AI-driven SecOps platform delivers the visibility, control, and orchestration to break the kill chain at every stage

Stop Breaches with FortiEDR!



Discover, Enrich and Patch

Find unmanaged, IoT devices, enrich vulnerabilities w/ threat intel, enforce virtual patching.

Real-time Prevention

Stop threats with AI-powered NGAV, sandboxing, and ransomware rollback.

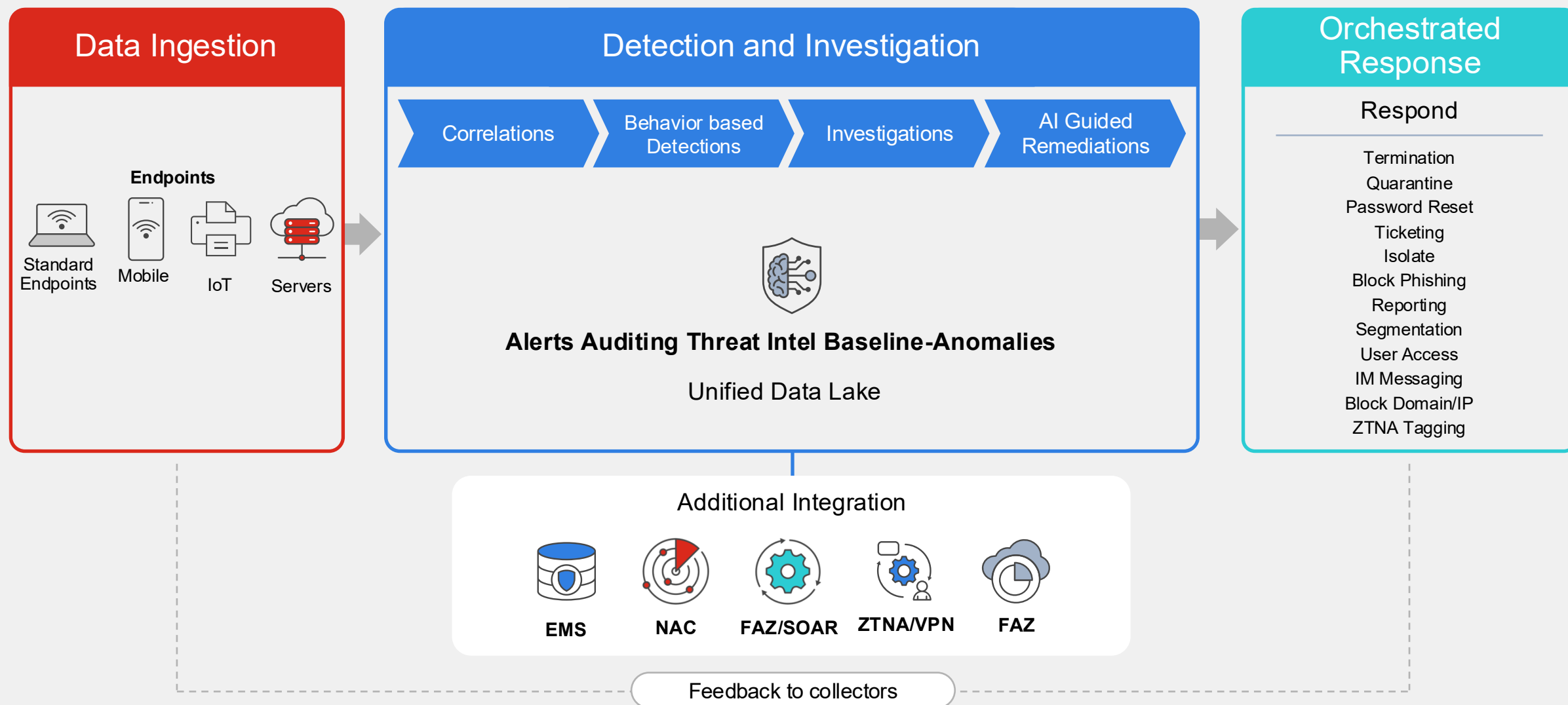
Detect, Defuse and Audit

Block exfiltration and encryption post-breach with behavioral containment.

Orchestrated Incident Response

Automate response with playbooks across Fabric and third-party tools.

