

Extending Zero Trust from Network to the Endpoint

Jani Haapio

jhaapio@paloaltonetworks.com

Channel SE

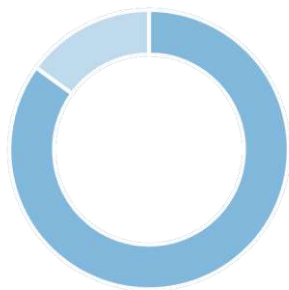
ZERO TRUST

 paloalto
NETWORKS®

The world's leading cybersecurity company

85

of Fortune 100
rely on Palo Alto Networks

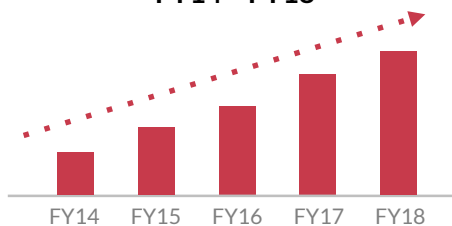


63% of the Global 2K
are Palo Alto Networks customers

#1

in enterprise
security

Revenue trend 40% CAGR
FY14 – FY18



28% year over year
revenue growth*

60,000+

customers
in 150+ countries



tsia
RATED
OUTSTANDING
ASSISTED SUPPORT
GLOBAL | PALO ALTO NETWORKS

9.1/10
average CSAT score

Q4FY2018. Fiscal year ends July 31

Gartner, Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 1Q18, 14 June 2018



Securing Your Transformed Enterprise



Hybrid data center

Internet Perimeter

Branch & mobile

5G & IoT

Endpoint

SECURE
THE ENTERPRISE



SECURE
THE CLOUD



Secure access

SaaS

Public cloud

DATA LAKE



SECURE
THE FUTURE



Detection &
response

Automation &
orchestration

Network traffic &
behavioral analytics

Threat
intelligence



We Are a Leader Among ZTX Ecosystem Providers

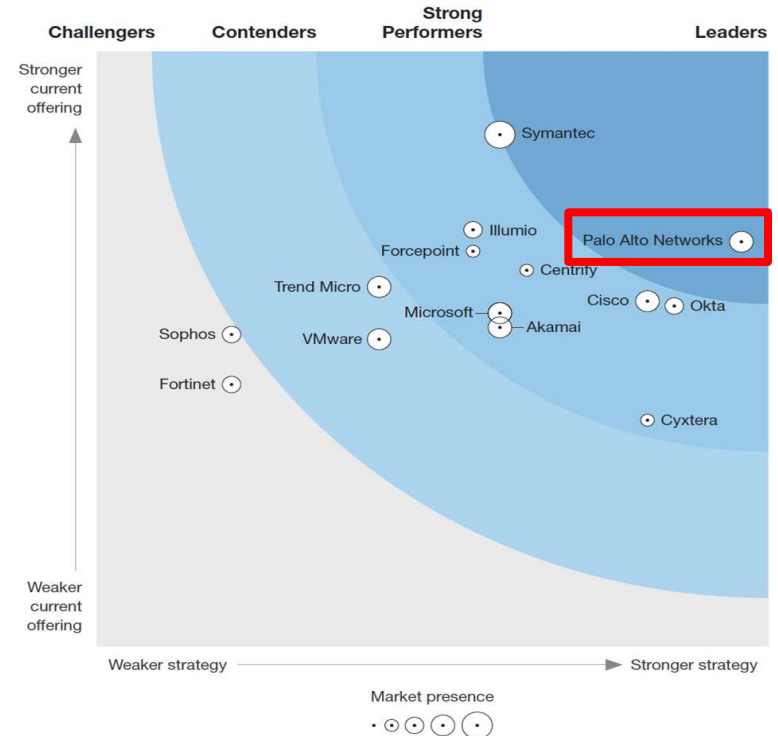
We received the highest score in the strategy category

Our position validates the Security Operating Platform as an integrated platform that customers can use to implement Zero Trust and prevent successful cyberattacks

THE FORRESTER WAVE™

Zero Trust eXtended (ZTX) Ecosystem Providers

Q4 2018

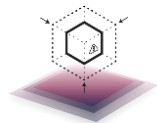


TRUST IS A DANGEROUS VULNERABILITY

THAT IS **EXPLOITED** BY MALICIOUS ACTORS

“An integrated platform approach that combines endpoint and network security is the only way to achieve holistic protection and implement the Zero Trust model across your entire security architecture.”

5 Steps to Deploying Zero Trust



1. Define your Protect Surface



Next-Generation Firewall



Cortex™ Data Lake



Cortex™ XDR



Transformation Services



2. Map the transaction flows



Next-Generation Firewall



Cortex™ Data Lake



Cortex™ XDR



Traps



Transformation Services



3. Build a Zero Trust architecture



Next-Generation Firewall



Cortex™ Data Lake



Cortex™ XDR



Traps



GlobalProtect



Prisma Access



Transformation Services



4. Create Zero Trust Policy



Panorama



WildFire



Threat Prevention



URL Filtering



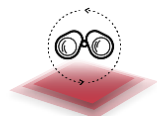
DNS Service



Prisma SaaS



Transformation Services



5. Monitor and maintain the network



Cortex™ Data Lake



Cortex™ XDR



AutoFocus



MineMeld



Demisto



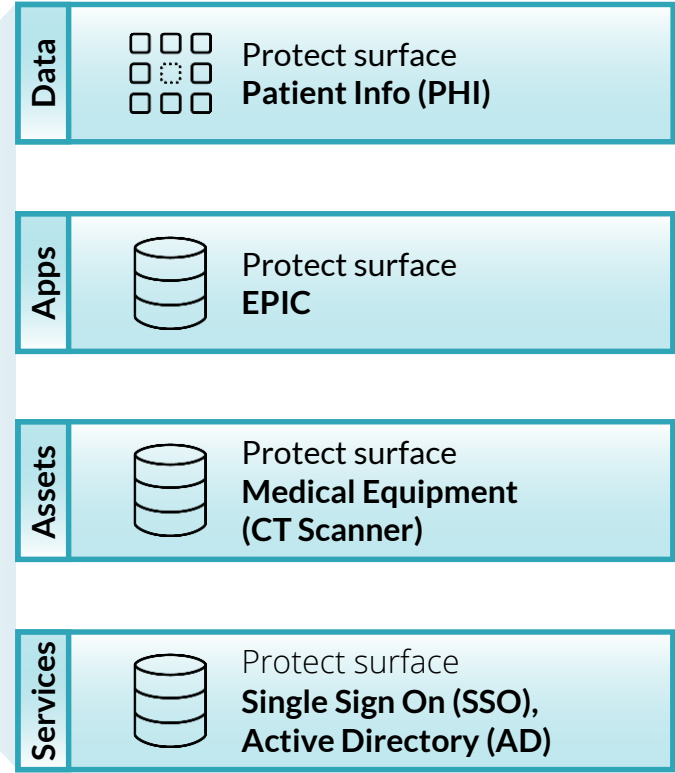
Prisma Cloud



Transformation Services

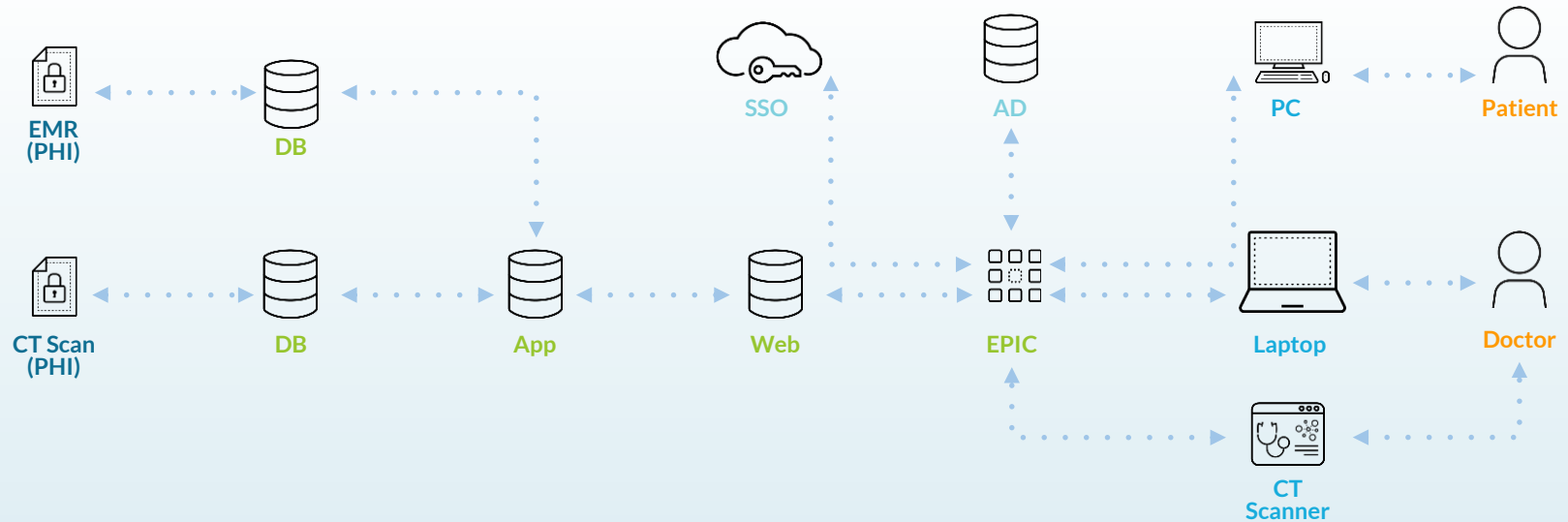
Step 1: Define Your Protect Surface

- Identify where the protect surface exists
- Discover and classify data, applications, assets, & services (DAAS)
- Gain visibility and contextual awareness
 - Application awareness
 - User identification
 - SSL decryption
 - Files and data fingerprinting



