Protect your company against Zero Day attacks

Mikkel Bossen | Channel SE

May 2021

2020 Top Ransomware Variants

Threat Assessment: WastedLocker Ransomware

28,816 people reacted | 9 | 4 min. read

SHARE

By Alex Hinchliffe, Doel Santos, Adrian McCabe and Robert Falcone
July 30, 2020 at 6:00 AM
Category: Unit 42
Tags: AutoFocus, Cortex, Cybercrime, JavaScript, malware, PANDB, ransomware, SocGholish, threat assessment, threat prevention, URL filtering, WastedLocker, WildFire

tag: WastedLocker.

- Ryuk
- Maze (ChaCha)
- Defray777
- WastedLocker
- GandCrab + REvil
- NetWalker
- DoppelPaymer
- Dharma
- Phobos
- Zepplin

UNIT 42

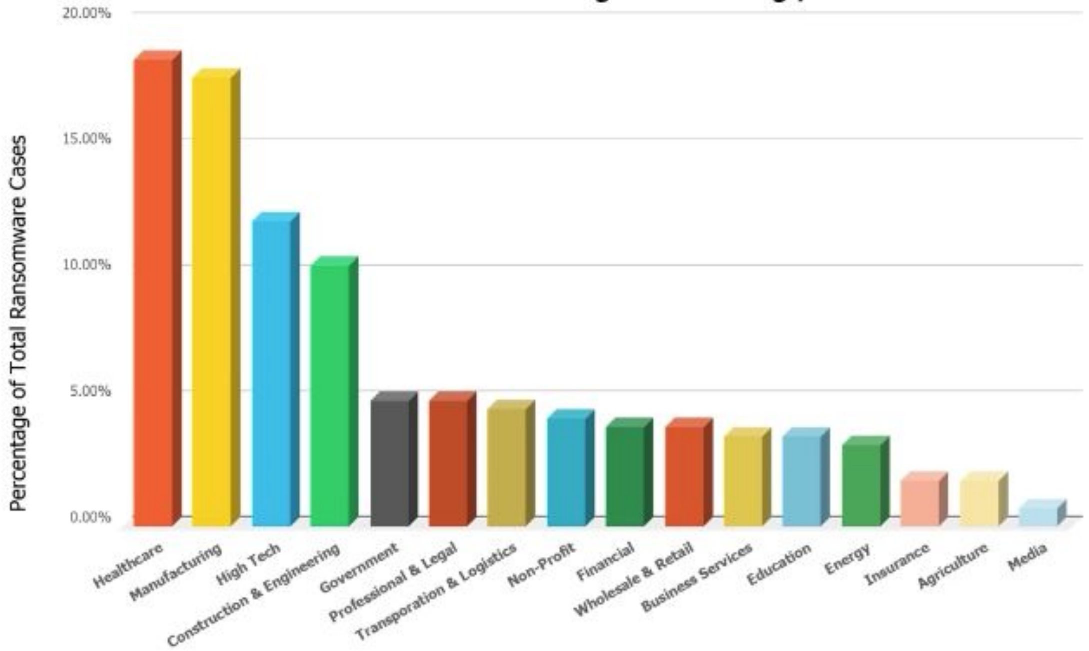
Ransomware Threat Report

2021

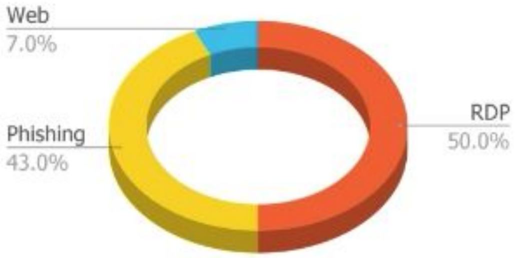
https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html

Ransomware by the Numbers

Ransomware Cases by Industry, 2020



Most Frequent Attack Vectors



Ransom Demands

- 2019 Average Paid: $115k
- 2020 Average Paid: $312k
- 2020 Highest Demand: $30m
- 2020 Highest Paid: $10m

Sources: 2020 Crypsis Incident Response and Data Breach Report, Crypsis; 2021 Ransomware Report, Unit 42

Global Cybercrime Damage Costs:

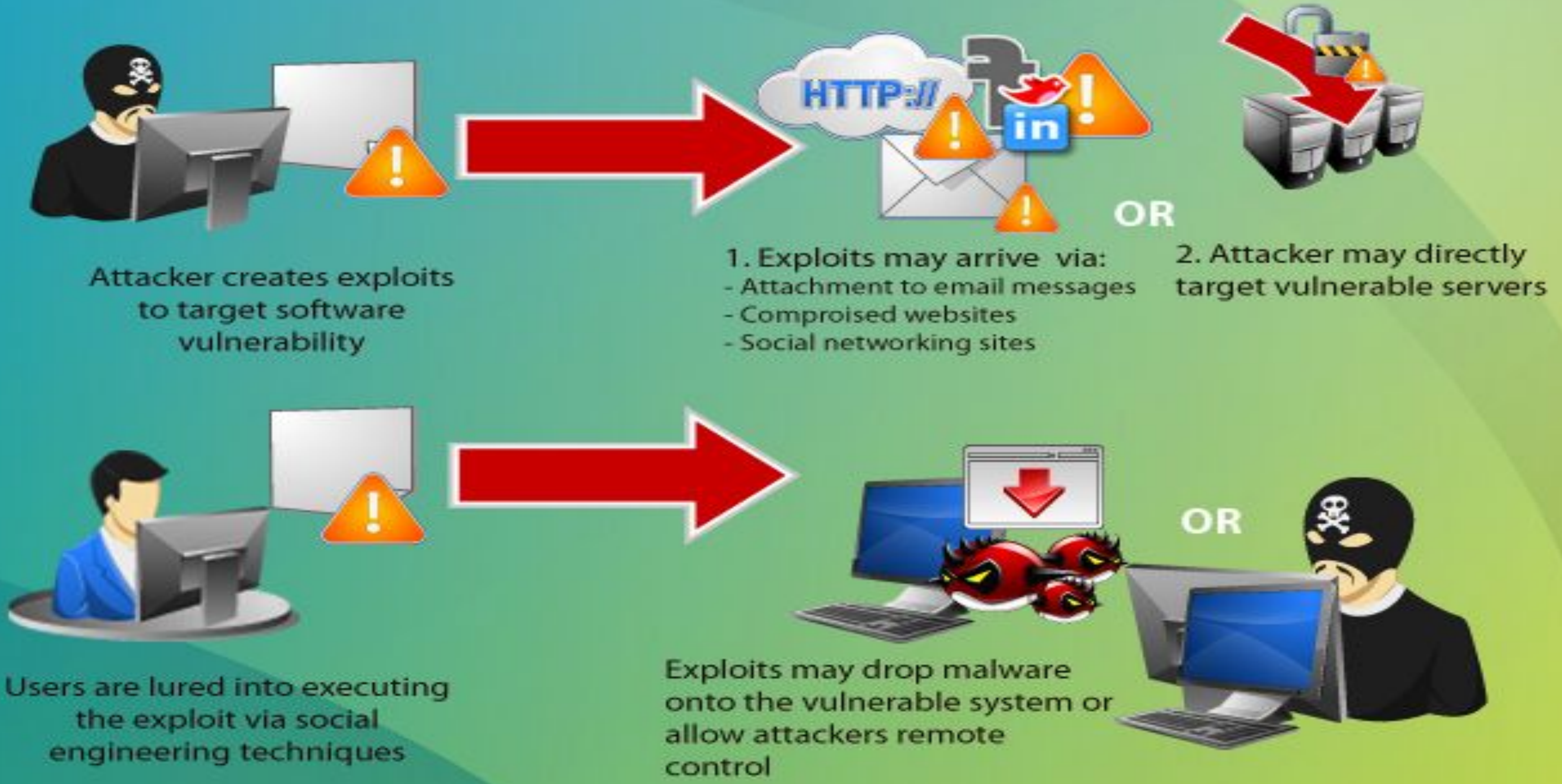
- $6 Trillion USD a Year. *
- $500 Billion a Month.
- $115.4 Billion a Week.
- $16.4 Billion a Day.
- $684.9 Million an Hour.
- $11.4 Million a Minute.
- $190,000 a Second.