Delivering Endpoint Security with FortiEDR



FORTINET | COLOMBIA
& ECUADOR
XPERTS26

Advanced Mechanics

Kernel-level defense capabilities

Cartagena

Kernel-Level Integration

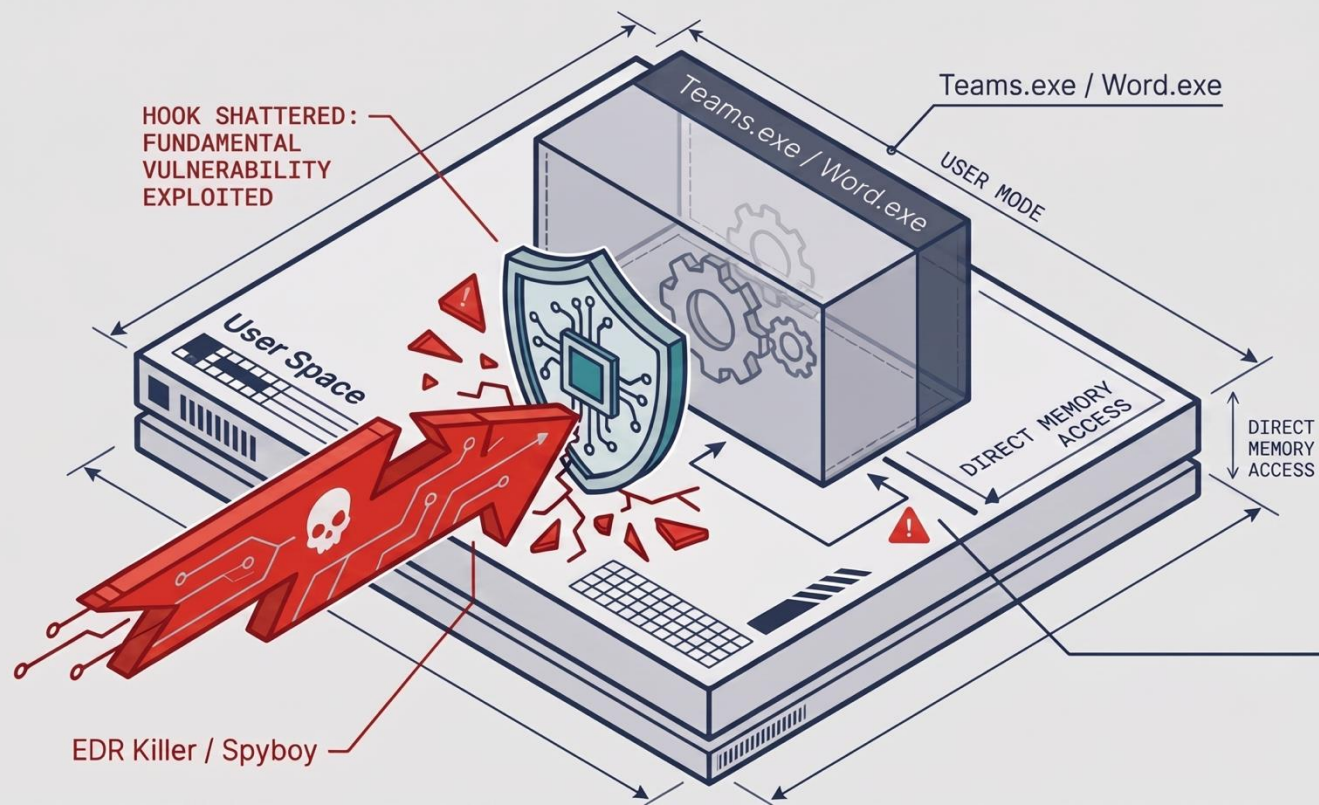
Patent US20160149887A1





Legacy EDRs/AVs behavior

Legacy EDRs rely on 'Application Hooking' in the User Space. Because they operate in the exact same ring as the malware, they are fundamentally vulnerable.



A TA going by the handle Spyboy is selling an AV/EDR killer that is allegedly capable of killing almost every AV/EDR on the market.

I'm selling a private program to terminate all AVs/EDRs/XDRs in a legitimate way and it has been tested on most of AVs/EDRs/XDRs that exist in the market on most of AVs/EDRs/XDRs that exist in the market such as WD, Sophos, Carbon black, Sentinelone, ESET, Kaspersky, etc.

I want to mention that this method is a private one "NOT like the one being sold on xss.is and other forums which does not work on windows 7 and windows server 2008"

FIRA CODE

VULNERABLE INTERFACE

Threat actors routinely use admin-level EDR Killers to unhook, blind, or permanently terminate EDRs before launching their primary payload.



EDR Bypass / Killers

A TA going by the handle Spyboy is selling an AV/EDR killer that is allegedly capable of killing almost every AV/EDR on the market.

I'm selling a private program to terminate all AVs/EDRs/XDRs in a legitimate way and it has been tested on most of AVs/EDRs/XDRs that exist in the mark such as, [REDACTED]

I want to mention that this method is a private one *"NOT like the one being sold on xss.is and other forums which does not work on windows 7 and windows server 2008"*

#satanisindor #proprietaria #dotanoceto #nature
#firewall #software #vreodenservarianre

A versão abrangente deste software, que afirma contornar vários EDRs bem conhecidos, está atualmente sendo vendida por US \$ 1.500. No entanto, como uma oferta antecipada, os cinco primeiros compradores podem aproveitá-la a um preço com desconto. Vale notar que o preço deve aumentar para US \$ 3.000 em um futuro próximo.

Abaixo está uma lista de EDRs que são supostamente suscetíveis ao encerramento usando este programa:

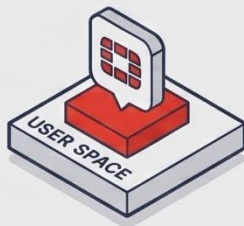


FortiEDR kernel integration benefits

Legacy Application Hooking

Location:

Operates in User Space.



Resilience:

Highly vulnerable to EDR Killers (Spyboy, etc.).



Impact:

High system overhead; prone to causing application crashes



FortiEDR Kernel Integration

Location:

Embedded in OS Kernel
(Native Windows / Linux)



Resilience:

Invisible and functionally immune to user-space termination.