Step 2: Map the Transaction Flows

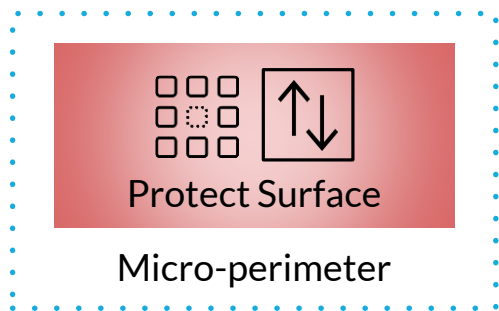
- Use automated tools for data mapping across all types of traffic
- Understand how data, applications, systems, and networks interact
- Catalog all traffic and summarize findings



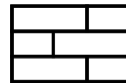
Step 3: Architect a Zero Trust Network

- Connect a protect surface to a Segmentation Gateway to define a micro perimeter in policy
- Use centralized management for unified and consistent Zero Trust policy
- Deploy physical, virtual and/or cloud-based NGFW as Segmentation Gateways
- Minimize bottlenecks with scalable security performance

Why you're segmenting?
Define the protect surface



Policy



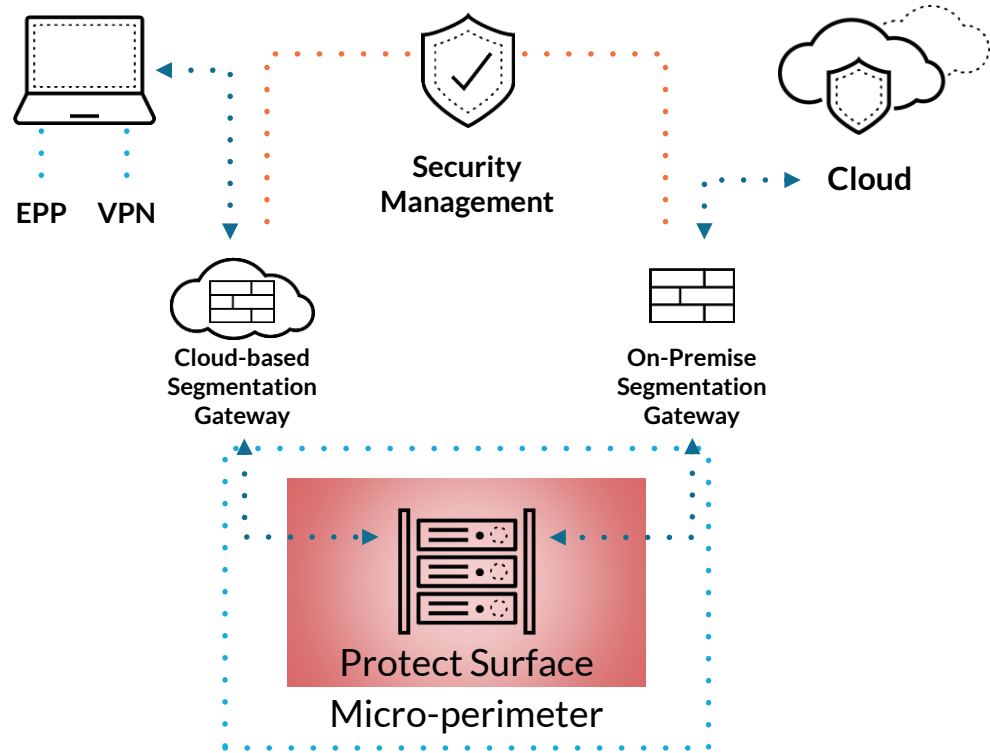
Segmentation
Gateway

**How you enforce
segmentation?**
Across layer 2-7

Policy Manager

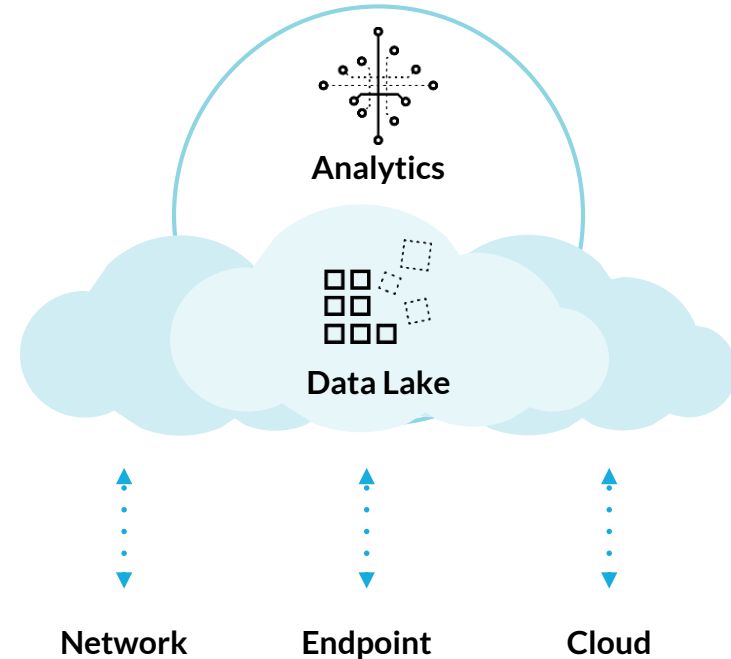
Step 4: Create a Trust Policy

- Create and automate application rules based on best practices
- Scan and mitigate threats with multilayered security