ALL FIGURES ARE PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES

CYBERSECURITY VENTURES

When Attackers Target Vulnerabilities



Attacker creates exploits to target software vulnerability

1. Exploits may arrive via:
- Attachment to email messages
- Comproised websites
- Social networking sites

OR

2. Attacker may directly target vulnerable servers

Users are lured into executing the exploit via social engineering techniques

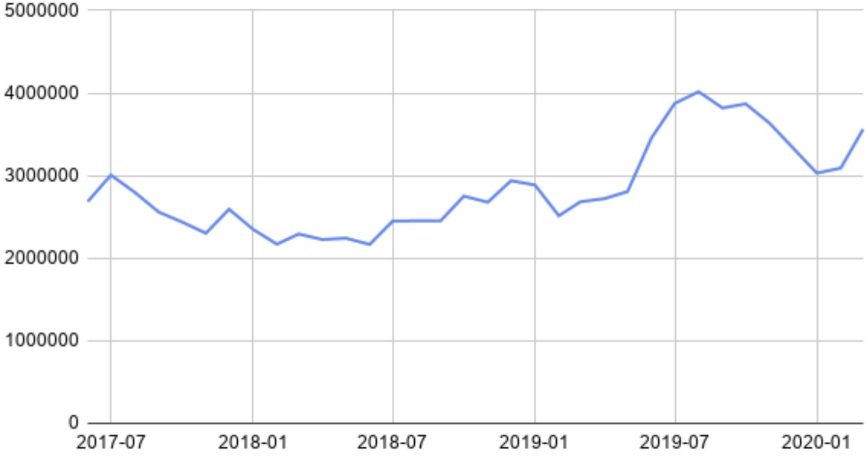
Exploits may drop malware onto the vulnerable system or allow attackers remote control

OR

Unsecured RDP Connections

Unsecured RDP connections.

69% of organizations expose RDP (port 3389). Up 30%

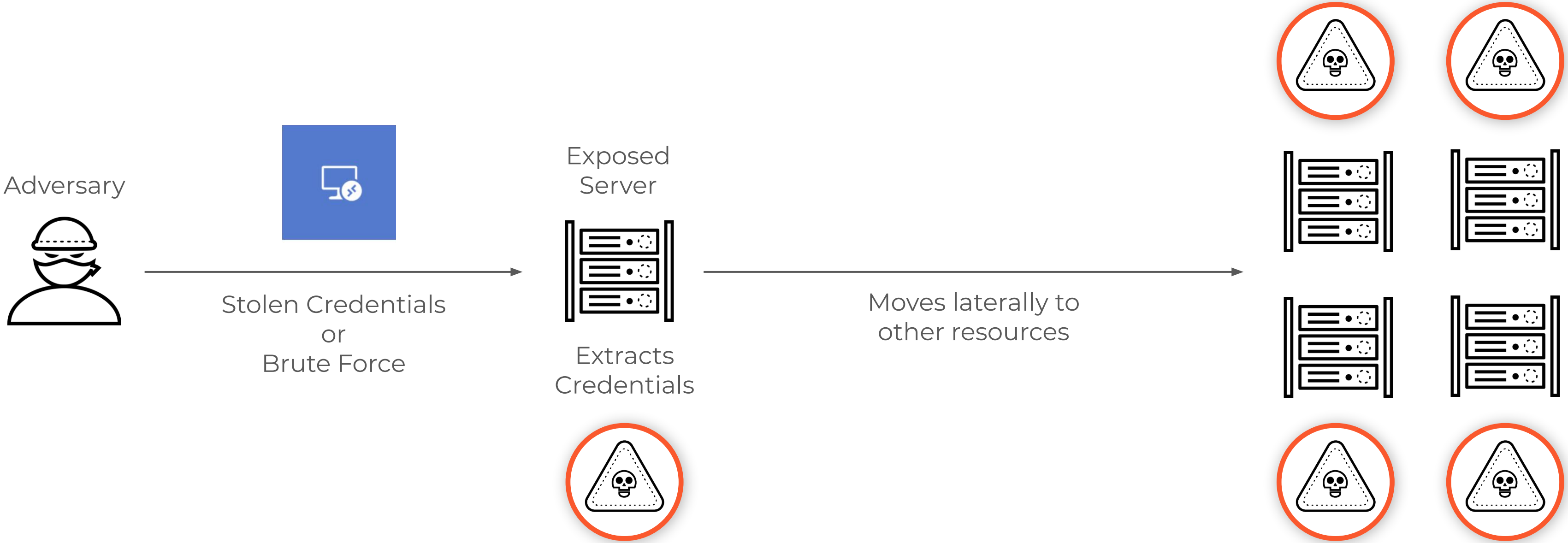


https://blog.shodan.io/trends-in-internet-exposure/

UNIT 42 **Cloud Threat Report**

* Putting the Sec into DevOps Spring 2020

Exposed RDP Adversary Workflow



Adversary

Stolen Credentials
or
Brute Force

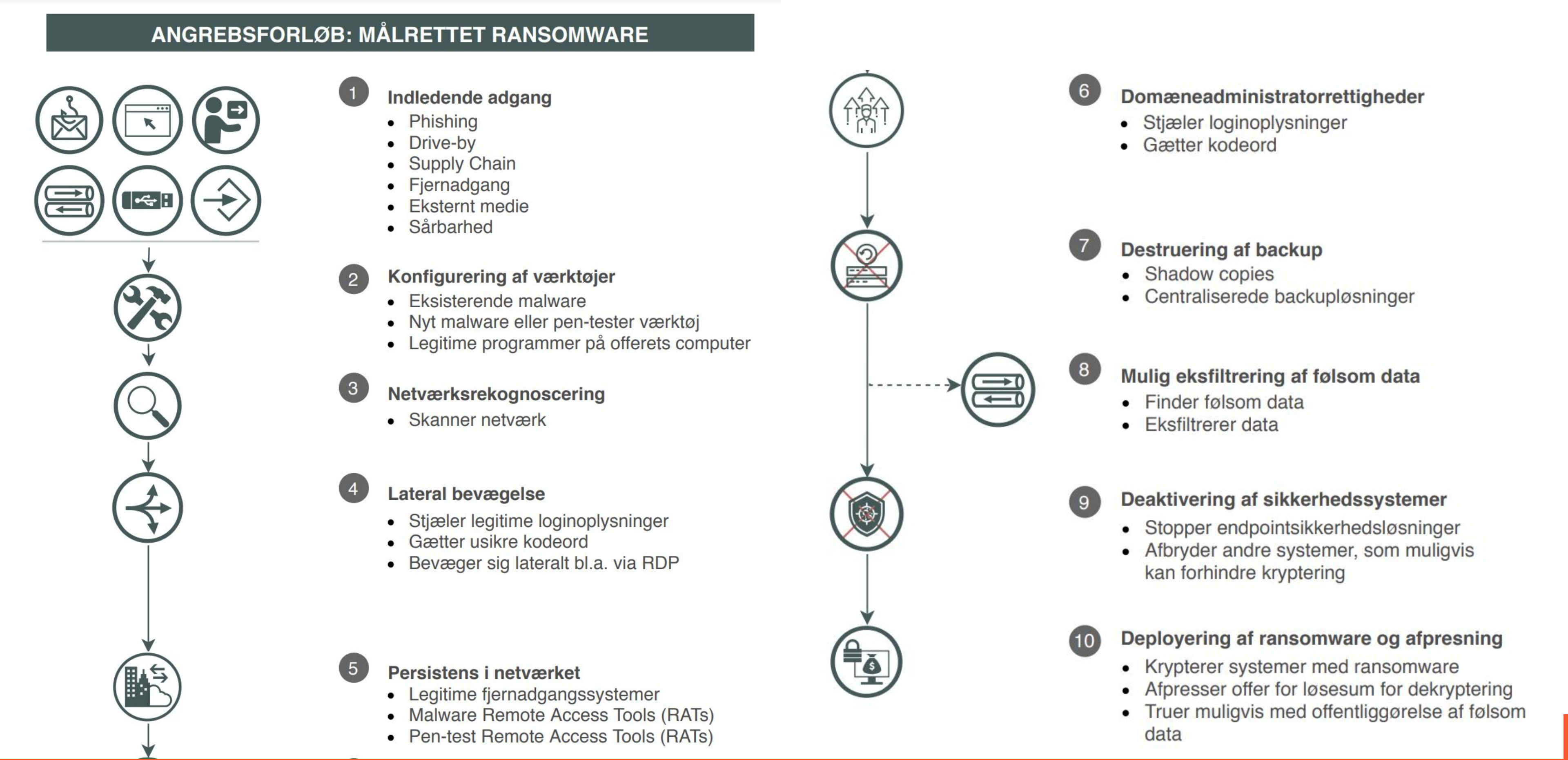
Exposed
Server

Extracts
Credentials

Moves laterally to
other resources

https://cfcs.dk/globalassets/cfcs/dokumenter/rapporter/CFCS-rapport-anatomien-af-maalrettede-ransomwareangreb.pdf

Anatomien af målrettede ransomware angreb



ANGREBSFORLØB: MÅLRETTET RANSOMWARE

1 **Indledende adgang**
- Phishing
- Drive-by
- Supply Chain
- Fjernadgang
- Eksternt medie
- Sårbarhed

2 **Konfigurering af værktøjer**
- Eksisterende malware
- Nyt malware eller pen-tester værktøj
- Legitime programmer på offerets computer