Impact:

Near-zero performance impact due to native OS filtering.



Resilience by design: You cannot kill what you cannot reach.



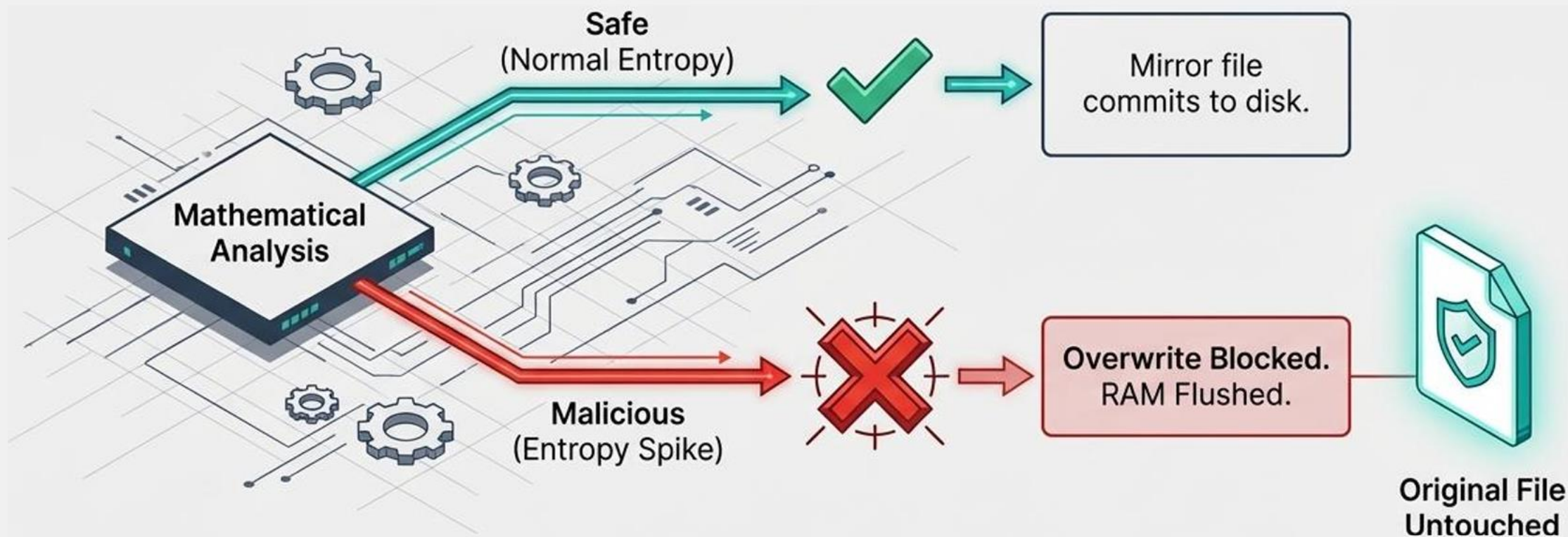
Anti-Ransomware Technique

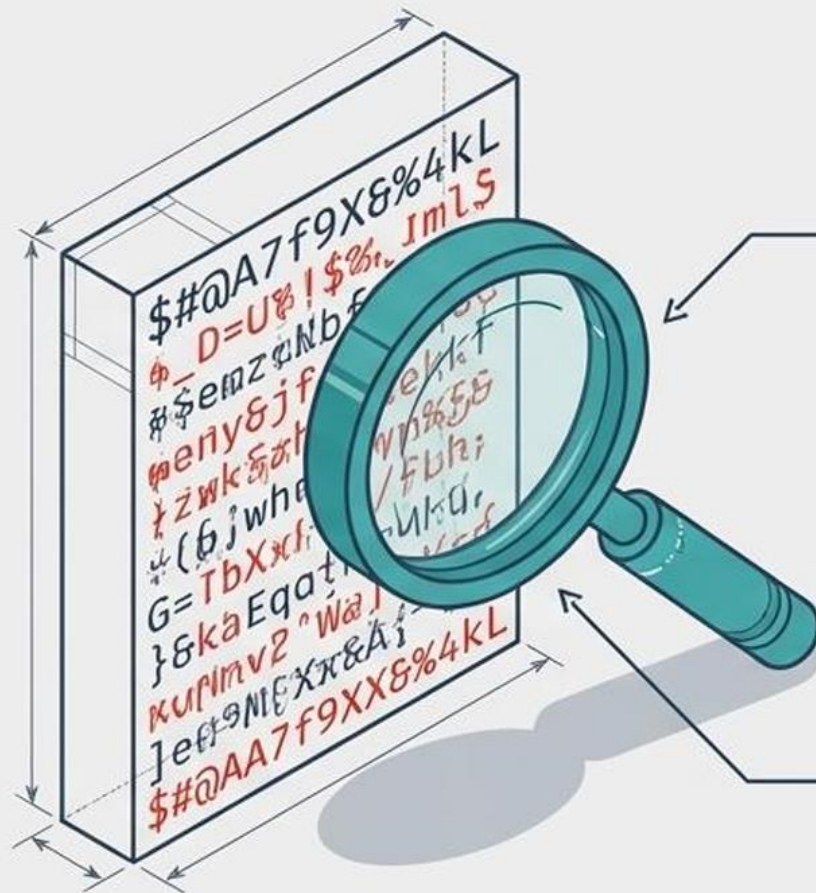
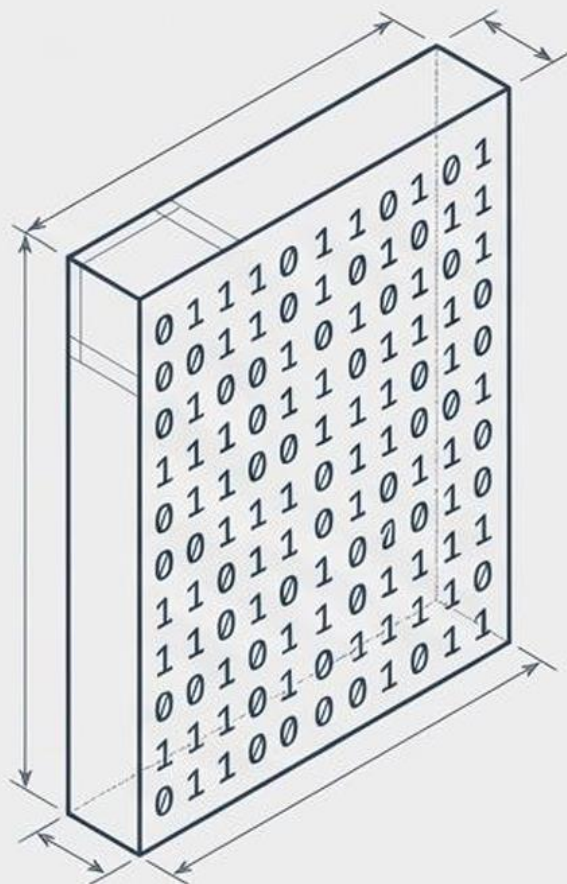
Patent US12174952B2