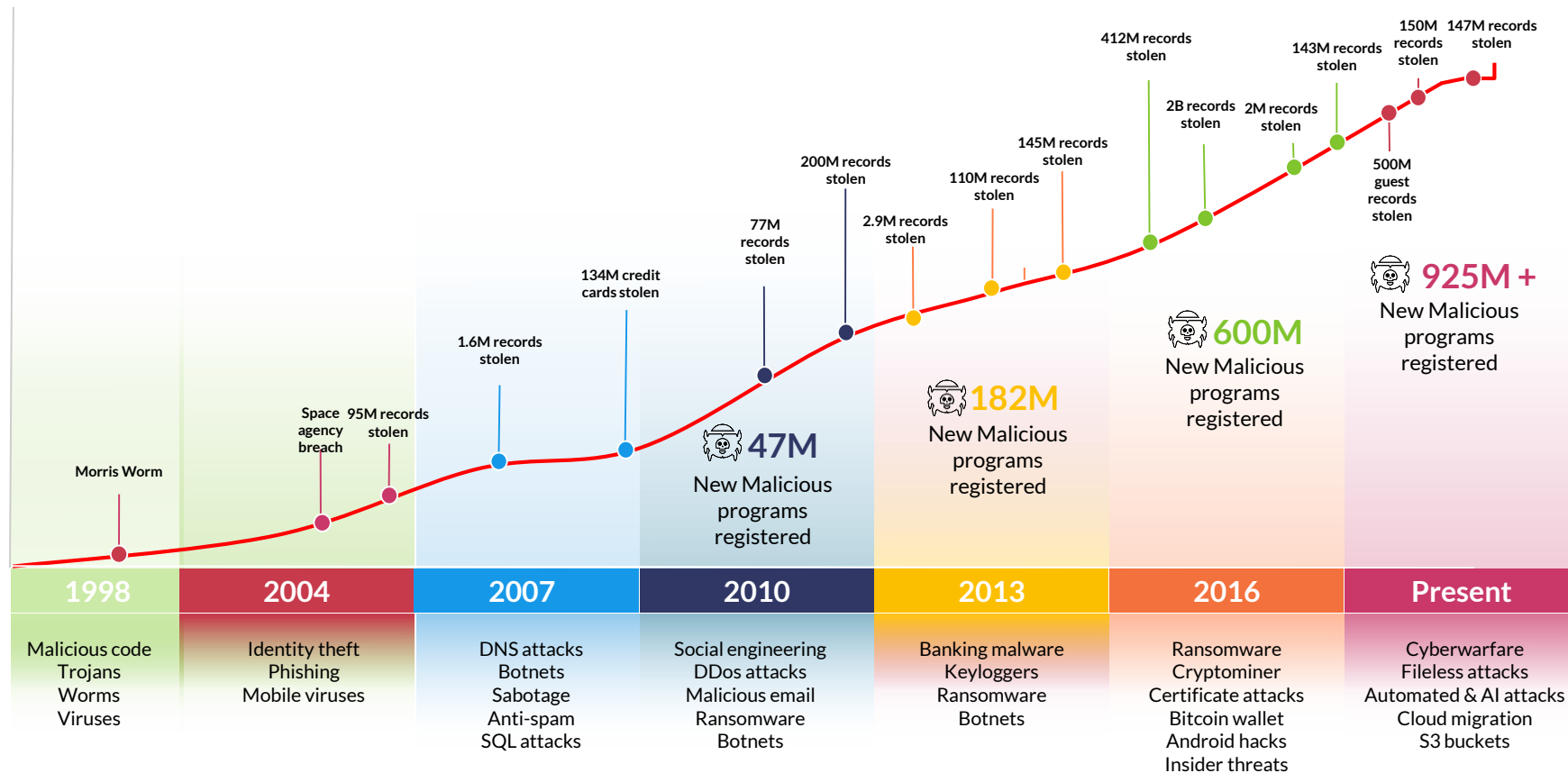


Step 5: Monitor and Maintain Your Environment with SecOps

- Continuously monitor, enhance, and evolve your environment
- Use machine learning to quickly identify and respond to threats, and high priority alerts across the network, endpoint, and cloud