3 **Netværksrekognoscering**
- Skanner netværk

4 **Lateral bevægelse**
- Stjæler legitime loginoplysninger
- Gætter usikre kodeord
- Bevæger sig lateralt bl.a. via RDP

5 **Persistens i netværket**
- Legitime fjernadgangssystemer
- Malware Remote Access Tools (RATs)
- Pen-test Remote Access Tools (RATs)

6 **Domæneadministratorrettigheder**
- Stjæler loginoplysninger
- Gætter kodeord

7 **Destruering af backup**
- Shadow copies
- Centraliserede backupløsninger

8 **Mulig eksfiltrering af følsom data**
- Finder følsom data
- Eksfiltrerer data

9 **Deaktivering af sikkerhedssystemer**
- Stopper endpointsikkerhedsløsninger
- Afbryder andre systemer, som muligvis kan forhindre kryptering

10 **Deployering af ransomware og afpresning**
- Krypterer systemer med ransomware
- Afpresser offer for løsesum for dekryptering
- Truer muligvis med offentliggørelse af følsom data

Security Needs - When Talking about Zero Day Attacks

Protection against Vulnerability Exploitation

Protection against Execution of Malicious Code

Visibility into Attack Surface

Segmentation of Infrastructure - Zero Trust

Backup and Recovery is Essential

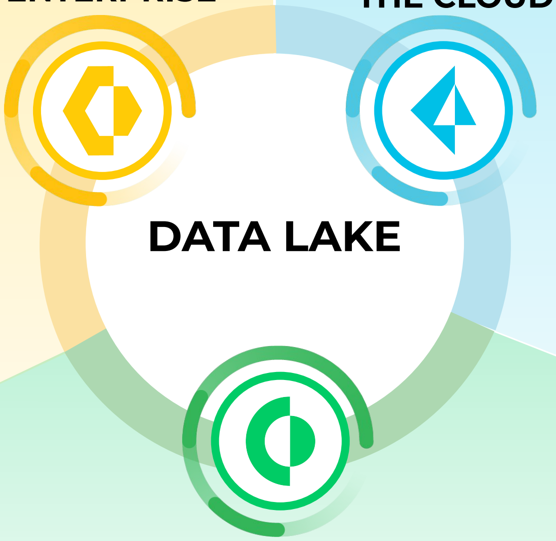
STRATA™
BY PALO ALTO NETWORKS

Preventing ransomware with machine learning powered NGFW

March 2021

paloalto®
NETWORKS

Securing Your Transformed Enterprise



STRATA
SECURE
THE ENTERPRISE

Hybrid data center

Internet Perimeter

Branch & mobile &
SD-WAN

5G & IoT

Secure access

PRISMA
SECURE
THE CLOUD

SaaS

Public cloud

DevOps

DATA LAKE

CORTEX
SECURE
THE FUTURE

Endpoint
protection

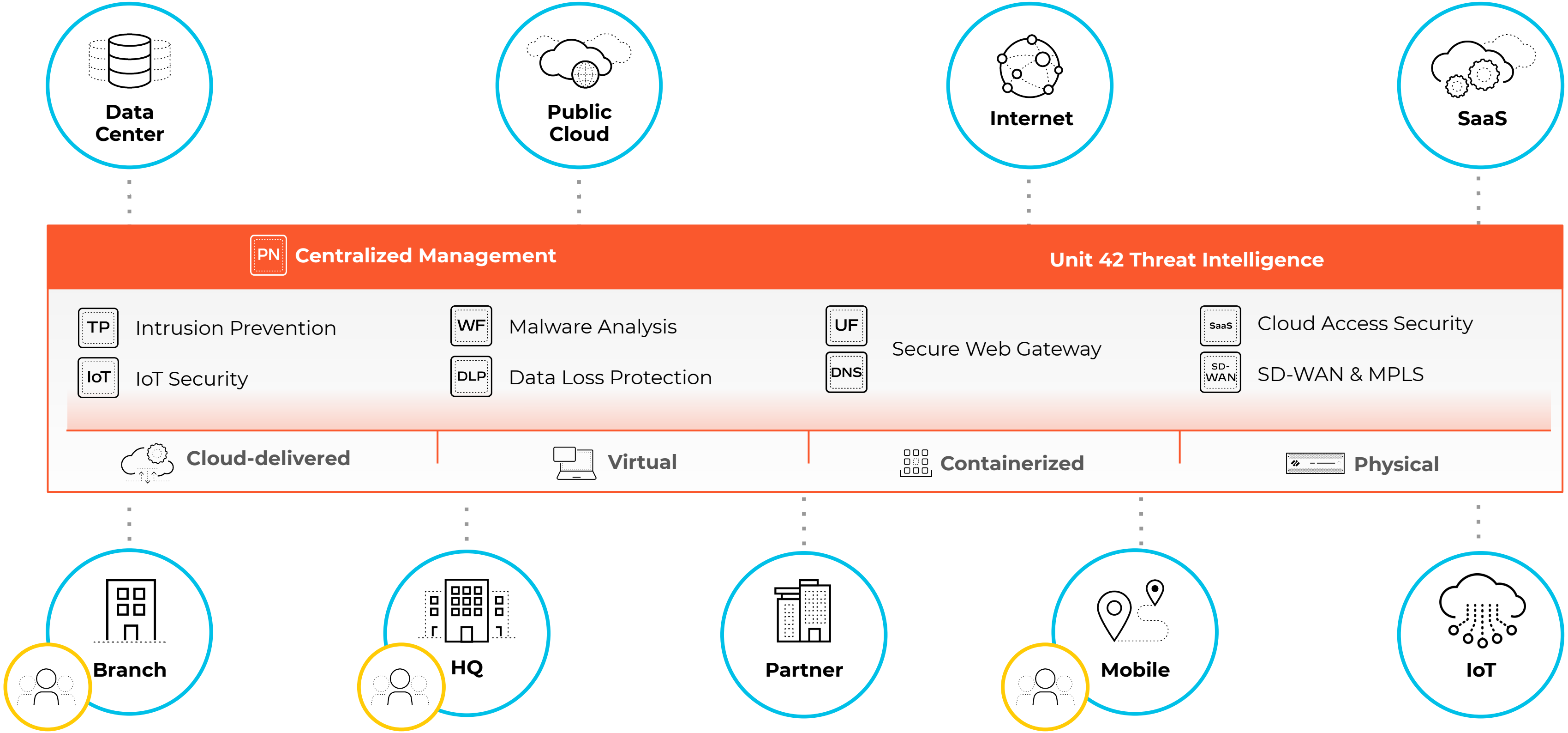
Detection &
response

Automation &
orchestration

Network traffic &
behavioral analytics

Threat
intelligence

A Single Platform to Connect and Secure Everything



Data Center

Public Cloud

Internet

SaaS

PN Centralized Management

Unit 42 Threat Intelligence

TP Intrusion Prevention