Anti-Ransomware: The Mirror idea





0x80 Entropy Calculation

FortiEDR calculates the randomness of the mirror file against the original file (using Shannon's method). High entropy spikes indicate cryptographic scrambling.

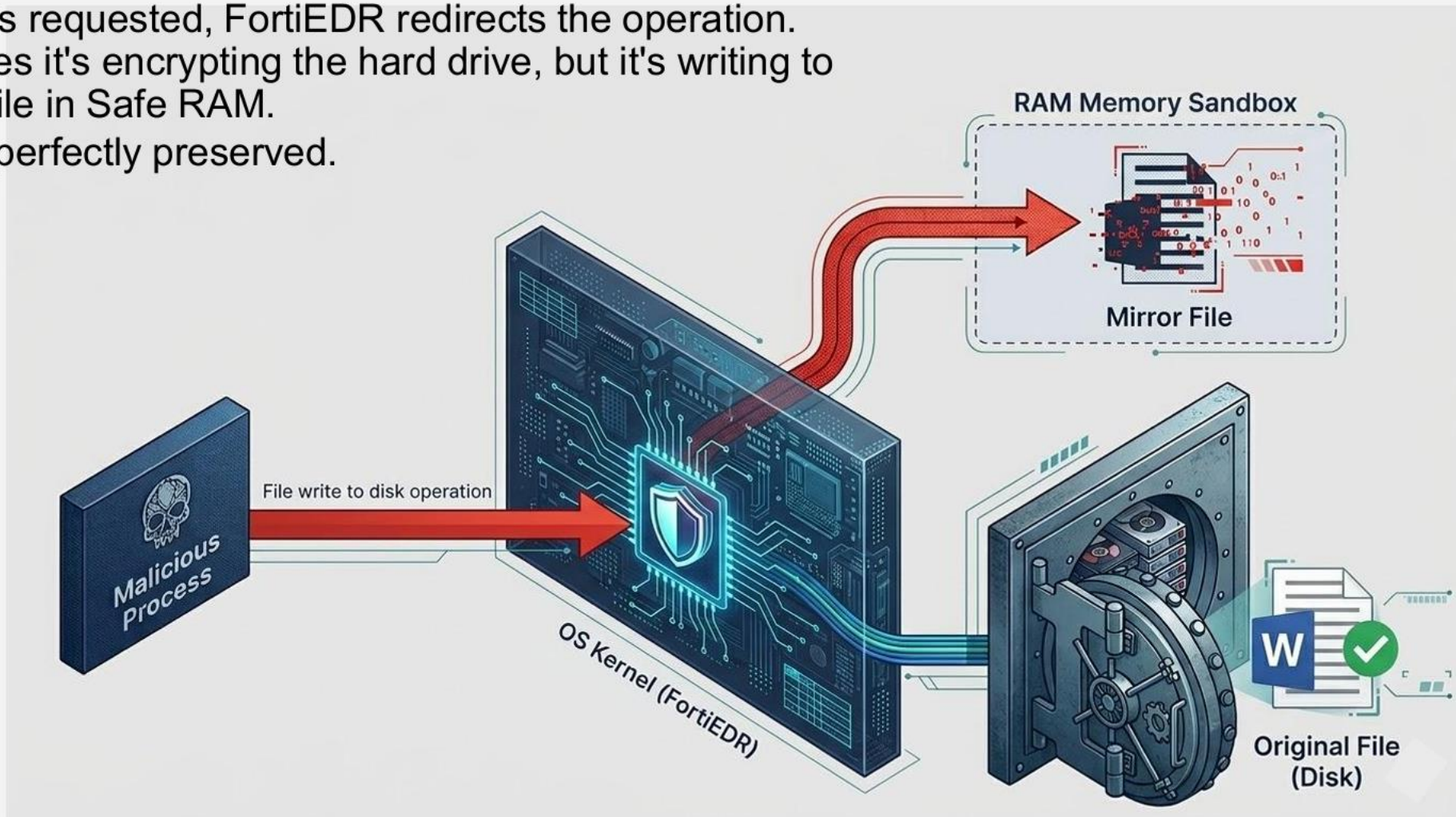
H_ENT Illegal Values

The system parses the file structure, comparing headers and fields against predefined allowed values to catch corrupted or invalid modifications.



Anti-Ransomware technique

When an overwrite is requested, FortiEDR redirects the operation. The malware believes it's encrypting the hard drive, but it's writing to a temporary Mirror file in Safe RAM. The original data is perfectly preserved.



Exclusions vs Exceptions





Exclusions vs Exceptions