As threats escalate, SecOps is more important than ever



Why security teams struggle



Gaps in Prevention

Legacy tools generate too many alerts

174k
alerts per week



Lack of Time

Manual tasks across siloed tools take too long

30+
point products

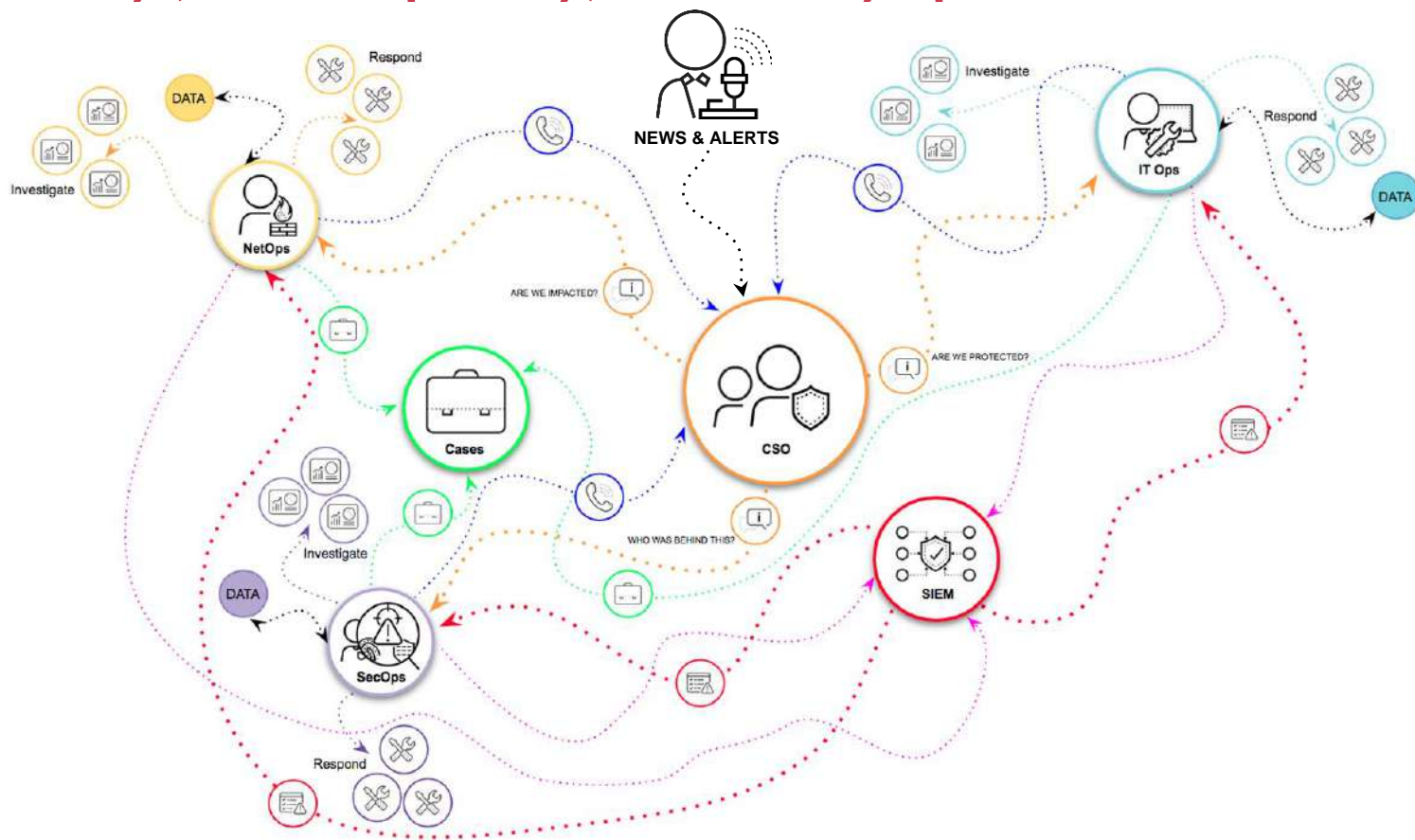


Limited Context

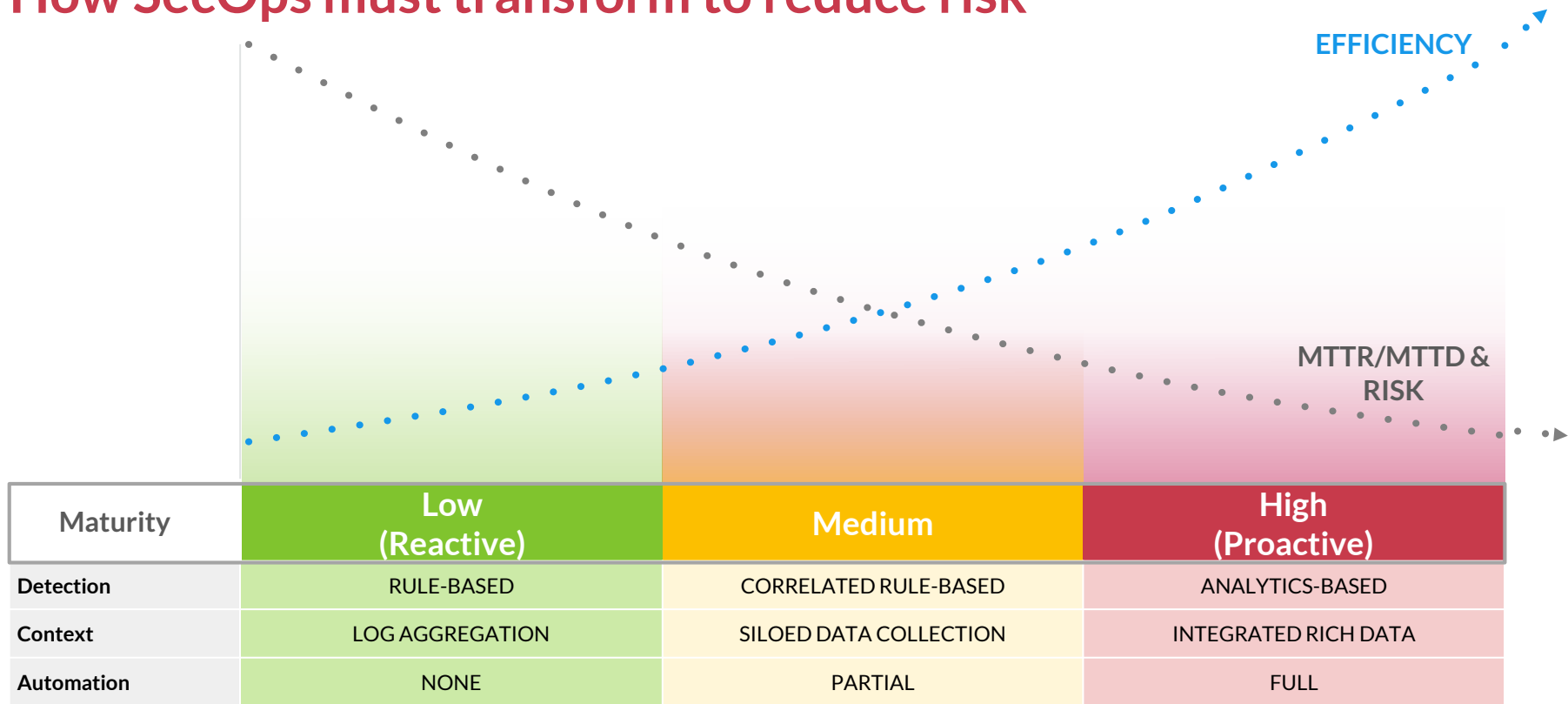
It takes days to investigate threats

4+ days
to complete an investigation

The reality (and complexity) of security operations



How SecOps must transform to reduce risk



Reinventing SecOps with Cortex



Prevent everything
you can

**Traps & Next-Generation
Firewall**



Everything you can't
prevent, detection
and investigate fast

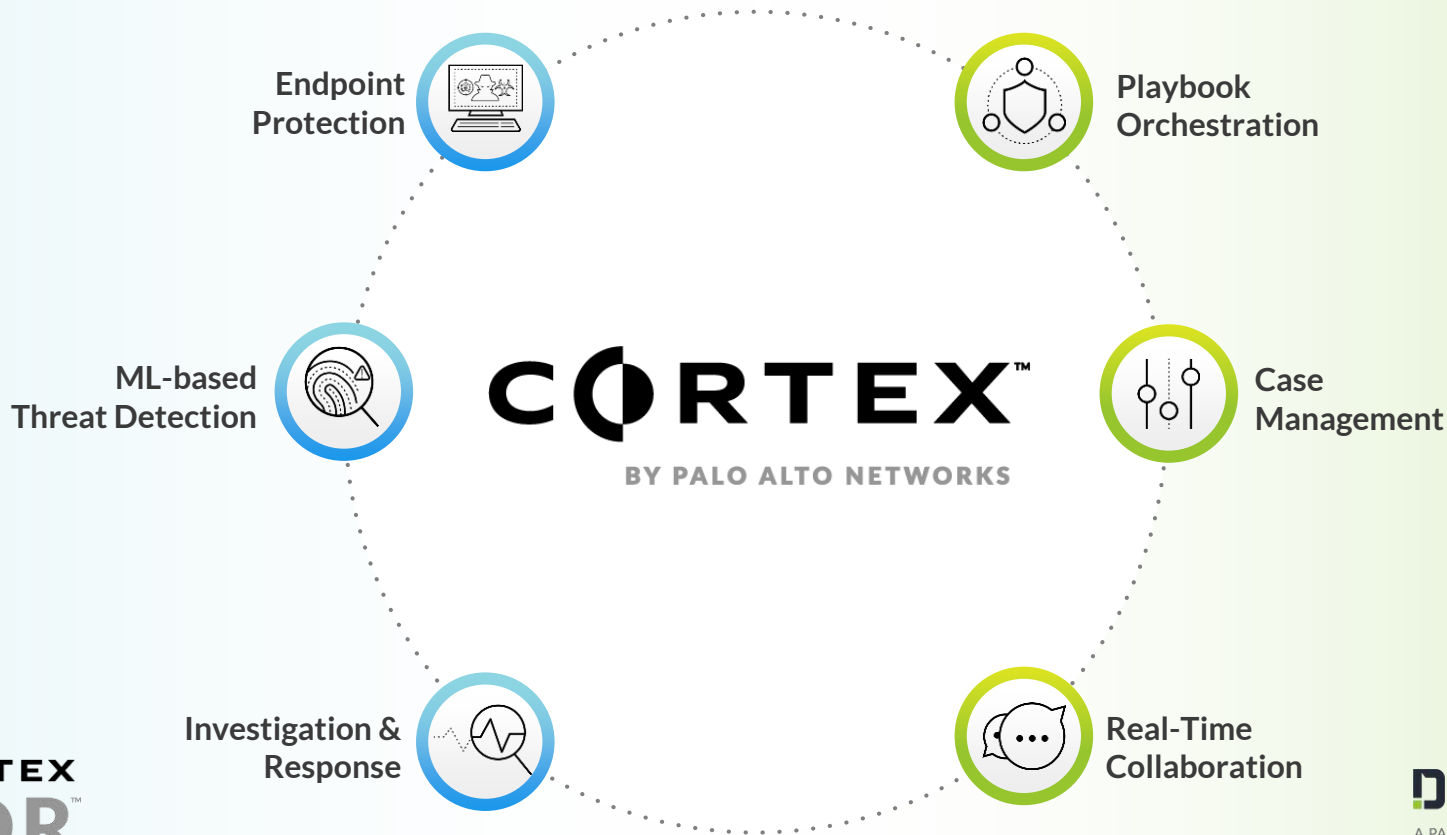
**Cortex XDR
& Autofocus**



Automate response
and get smarter with
each incident

Demisto

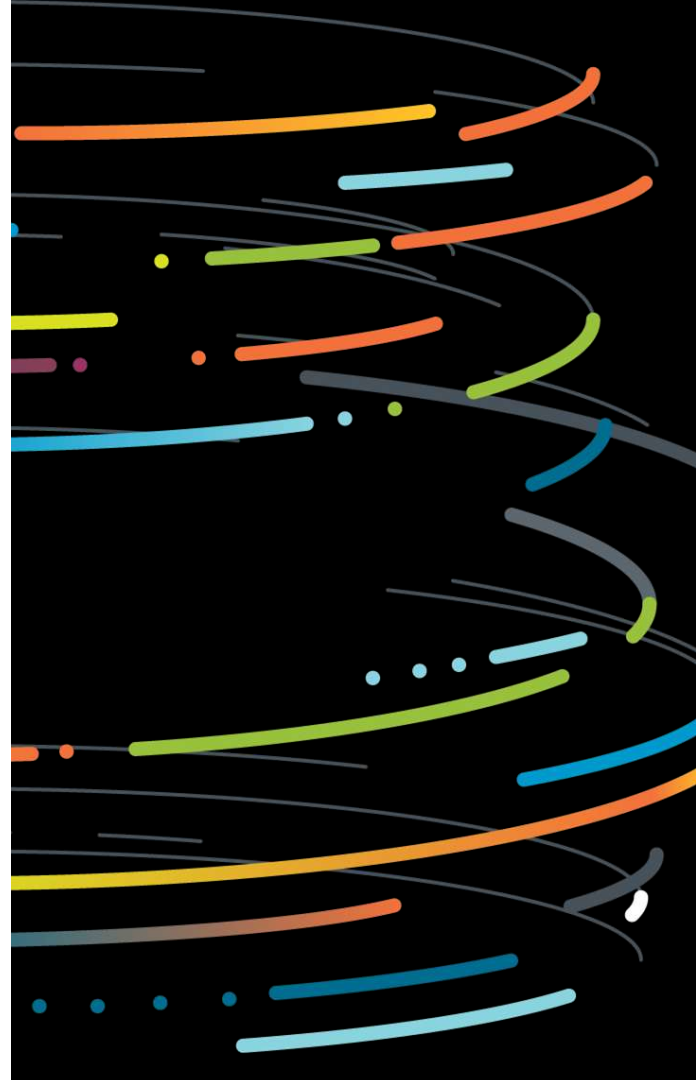
Reinventing SecOps with Cortex



CORTEX
XDR™

DEMISTO
A PALO ALTO NETWORKS® COMPANY

Use Case: Endpoint Protection



The Problem: Endpoint infections continue despite best efforts



Legacy Endpoint Security Has Failed

Legacy EPPs can't keep up with advanced threats and burden local systems



Siloed Network & Endpoint Protection

Current approaches do not share protections between different parts of the enterprise