IoT IoT Security

WF Malware Analysis

DLP Data Loss Protection

UF DNS Secure Web Gateway

SaaS Cloud Access Security

SD-WAN SD-WAN & MPLS

Cloud-delivered

Virtual

Containerized

Physical

Branch

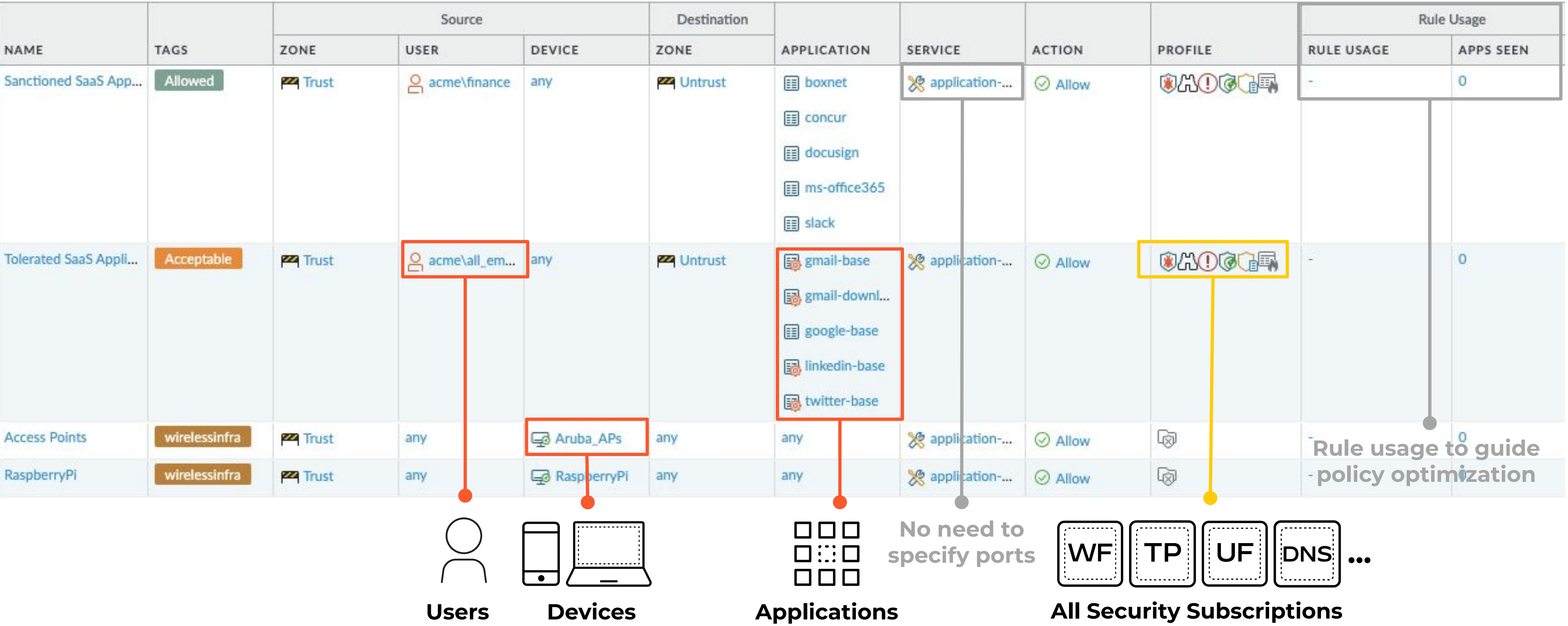
HQ

Partner

Mobile

IoT

Zero Trust based security rules that support your business



		Source			Destination					Rule Usage	
NAME	TAGS	ZONE	USER	DEVICE	ZONE	APPLICATION	SERVICE	ACTION	PROFILE	RULE USAGE	APPS SEEN
Sanctioned SaaS App...	Allowed	Trust	acme\finance	any	Untrust	boxnet concur docusign ms-office365 slack	application-...	Allow		-	0
Tolerated SaaS Appli...	Acceptable	Trust	acme\all_em...	any	Untrust	gmail-base gmail-downl... google-base linkedin-base twitter-base	application-...	Allow		-	0
Access Points	wirelessinfra	Trust	any	Aruba_APs	any	any	application-...	Allow		-	0
RaspberryPi	wirelessinfra	Trust	any	RaspberryPi	any	any	application-...	Allow		-	

Rule usage to guide policy optimization

Users

Devices

Applications

No need to specify ports

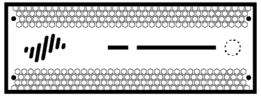
All Security Subscriptions

One Policy One Unified Console

NGFW features and subscriptions

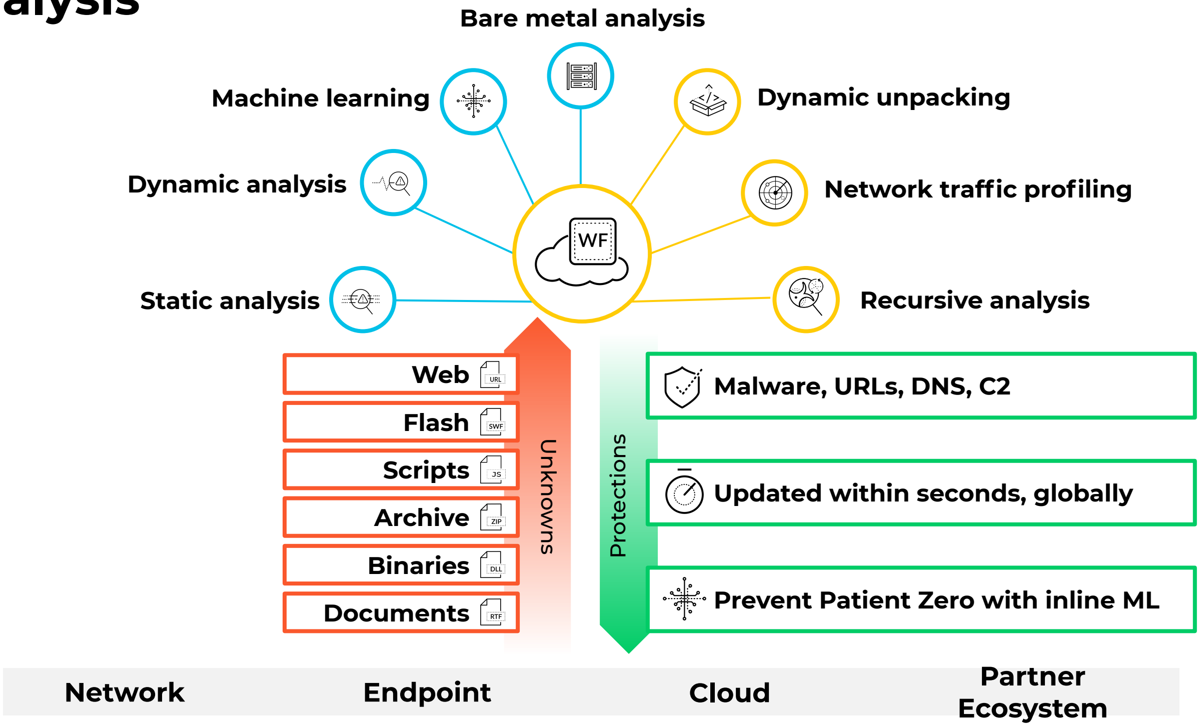
Cloud Delivered Security Subscriptions

TP	UF	WF	DNS	IoT	DLP	GP	SD-WAN
			PAN-OS 9.0	PAN-OS 8.1 (PAN-OS 10)	PAN-OS 10.0		PAN-OS 9.1
Threat Prevention	URL Filtering	WildFire	DNS Security	IoT Security	Data Loss Prevention	Global Protect	SD-WAN
Prevent all known threats across all traffic in a single pass	Prevent access to known and new malicious websites	Ensures files are safe with automatic detection and prevention of unknown malware	Disrupts attacks that use DNS for command-and-control and data theft	Visibility and protection of IoT and OT devices	Consistent protection from sensitive data loss	VPN service to extends NGFW capabilities everywhere	Networking and security natively integrated