When working with Exclusions, you can create exclusions based on a Process or the Security policy “Execution Prevention”. This feature is used when you need to avoid EDR of inspecting/blocking a particular software in a user device.

PROCESS EXCLUSION

Exclude the process below from monitoring by the various FortiEDR features
Note: all Process activities will be ignored

Operating system: Windows

Define process by:

☒ **Hash**
SHA-1 or SHA-2 or MD5. For example 418c1f073782a1c855890971ff18794f7a298f6d

☐ **Attributes** (Specify at least one attribute)

☐ File name

The problem is in this message:

Exclude the process below from monitoring by the various FortiEDR features

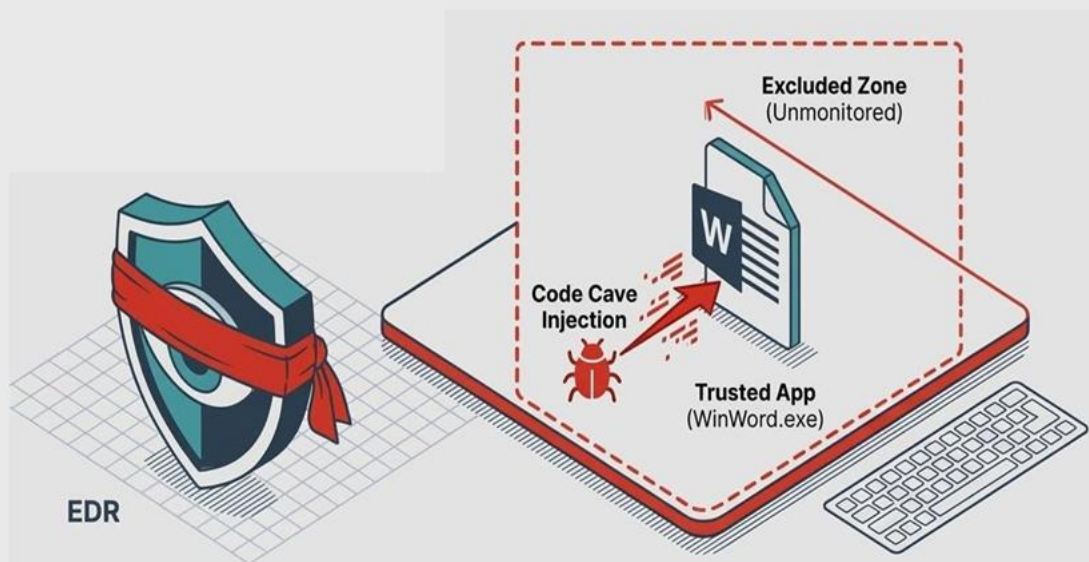
Note: all Process activities will be ignored