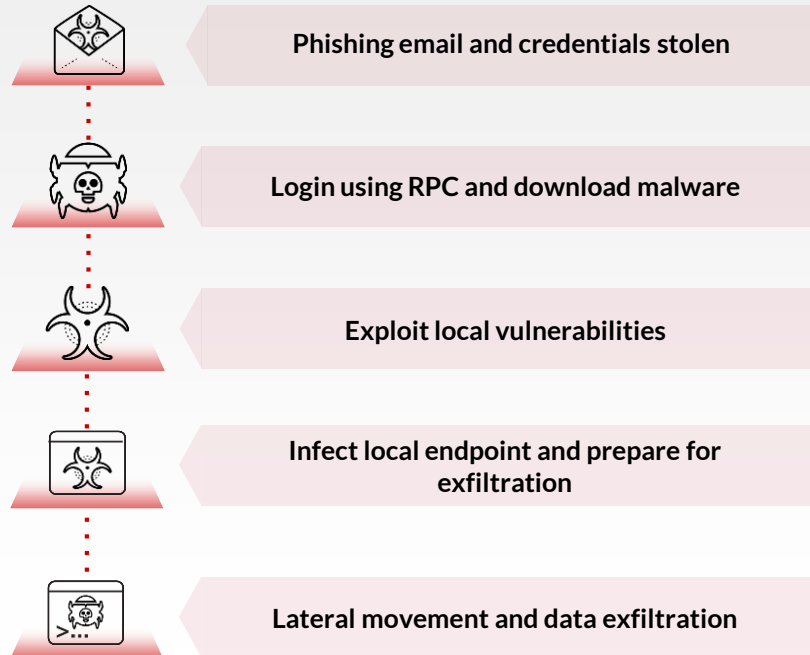


Endpoint Detection & Response is Limited

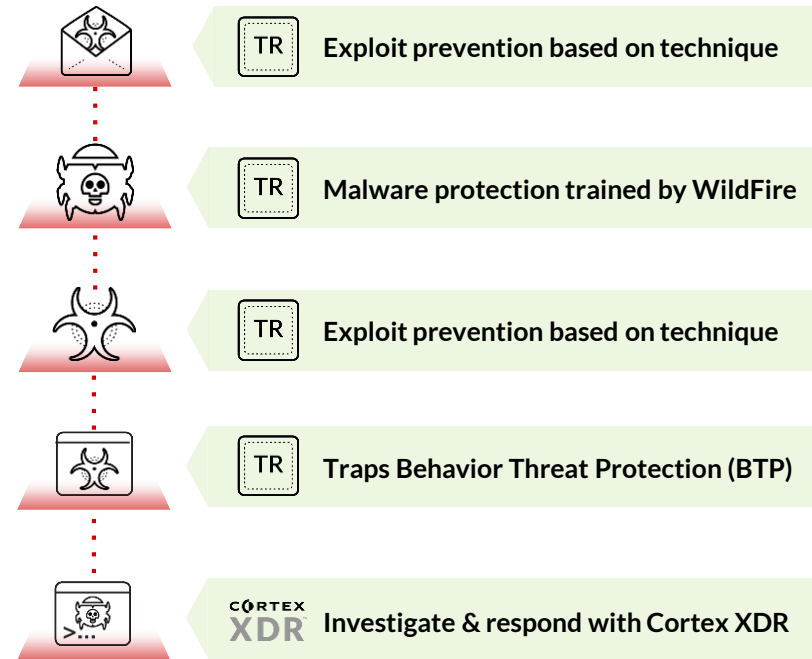
EDR is locked to the endpoint and lacks a solution for unmanaged devices

Our Approach: Endpoint protection

Before



After



Sample Traps Security Event (BTP)

Endpoint behaviors that triggered the rule.

Can you determine the root cause:

1. Drive by download?
2. USB installation?
3. Phishing?

The screenshot displays the 'Behavioral Threat' interface in Cortex XDR. The top bar shows 'Behavioral Threat' with a 'New' status and an 'Analyze in Cortex XDR' button. Below the bar are tabs for 'Details', 'Analysis', 'Exception', 'Comments', and 'History'. The main content area is titled 'Observed Behaviors for Rule: heuristic.b.virlock_simulation'. It lists a series of events with timestamps and descriptions of behaviors triggered by 'wscript.exe' and 'CGO'.

Timestamp	Behavior	Process	Source
18:33:31 23 Jul, 2019	Launched cscript.exe or wscript.exe	wscript.exe	CGO
18:33:34	Created a script file	wscript.exe	CGO
18:33:34	Modified the Windows File System to enable auto-start	wscript.exe	CGO
18:33:34	Created an executable file in a user folder	wscript.exe	CGO
18:33:34	Process created or set a hidden file	wscript.exe	CGO
18:33:34	Process created or set a hidden executable file	wscript.exe	CGO
18:33:35	Launched reg.exe or regedit.exe	reg.exe	
18:33:35	Launched mshta.exe	mshta.exe	
18:33:35	Launched PowerShell.exe	powershell.exe	

Best-in-class prevention with Traps



Prevent all malware

High fidelity local detection
trained by WildFire



Block exploits

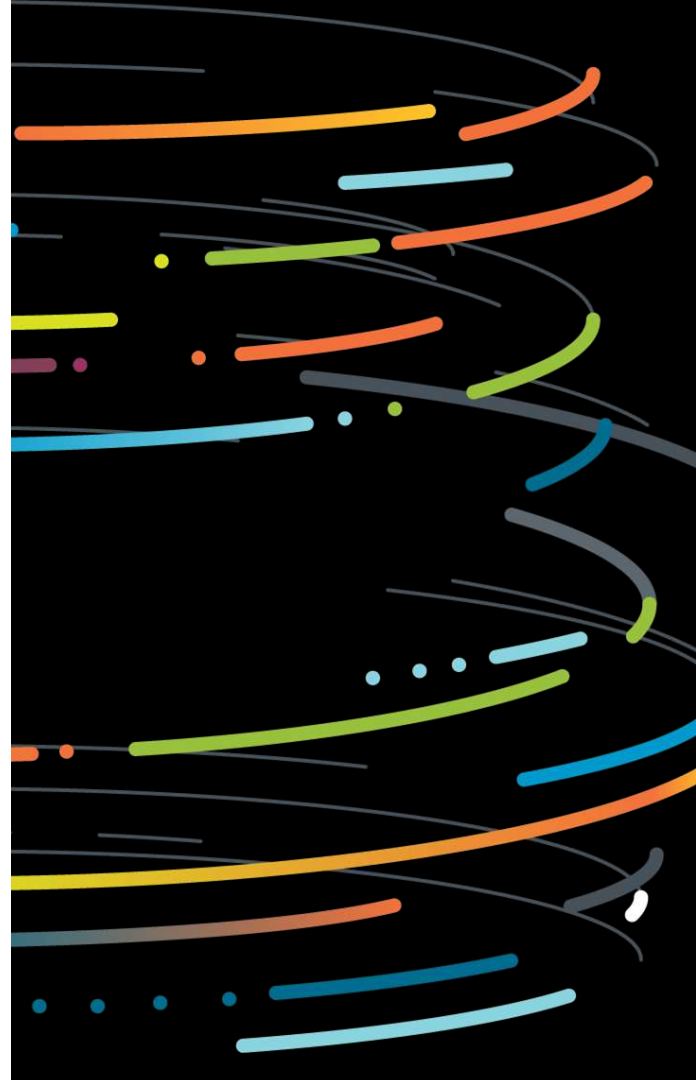
Block exploits based
on techniques



Analyze suspicious patterns

Behavioral Threat Protection
analyzes multiple behaviors
together to flag complex
attacks

Use Case: Threat Detection with Investigation & Response



The Problem: Too many false positives and missed attacks



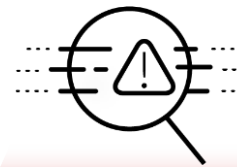
**You Can't Prevent
All Attacks**

Sophisticated attacks
& insider abuse can bypass
controls



**Detection Yields Too
Many False Positives**

Teams waste time and miss
threats chasing low-context
false positive alerts

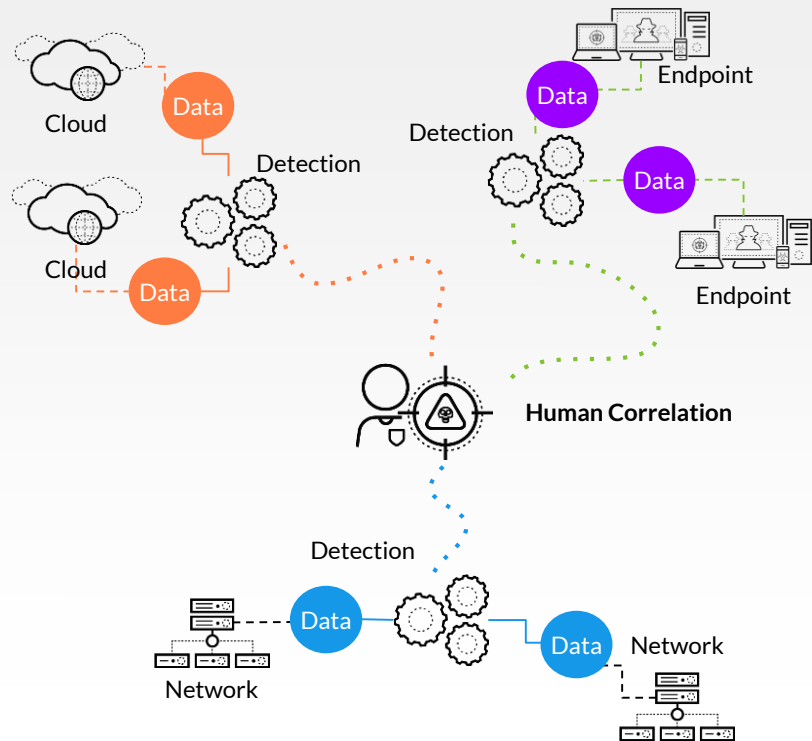


**Anomaly Detection is
not a "Human" Job**

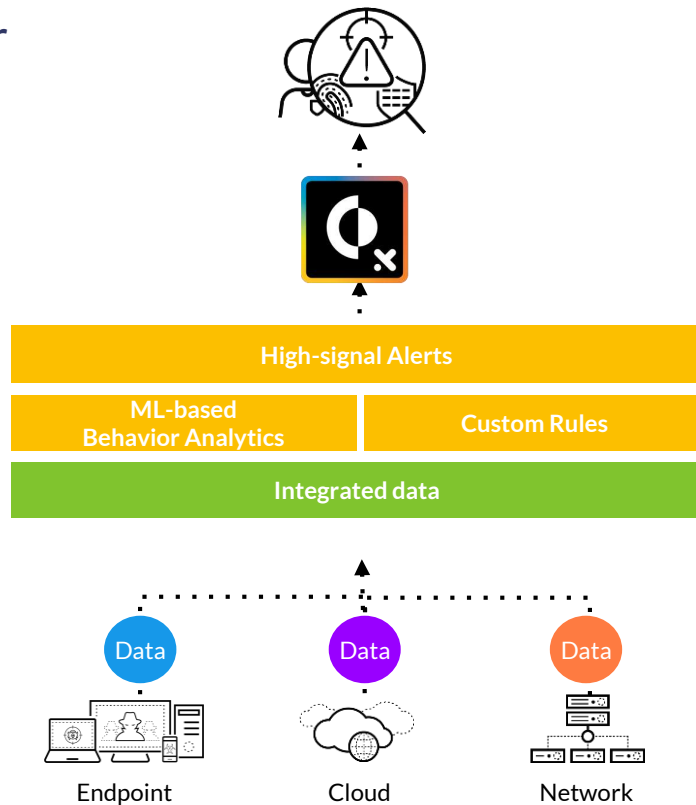
Detecting anomalies requires
analyzing a comprehensive
data set