NGFW value keeps increasing through continuous innovation

Detect and Prevent New and unknown Threats with WildFire Malware Analysis



Bare metal analysis

Machine learning

Dynamic unpacking

Dynamic analysis

Network traffic profiling

Static analysis

Recursive analysis

Web

Flash

Scripts

Archive

Binaries

Documents

Unknowns

Protections

Malware, URLs, DNS, C2

Updated within seconds, globally

Prevent Patient Zero with inline ML

Network

Endpoint

Cloud

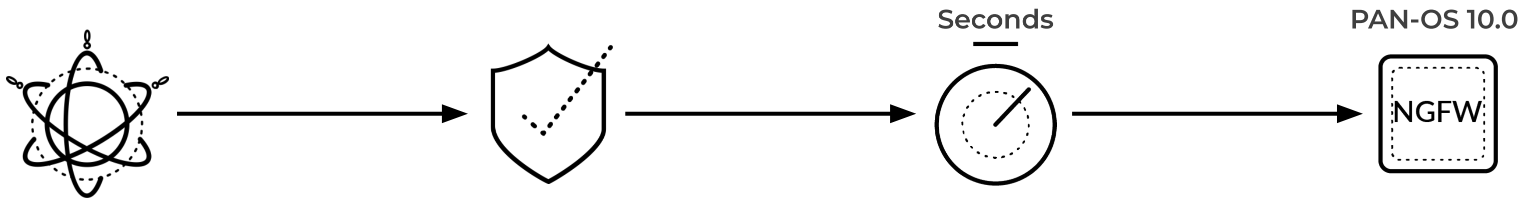
Partner Ecosystem

Data collected from a vast global community

Analysis techniques far beyond traditional sandboxing

Automated protection against multiple attack variants

Slashing Our Industry-Leading Time for Distributed Protections



Threat detected across 35K+ WF installed base

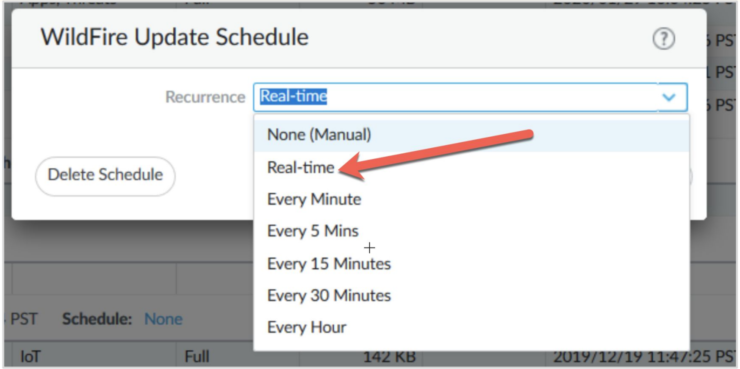
Content-Based Signature Created

Protection streamed in seconds

All customers with WildFire updated

BEFORE

Industry-leading *5-minute* signature generation/ distribution time



WildFire Update Schedule

Recurrence: Real-time

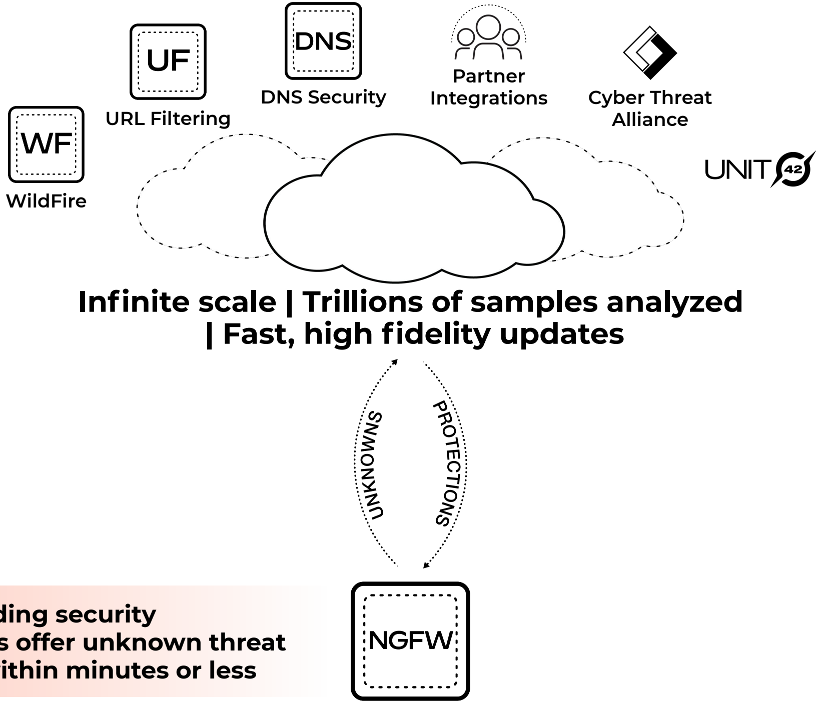
PST Schedule: None

IoT Full 142 KB 2019/12/19 11:47:25 PST

With PAN-0S 10.0

Protection streams to NGFW in *single-digit seconds*

Today’s Prevention of Unknown Threats Through Cloud Scale, PAN-OS 9.X



Infinite scale | Trillions of samples analyzed | Fast, high fidelity updates

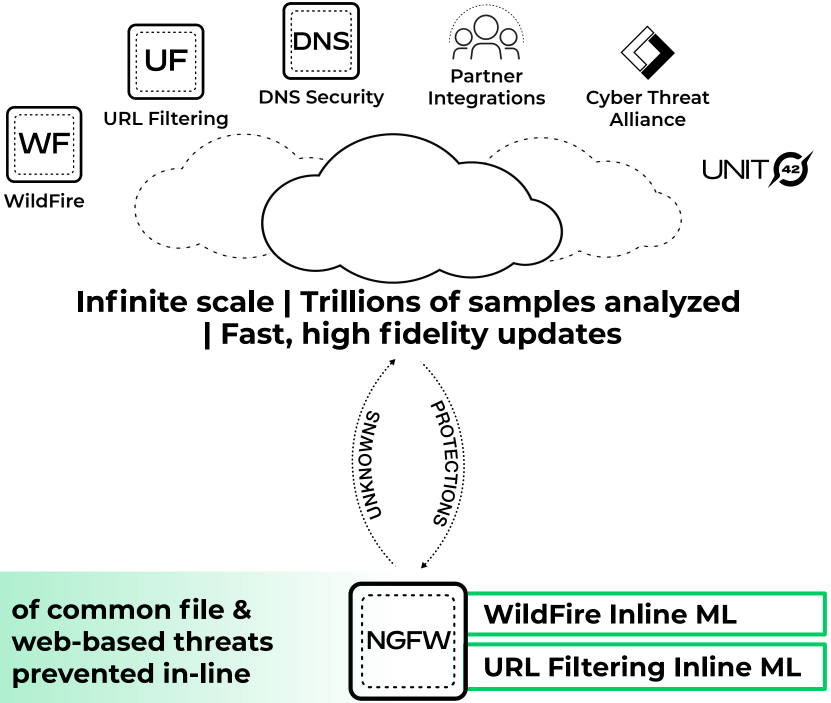
Industry-leading security subscriptions offer unknown threat protection within minutes or less

Cloud-delivered security services **scale prevention** capabilities

Shared intelligence allows the **fastest distribution** of protections

- File Protections: **5 min**
- URL Protections : **1 min**
- DNS Protections: **Instant**

Prevention of Unknown Threats with Inline Machine Learning, PAN-OS 10



Infinite scale | Trillions of samples analyzed | Fast, high fidelity updates

Up to 95% **of common file & web-based threats prevented in-line**

Cloud-delivered security services **scale prevention** capabilities

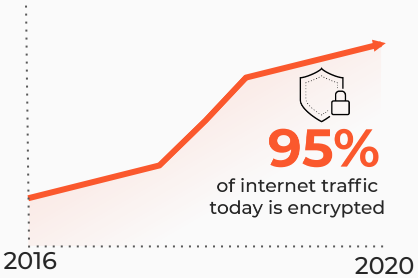
Shared intelligence allows the **fastest distribution** of protections

File Protections: **Instant**

URL Protections : **Instant**

DNS Protections: **Instant**

Current Trends With TLS



95%
of internet traffic
today is encrypted

Encrypted traffic is now the norm

70% of malware campaigns in 2020 will use encryption to conceal malicious activity (Gartner)

Weak protocols will not be supported

TLS 1.0 and TLS 1.1 can be deprecated anytime and modern protocols (HTTP/2, TLS 1.3) gaining popularity

Obtaining certs is easier than ever

Services like Let's Encrypt offer certificates for free

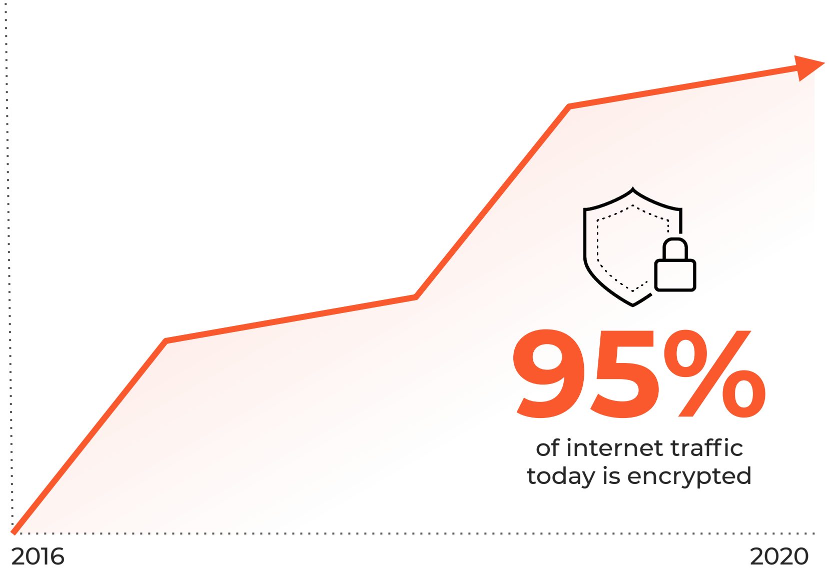
([Let's Encrypt]())

Rapid move to secure web (HTTPS)

Major browsers mark non-HTTPs sites as "Not Secure"

Massive Risks Within Encrypted Traffic

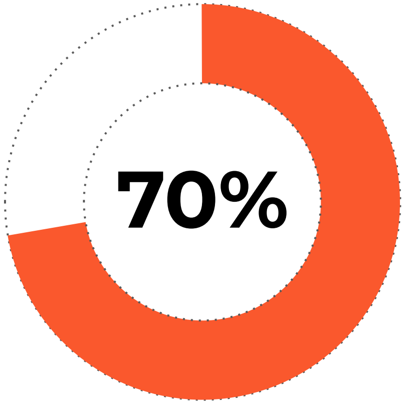
Encrypted traffic is now the norm



95%

of internet traffic
today is encrypted

And attackers are taking advantage



More than 70% of malware campaigns in 2020 will use some type of encryption to conceal malicious activity, says Gartner

Source: Encrypted Traffic (2016) | Encrypted Traffic (2020) | Encrypted Walwave (Gartner)

|

Deploying Decryption Is Now Easier Than Ever with PAN-OS 10

Mitigate security risks

Control use of legacy TLS protocols, insecure ciphers & incorrectly configured certs