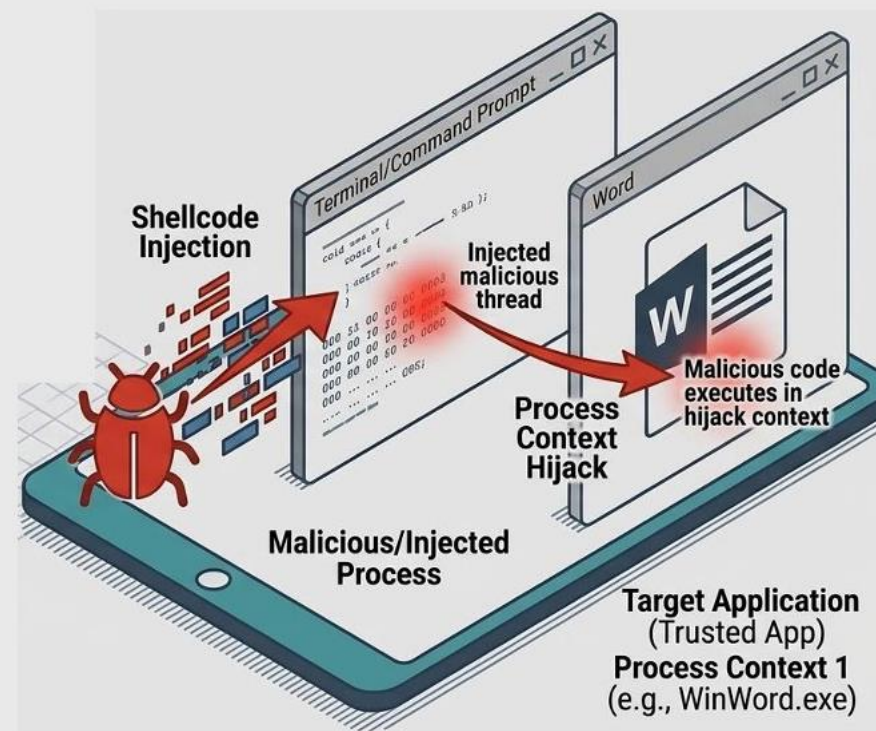
Exclusions vs Exceptions

Code Cave and Process Injection techniques

Code Cave



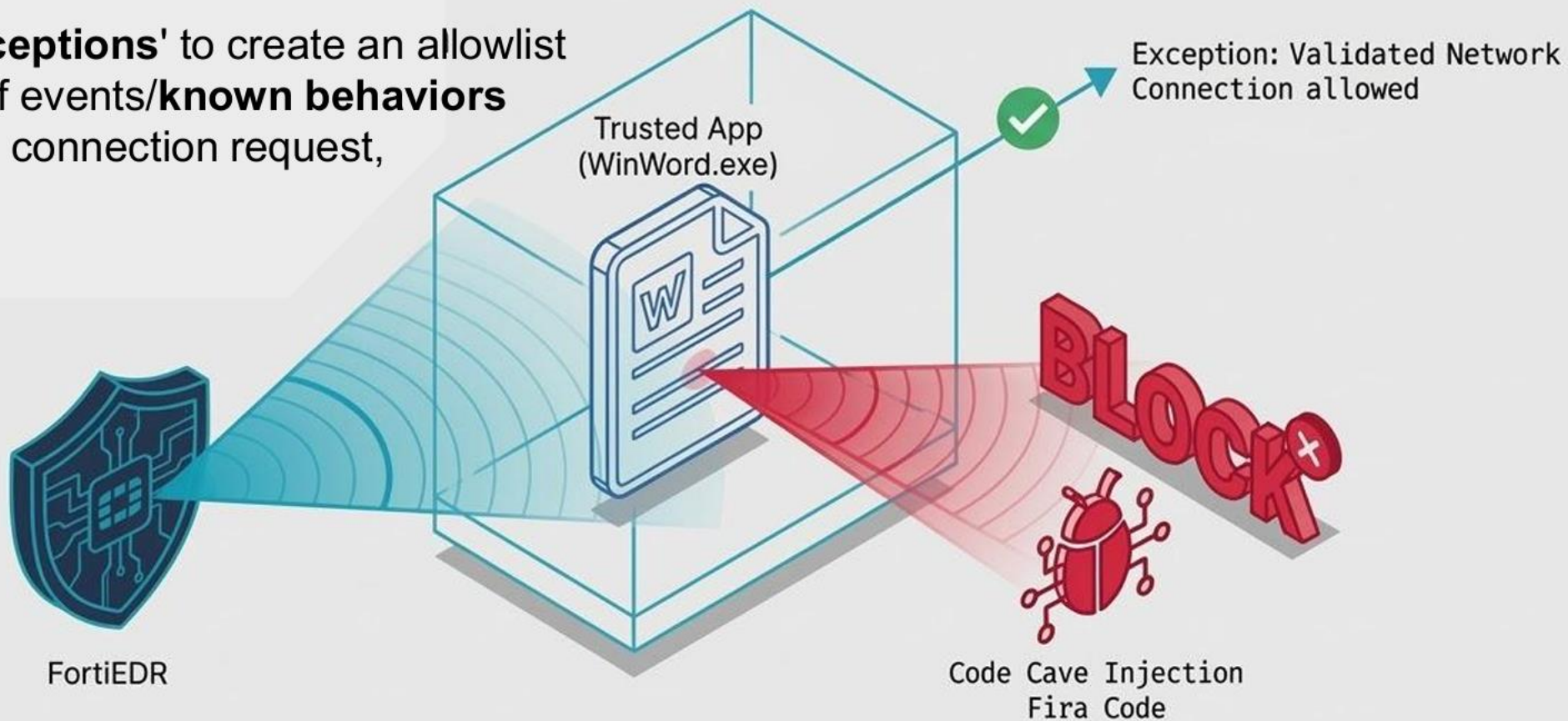
Process Injection





Exclusions vs Exceptions

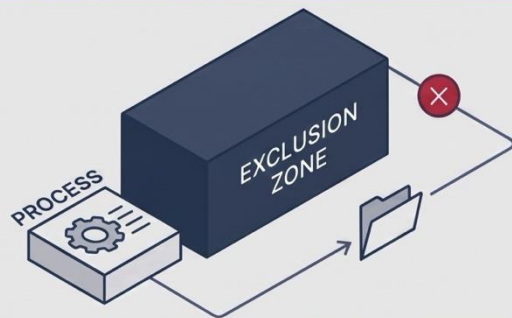
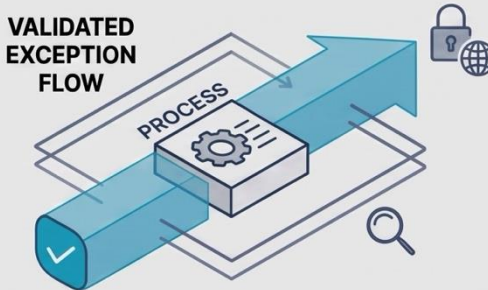
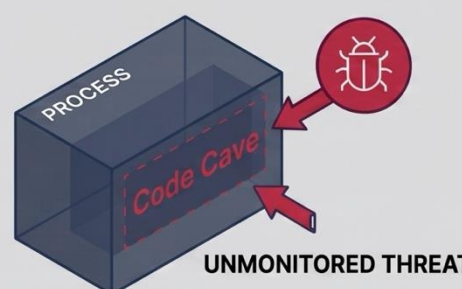
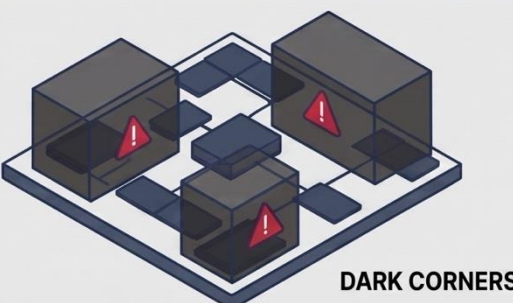
FortiEDR uses '**Exceptions**' to create an allowlist for **specific** flows of events/**known behaviors** (e.g., a known valid connection request, or script execution)



The system never stops watching. It continues to rigorously investigate all other behaviors within the process, instantly catching injected Code Caves while allowing legitimate business functions to run.