Our Approach: Threat detection

Before



After



The Problem: Threat containment takes too long



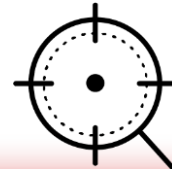
Limited Context Across Multiple Alerts

Analysts have to review each alert individually



Investigations Are Highly Manual

Teams must manually piece together data from siloed tools & data sources

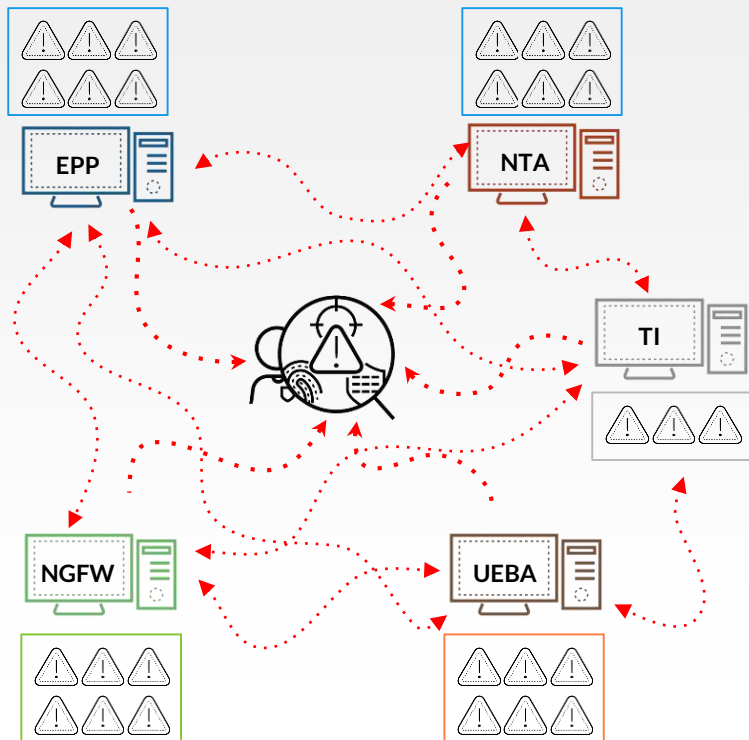


Finding Root Cause Takes Too Long

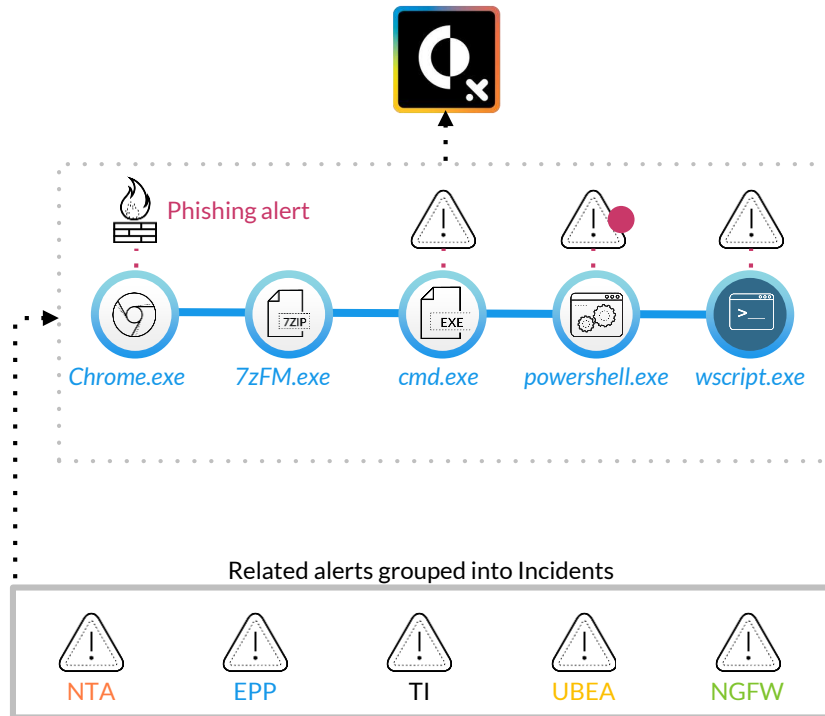
By the time you find root cause, the attack has progressed

Our Approach: Investigation & response

Before



After



Stitching of Network (NGFW Logs) and Endpoint Data (Traps Logs)



CORTEX XDR
Investigation & Response

ALERTS

INCIDENTS

INVESTIGATION

RULES

RESPONSE



Jani Haapio



INCIDENT ID - 4 | Add name here

'BabyShark Command and Control Traffic Detection' along with 9 other alerts generated by Traps, PAN NGFW, IOC and BIOC detected on 2 hosts

Created on: May 5th 2019 16:23:34 | Updated on: Sep 4th 2019 17:42:27

Under Investigation

Michael Wood

Actions

Key Artifacts

NAME	DESCRIPTION	SIGNATURE	THREAT INTELLIGENCE
kernal.exe (0f6166d9b707f861...	Process involved in 2 Alerts	Unsigned	WF Malware VT 32/63
WinRAR.exe (da4489872e5eccd9...	Process involved in 8 Alerts	win.rar GmbH	WF Benign VT 0/69
curl.exe (f7617f1e6d8300769c45...	Process involved in 3 Alerts	Invalid	WF Benign VT 0/70
cmd.exe (db06c3534964e3fc79d2...	Process involved in 3 Alerts	Unavailable	WF Benign VT 0/68