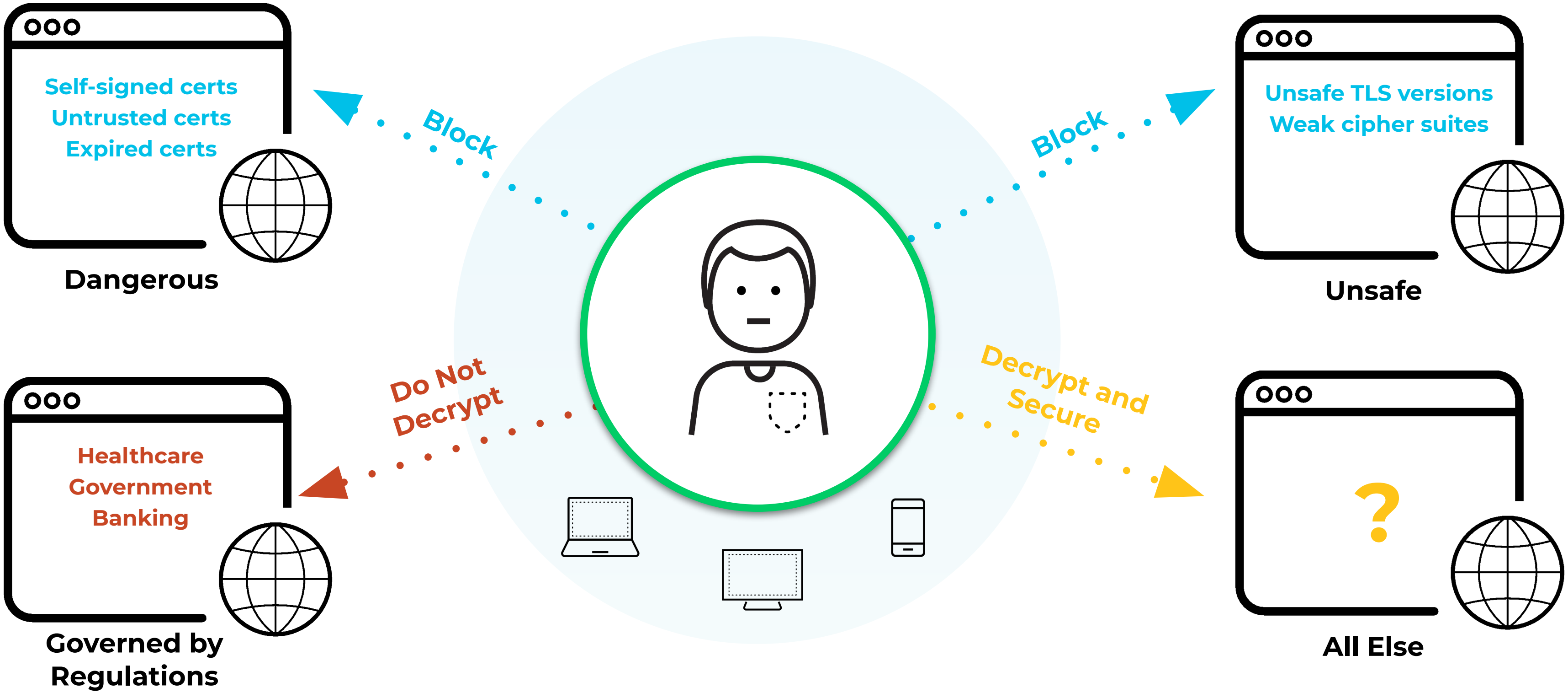
Deploy decryption, worry-free

Easily deploy and maintain decryption using purpose-built troubleshooting & visibility

Secure cloud apps quickly

Secure traffic that uses protocols like TLS 1.3 and HTTP/2.