Exclusions vs Exceptions

	Exclusions (Legacy) 	Exceptions (FortiEDR) 
Scope	Ignores the entire process, file, or path. 	Allows only a specific, validated flow of events or connections. 
Vulnerability	Highly vulnerable to Code Cave/Shelter injections. 	Completely secure; continuous behavioral investigation remains active. 
Management	Creates dark, unmonitored corners in the IT environment. 	Applies intelligently across all policies via the FortiEDR Exception Manager. 

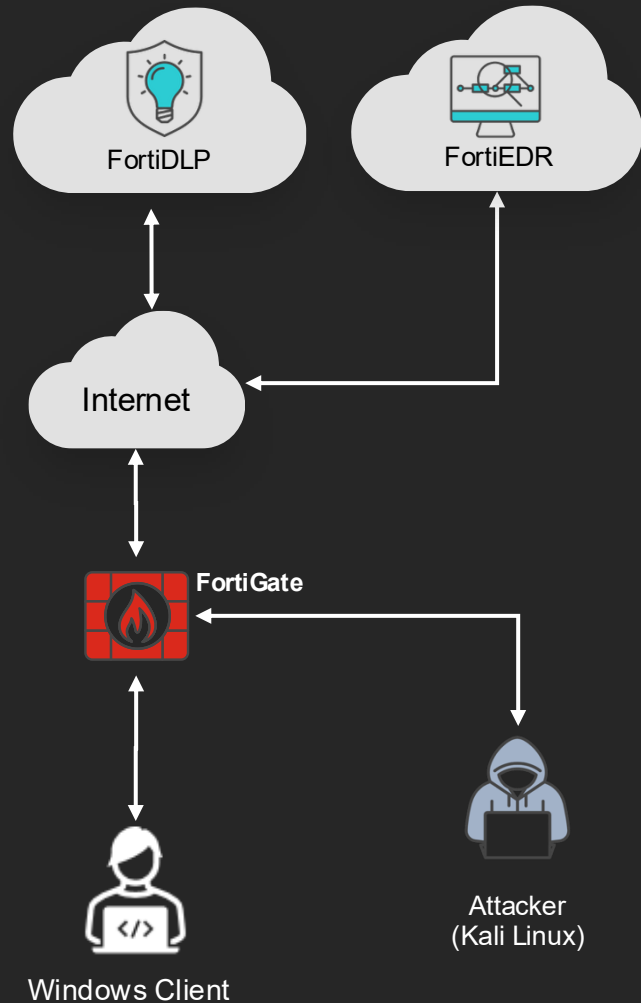
FORTINET | COLOMBIA
& ECUADOR
XPERTS26

Hands on Lab





Architecture



1.

Initial Setup

2.

Testing New FortiEDR Features

3.

Step-by-Step Post-Exploitation Guide

4.

Encrypting user files

5.