Key Assets

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

Alerts
12 Results

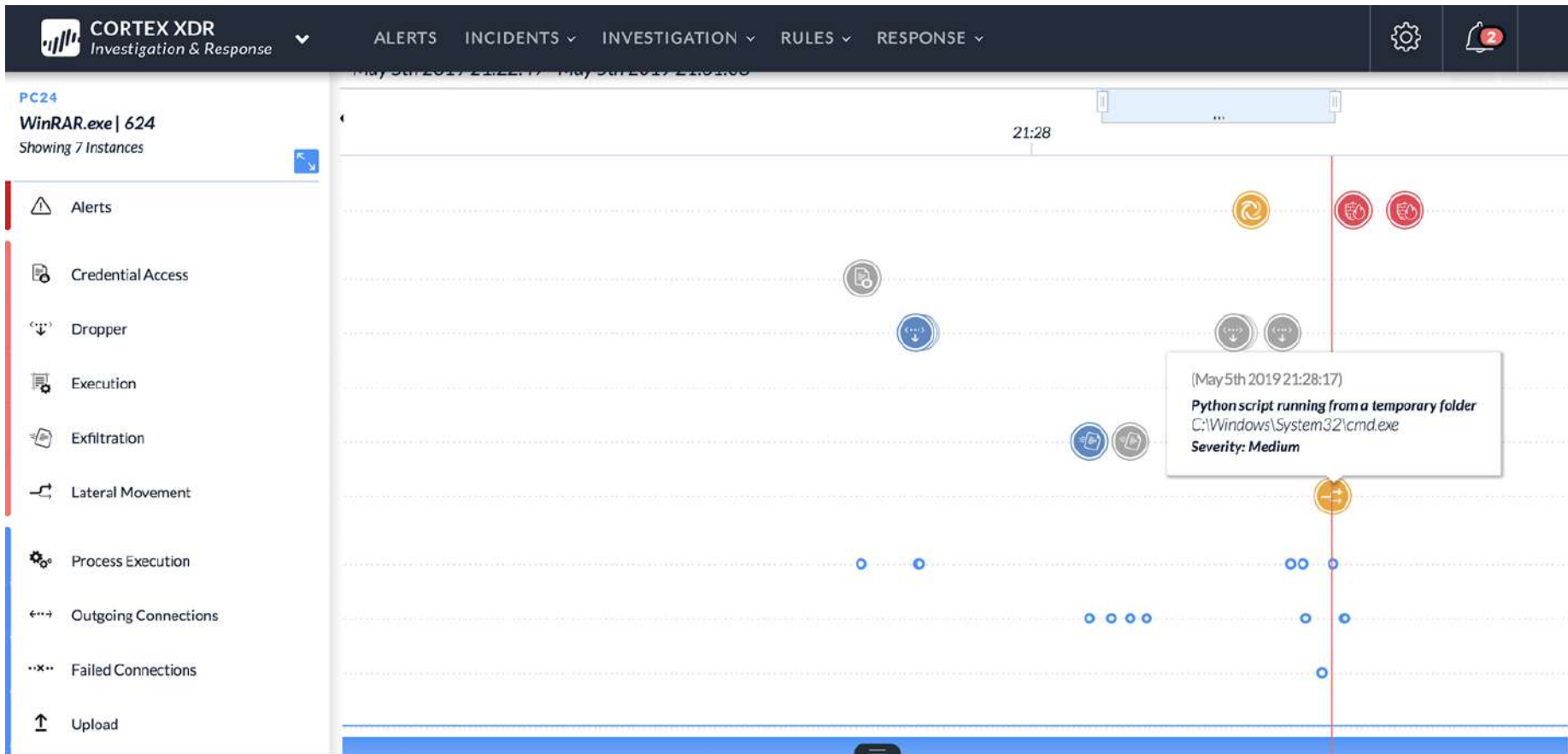
Insights
27 Results

Export to file

Filter

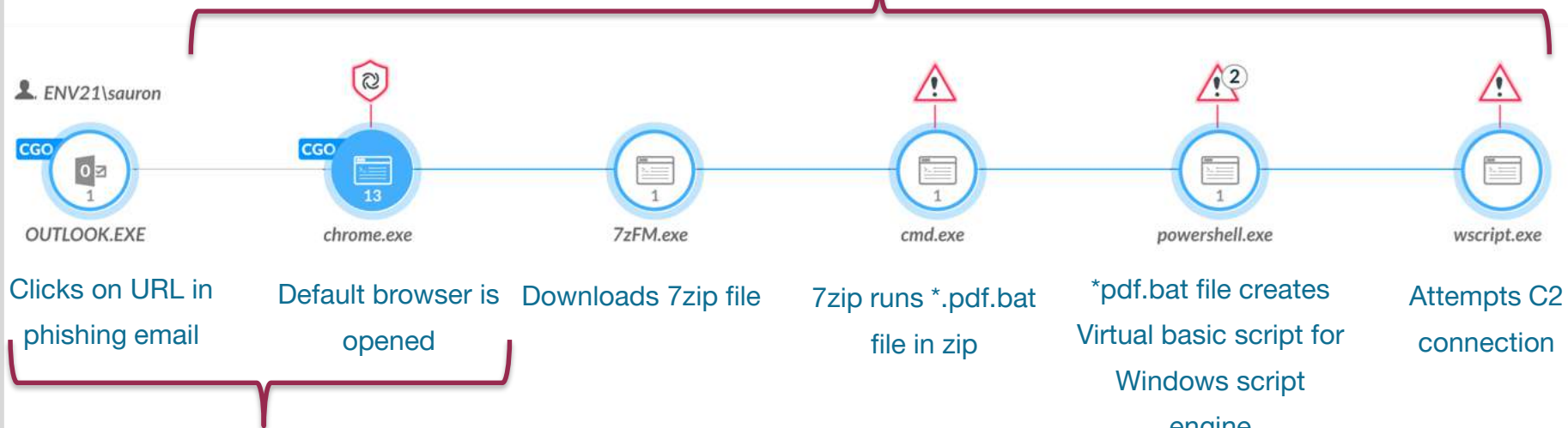
	HOST	USER NAME	SEVERI...	ALERT S...	ACTION	CATEGORY	ALERT NAME
	PC24	ENV21\frodo	High	PAN NGFW	Detected (Raised An Alert)	Vulnerability	Microsoft Windows SMB Remote Code Execution Vulnerability
	PC24	ENV21\frodo	High	PAN NGFW	Detected (Raised An Alert)	Spyware Detected via Anti...	BabyShark Command and Control Traffic Detection
	PC24	ENV21\frodo	Medium	BIOC	Detected	Lateral Movement	Python script running from a temporary folder
	PC24	ENV21\frodo	Medium	Traps	Prevented (Blocked)	Malware	WildFire Malware
	PC24	ENV21\frodo	Low	BIOC	Detected	Exfiltration	Powershell process makes network connections to the internet
	PC24	ENV21\frodo	Low	BIOC	Detected	Dropper	Compressing software executes a script engine
	PC22	ENV21\gandalf	High	PAN NGFW	Detected (Raised An Alert)	Spyware Detected via Anti...	BabyShark Command and Control Traffic Detection

Investigate in timeline



Determining Root Cause of Security Events

Causality Group: All processes, files, and threads involved as a part of the security event



Causality Group Owner (CGO): The process that initiated the chain of events

Integrated response via live terminal

PC13
10.208.213.144
[Disconnect](#)

Task Manager

File Explorer
Command Line
Python

Filter results [Export CSV](#)

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
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, kC
svchost.exe		2	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe, kC
WmiPrivSE.exe		6	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\wbem\wmiprivs
powershell.exe		32	ENV21\Administrator	Powershell, NoLogo, NoProfile, NonInb
svchost.exe		2	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe, kR
svchost.exe		2	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe, kL
svchost.exe		2	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe, kL
svchost.exe		2	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe, kL
svchost.exe		2	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe, kn
svchost.exe		2	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe, kN

- Terminate process
- Suspend process
- Resume process
- Open in VirusTotal
- Get Wildfire score
- Add SHA256 as IOC
- Download Binary
- Mark as interesting
- Copy Value