Secure Encrypted Traffic Without Compromising Privacy



Return to Security

CORTEX™
BY PALO ALTO NETWORKS

CORTEX XDR

Extended detection and response

paloalto® NETWORKS

Cortex Vision for Proactive Security

Scope and protect your attack surface

EXPANSE
A PALO ALTO NETWORKS COMPANY

Prevent everything you can

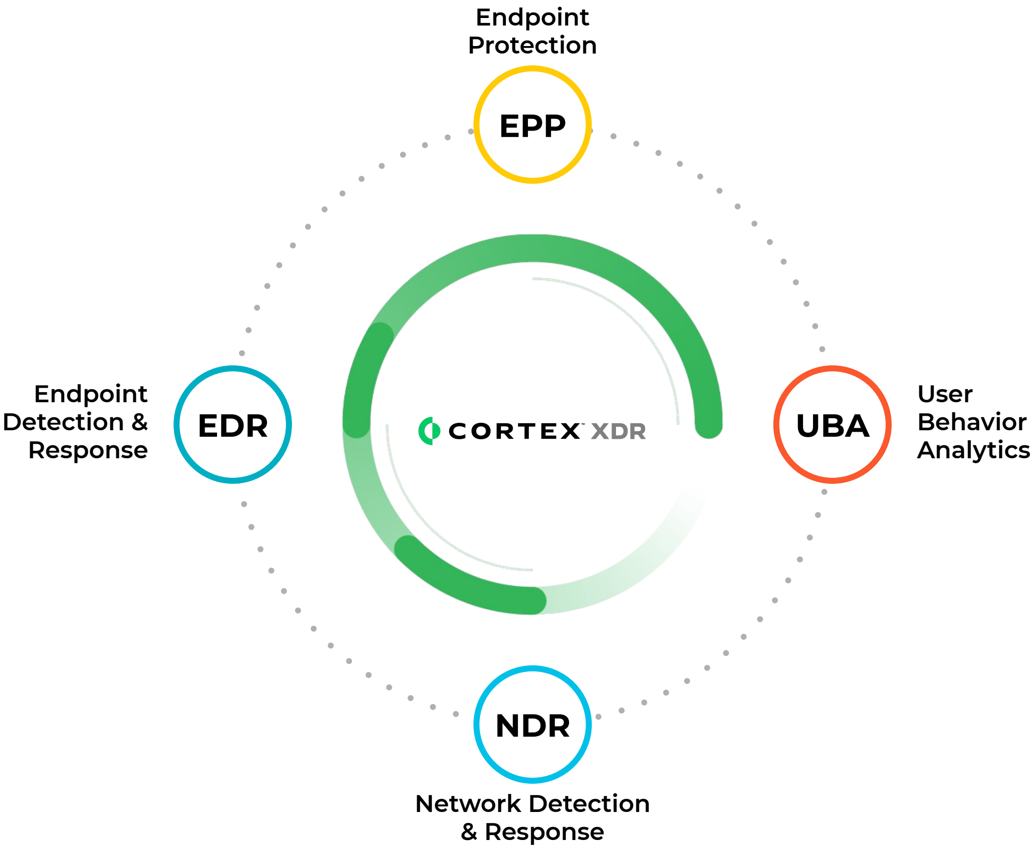
CORTEX XDR
BY PALO ALTO NETWORKS

Everything you can't prevent, detect and investigate fast

CORTEX XDR
BY PALO ALTO NETWORKS

Automate response and get smarter with every incident

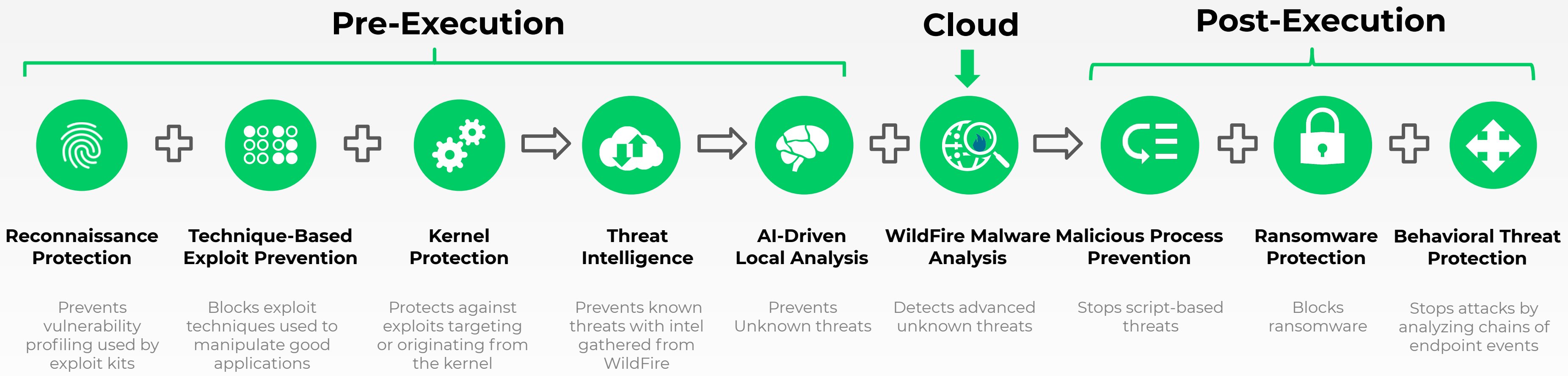
CORTEX XSOAR
BY PALO ALTO NETWORKS



Our Approach: Breaking down data and product silos

Prevention, Detection and Response Across Endpoint, Network & Cloud Data

Cortex XDR Agent Protection



Pre-Execution

Cloud

Post-Execution

Reconnaissance Protection

Prevents vulnerability profiling used by exploit kits

Technique-Based Exploit Prevention

Blocks exploit techniques used to manipulate good applications

Kernel Protection

Protects against exploits targeting or originating from the kernel

Threat Intelligence

Prevents known threats with intel gathered from WildFire

AI-Driven Local Analysis

Prevents Unknown threats

WildFire Malware Analysis

Detects advanced unknown threats

Malicious Process Prevention

Stops script-based threats

Ransomware Protection

Blocks ransomware

Behavioral Threat Protection

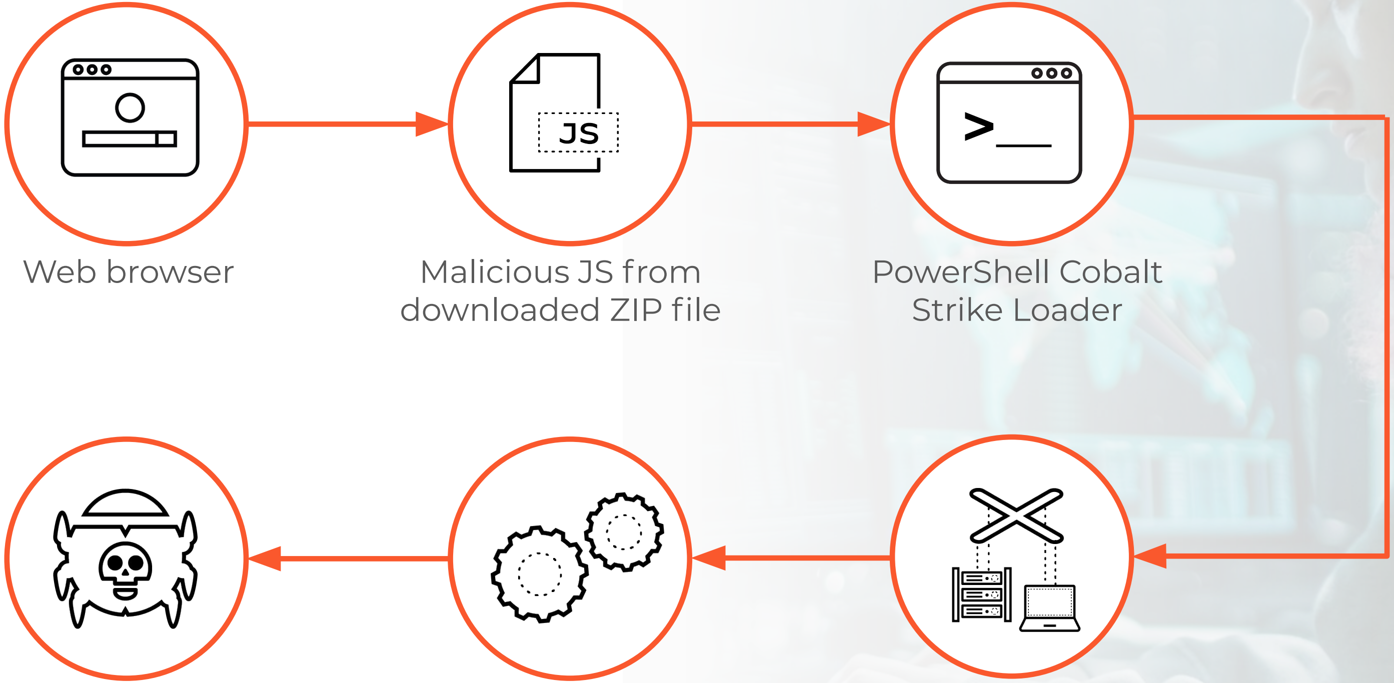
Stops attacks by analyzing chains of endpoint events

On and Offline Protection

Scheduled and On-Demand Scanning

Cross-Platform Protection (Win, MacOS, Linux)