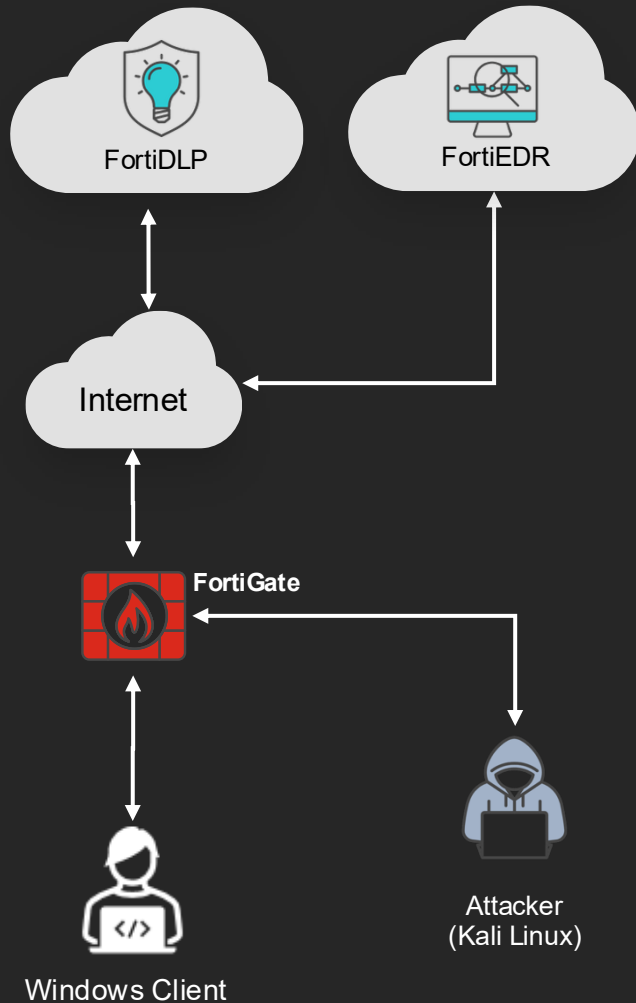
Data Exfiltration

6.

Cover your tracks



Architecture



Lab Access

<https://fndn.fortinet.net/index.php?/fortidemocse/signup/3AFF33>

Lab Guide



<https://latam.amerintxperts.com/secops/AntiRansomware-26/index.html>

amerintxperts
xPerts2026!



XPERTS26

Phase 1 – Initial Setup

Activities

- Onboard endpoint
- Apply protection controls
- Activate automated response
- Validate security readiness

Discovery

- Endpoint status
- Security coverage
- Protection gaps

Result

- Protected endpoint
- Active controls
- Ready environment

```
msiexec /i C:\Fortinet\Collector\Installer.MSI /qr  
AGG=35.198.34.136:8081 PWD=fortiedr-xperts26  
ORG=XPRTS_SOLA_GIZAGALLEGOS
```

Impact

- Reduced attack surface
- Increased visibility
- Stronger protection

Tests Performed

- Endpoint onboarding
- Security validation
- Policy enforcement
- Response verification



30 min

Phase 2 – Testing New FortiEDR Features

Activities

- Validate endpoint controls
- Test browser protection
- Review security posture
- Explore data protection features

Discovery

- Unauthorized connections
- Risky web activity
- Security gaps
- Device protection status

Result

- Enhanced visibility
- Stronger endpoint controls
- Improved policy effectiveness
- Better user protection

Impact

- Reduced attack surface
- Lower data exposure risk
- Improved compliance readiness
- Increased security posture

Tests Performed

- Firewall control testing
- Secure browser validation
- Web access restrictions
- Security posture verification



30 min

Phase 3 – Step-by-Step Post-Exploitation Guide

Activities

- Simulate attacker activity
- Validate threat visibility
- Track user and system actions
- Monitor security controls

Discovery

- Compromised endpoints
- Privilege abuse attempts
- Credential exposure
- Suspicious user activity

Result

- Attack path identified
- Security events generated
- Threat activity correlated
- Detection coverage validated

Impact

- Improved threat visibility
- Faster investigation
- Better risk awareness
- Stronger response readiness

Tests Performed

- Initial compromise validation
- Privilege escalation testing
- User activity monitoring
- Credential access detection



60 min

Phase 4 – Encrypting user files

Activities

- Simulate ransomware execution
- Monitor file encryption activity
- Analyze security incidents
- Review attack progression

Discovery

- Ransomware behavior
- Affected files
- Security alerts
- Attack timeline

Result

- Encryption attempt detected
- Malicious activity blocked
- Incident correlated
- Attack path identified

Impact

- Data loss prevention
- Reduced business disruption
- Faster incident response
- Improved threat visibility

Tests Performed

- Ransomware simulation
- File protection validation
- Incident analysis
- Attack flow investigation



45 min

Phase 5 – Data Exfiltration

Activities

- Simulate data collection
- Attempt external data transfer
- Monitor user file access
- Validate protection controls

Discovery

- Sensitive documents
- Unauthorized transfers
- Data movement activity
- High-risk behavior

Result

- Exfiltration attempt detected
- Data transfer blocked
- Incident generated
- User data protected

Impact

- Reduced data loss risk
- Improved data visibility
- Stronger protection controls
- Faster threat containment

Tests Performed

- File discovery validation
- Data transfer simulation
- Exfiltration detection
- Incident verification



45 min

Phase 6 – Cover your tracks

Activities

- Simulate log tampering
- Remove activity records
- Validate security monitoring
- Review incident visibility

Discovery

- Log deletion attempts
- Defense evasion activity
- Suspicious system actions
- Forensic gaps

Result

- Tampering detected
- Incident generated
- Activity correlated
- Visibility maintained

Impact

- Improved investigation readiness
- Better threat detection
- Stronger forensic visibility
- Reduced attacker concealment

Tests Performed

- Log clearing simulation
- Tampering detection
- Alert validation
- Incident review



15 min



FORTINET

COLOMBIA
& ECUADOR

XPERTS26