WastedLocker Attack Lifecycle



Web browser

Malicious JS from downloaded ZIP file

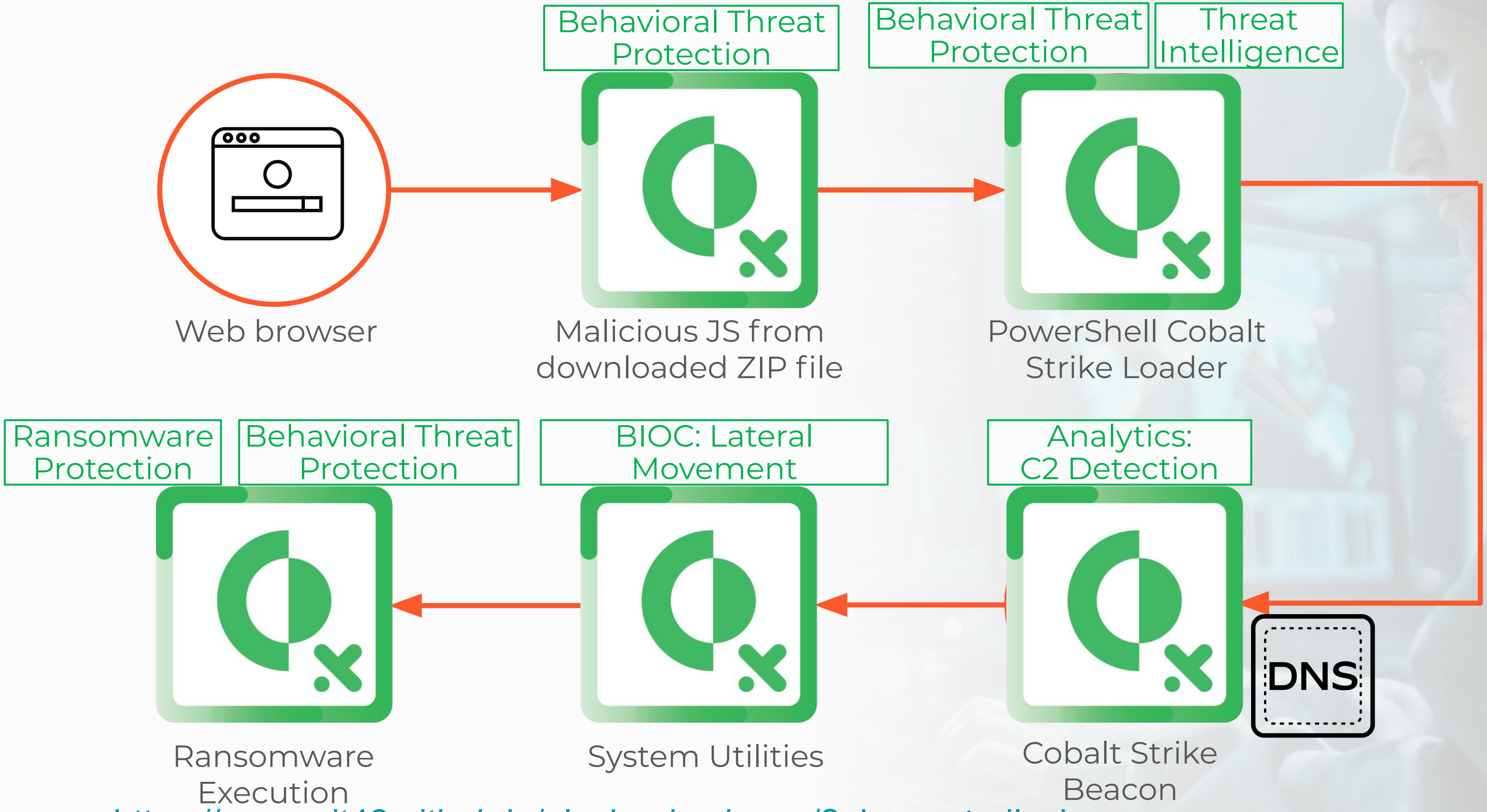
PowerShell Cobalt Strike Loader

Cobalt Strike Beacon

System Utilities

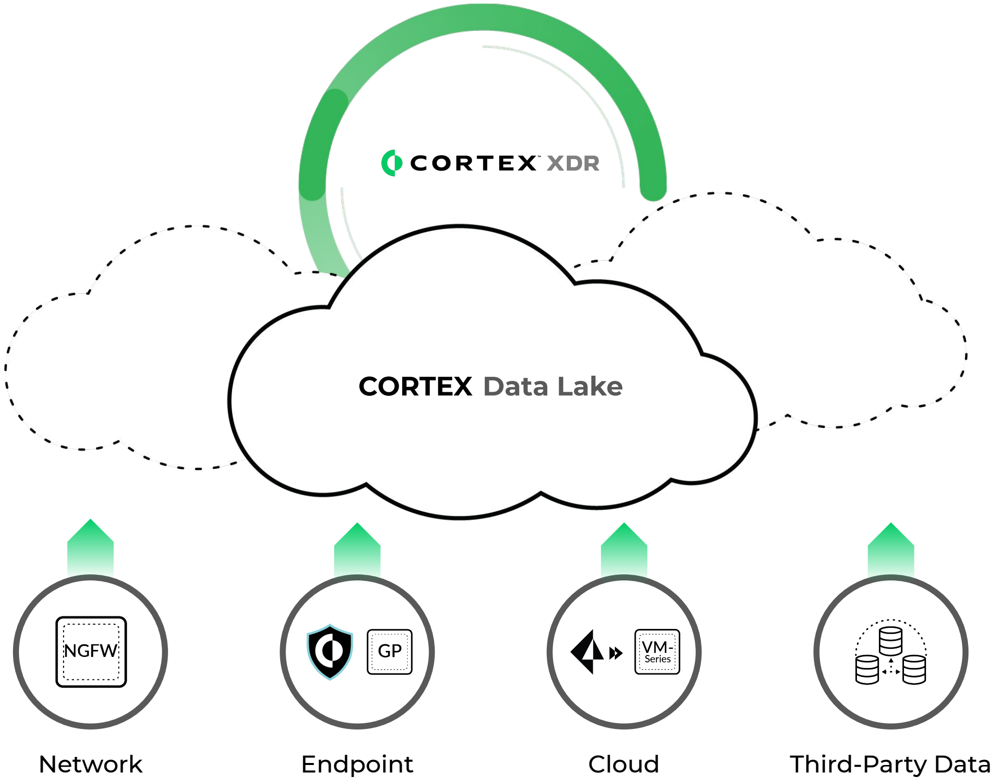
Ransomware Execution

Cortex XDR Stops WastedLocker at Every Step



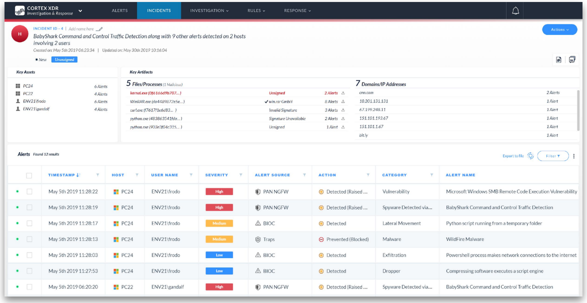
https://pan-unit42.github.io/playbook_viewer/?pb=wastedlocker-ransomware

Cortex XDR data sources for detection



Fortinet, Check Point, Cisco, Windows Events, OKTA, Azure AD, PingOne, GCP, AWS, LEEF, Filebeat, Kubernetes

Key differentiator: **supercharge investigation & response**



INCIDENT ID - 4 | Add name here

BabyShark Command and Control Traffic Detection along with 9 other alerts detected on 2 hosts involving 2 users

Created on: May 5th 2019 06:23:34 | Updated on: May 30th 2019 10:16:04

● New Unassigned

Key Assets

PC24	6 Alerts
PC22	4 Alerts
ENV21\frodo	6 Alerts
ENV21\gandalf	4 Alerts

Key Artifacts

5 Files/Processes (1 Malicious)

kernal.exe (0f6166d9b707...)	Unsigned	2 Alerts
WinRAR.exe (da4489872e5e...)	✓ win.rar GmbH	8 Alerts
curl.exe (f7617f1e6d83...)	Invalid Signature	3 Alerts
python.exe (483863541fda...)	Signature Unavailable	2 Alerts
python.exe (903e3f04c315...)	Unsigned	1 Alert

7 Domains/IP Addresses

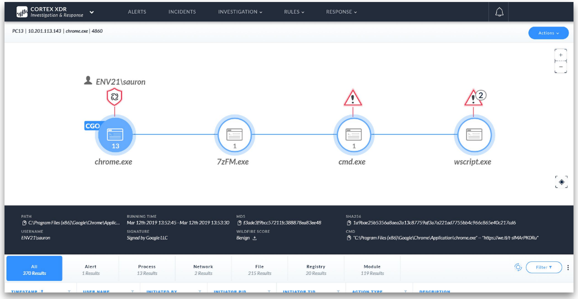
cnn.com	2 Alerts
10.201.131.131	1 Alert
67.199.248.11	1 Alert
151.101.193.67	1 Alert
151.101.1.67	1 Alert
bit.ly	1 Alert

Alerts Found 12 results

TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY	ALERT NAME
May 5th 2019 11:28:22	PC24	ENV21\frodo	High	PAN NGFW	Detected (Raised ...	Vulnerability	Microsoft Windows SMB Remote Code Execution Vulnerability
May 5th 2019 11:28:19	PC24	ENV21\frodo	High	PAN NGFW	Detected (Raised ...	Spyware Detected via...	BabyShark Command and Control Traffic Detection
May 5th 2019 11:28:17	PC24	ENV21\frodo	Medium	BIOC	Detected	Lateral Movement	Python script running from a temporary folder
May 5th 2019 11:28:13	PC24	ENV21\frodo	Medium	Traps	Prevented (Blocked)	Malware	WildFire Malware
May 5th 2019 11:28:03	PC24	ENV21\frodo	Low	BIOC	Detected	Exfiltration	Powershell process makes network connections to the internet
May 5th 2019 11:27:53	PC24	ENV21\frodo	Low	BIOC	Detected	Dropper	Compressing software executes a script engine
May 5th 2019 06:20:20	PC22	ENV21\gandalf	High	PAN NGFW	Detected (Raised ...	Spyware Detected via...	BabyShark Command and Control Traffic Detection

Unified Incident Engine

Intelligently group related alerts into one incident



PC13 | 10.201.113.143 | chrome.exe | 4860

PATH
C:\Program Files (x86)\Google\Chrome\Applic...

RUNNING TIME
Mar 12th 2019 13:52:45 - Mar 12th 2019 13:53:30

MD5
f3ade3f9bcc57211fc388878ea83ee48

SHA256
1a9bae25b5356a8aea2a13c87759af3a7a221ad7755bb4c966c865e40c217cd6

USERNAME
ENV21\sauron

SIGNATURE
Signed by Google LLC

WILDFIRE SCORE
Benign

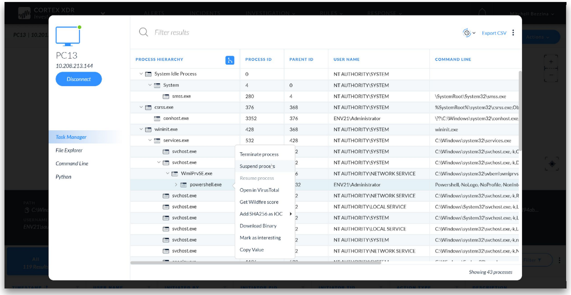
CMD
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -- "https://we.tl/t-sIMArPK0Ru"

All	Alert	Process	Network	File	Registry	Module
370 Results	1 Results	13 Results	2 Results	215 Results	20 Results	119 Results

TIMESTAMP | USER NAME | INITIATED BY | INITIATOR PID | INITIATOR TID | ACTION TYPE | DESCRIPTION

Automated Root Cause Analysis

Reveal the root cause of attacks in one click



PC13
10.208.213.144

PROCESS HIERARCHY	PROCESS ID	PARENT ID	USER NAME	COMMAND LINE
System Idle Process	0		NT AUTHORITY\SYSTEM	
System	4	0	NT AUTHORITY\SYSTEM	
smss.exe	280	4	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
csrss.exe	376	368	NT AUTHORITY\SYSTEM	%SystemRoot%\system32\csrss.exe,Ob
conhost.exe	3352	376	ENV21\Administrator	\??\C:\Windows\system32\conhost.exe
wininit.exe	428	368	NT AUTHORITY\SYSTEM	wininit.exe
services.exe	532	428	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
svchost.exe		2	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,C
svchost.exe		2	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,D
WmiPrvSE.exe		6	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvs
powershell.exe		32	ENV21\Administrator	Powershell,-NoLogo,-NoProfile,-NonInt
svchost.exe		2	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe,-k,R
svchost.exe		2	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe,-k,L
svchost.exe		2	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe,-k,L
svchost.exe		2	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe,-k,L
svchost.exe		2	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe,-k,n
svchost.exe		2	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe,-k,N

Showing 43 processes

Integrated Response

Quick actions to contain attacks, isolate hosts or run custom forensics

Summary

NGFW

Prevent unknown threats faster with Wildfire inline ML and SSL decryption

Cortex XDR Agent

Prevent advanced attacks and ransomware

Cortex XDR Pro

Speed up investigation and response by combining endpoint and network data

Thank You

Mikkel Bossen | Channel SE

May 2021