Showing 43 processes

Key Differentiators: Find advanced attacks with analytics



Full Visibility To Detect Complex Threats

Eliminate blind spots across network, endpoint, and cloud



Industry-leading Attack Coverage

Detect the most attack techniques according to MITRE ATT&CK evaluations

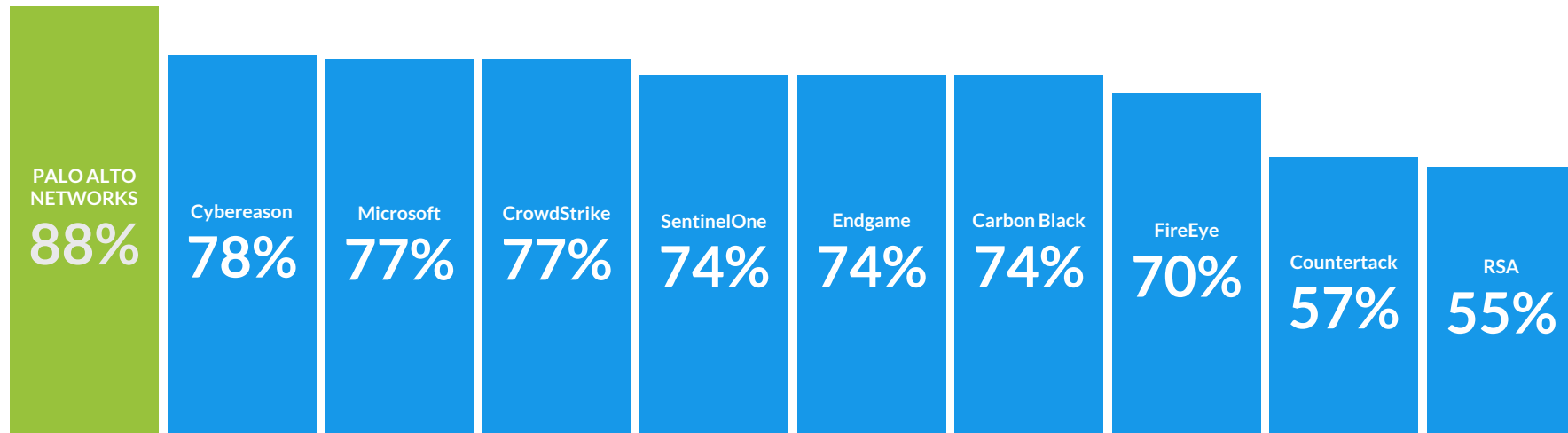


Patented Behavioral Analytics Technology

Find hidden threats with Machine Learning running across all data

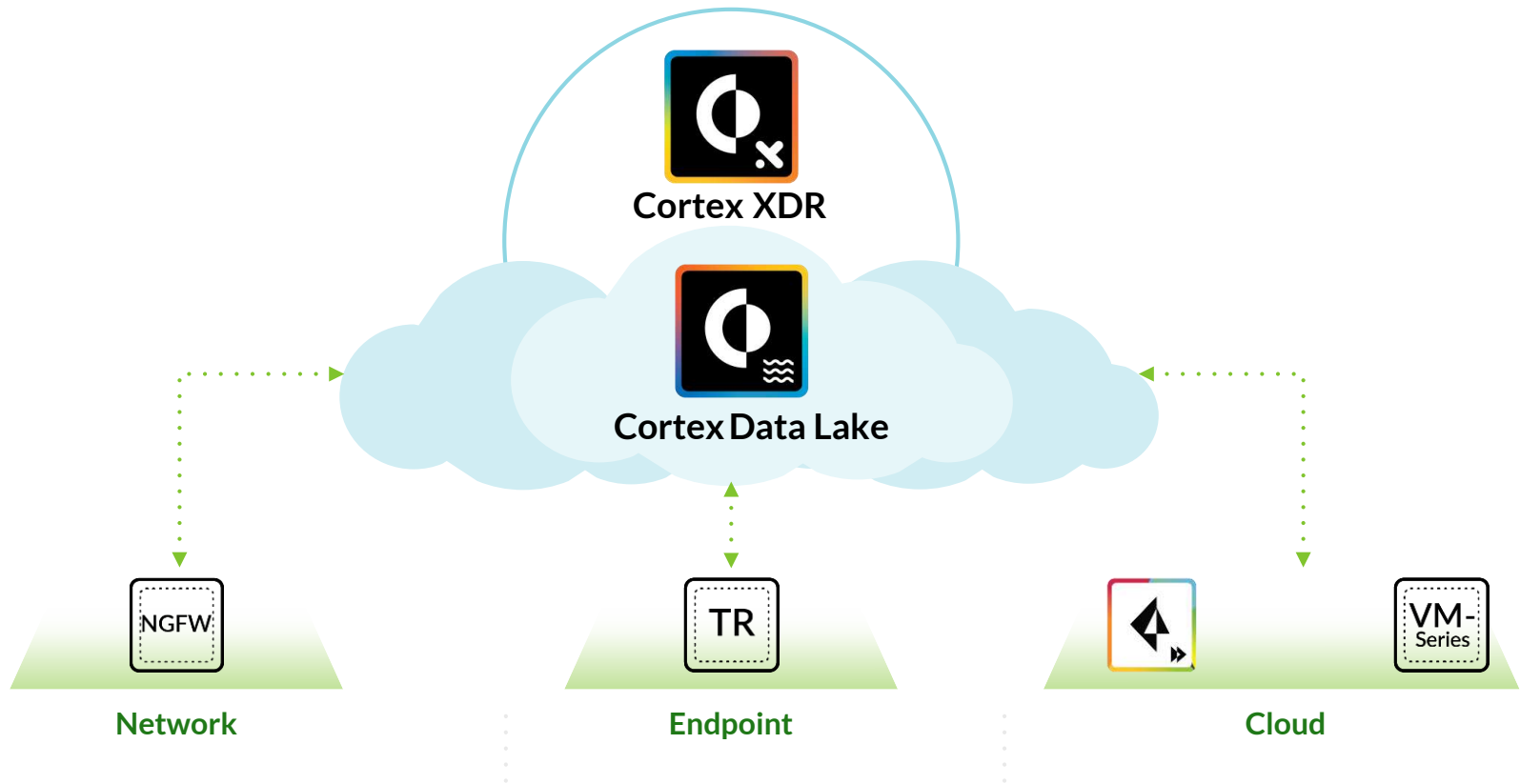
Cortex XDR achieves best MITRE ATT&CK coverage

Scored higher than all
other vendors with
93% fewer misses

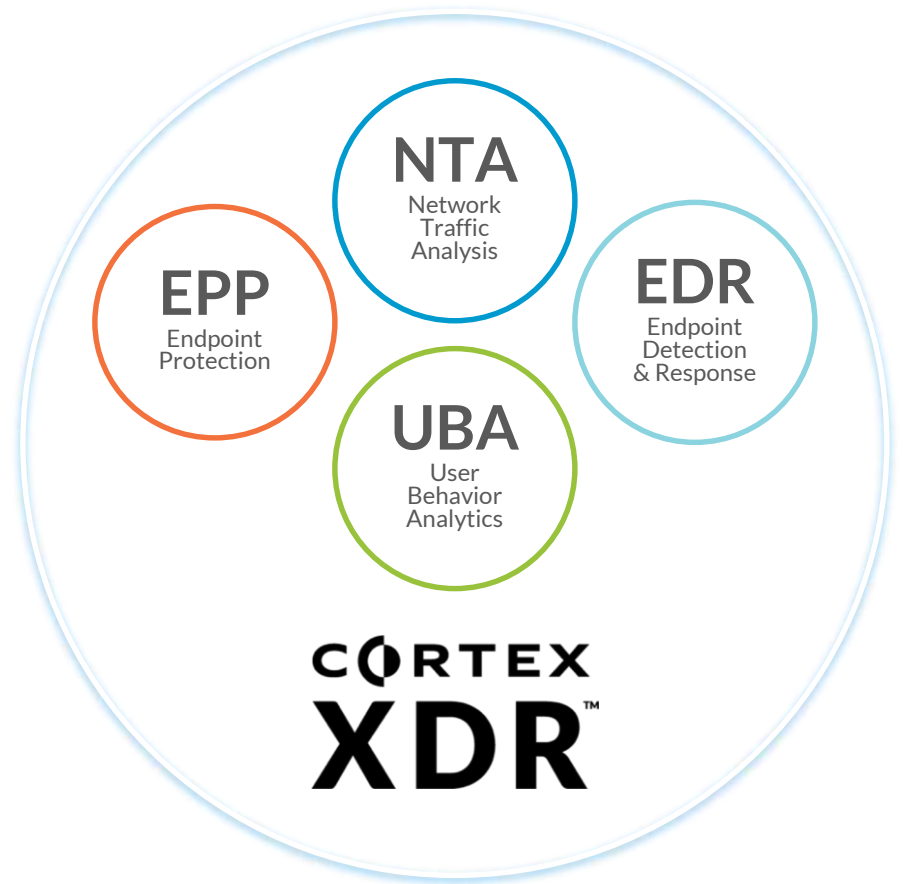


Attack technique coverage

The industry's best security data asset

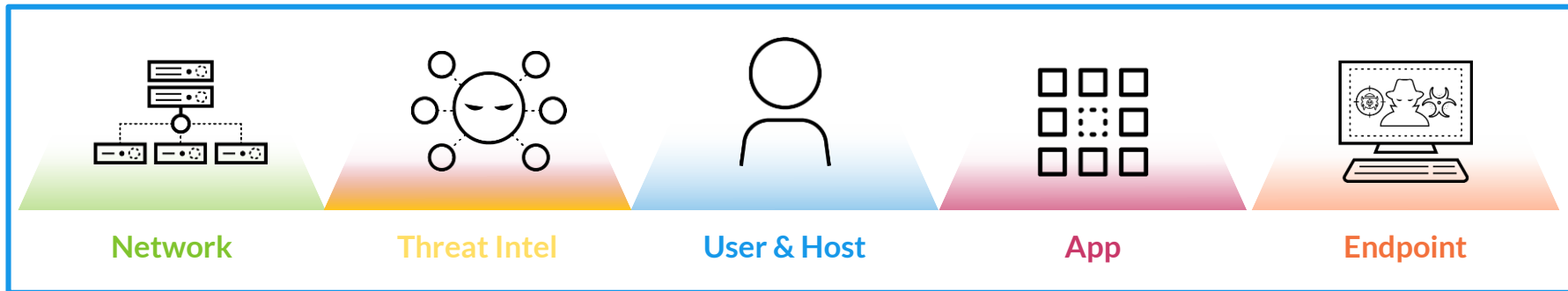


Breaking down point products operating in silos



Why is it critical we break down data silos?

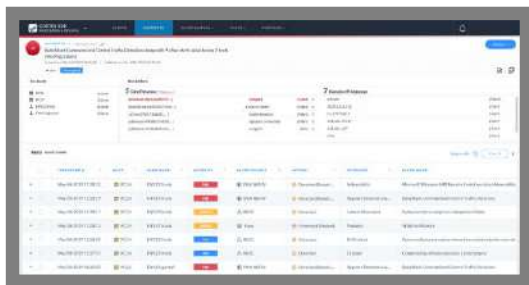
Cortex XDR provides an integrated view into all your data



Collect the right data for ML
and behavioral analytics

Automatically integrate data to
gain context for investigations

Automate root-cause analysis for investigation & response



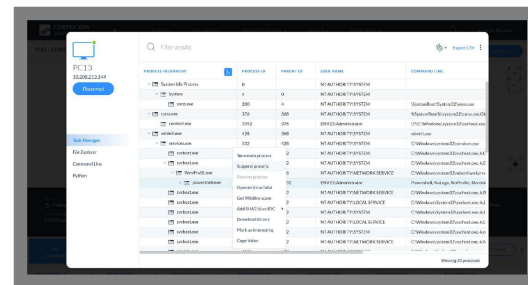
Intelligent Alert Grouping

Turn multiple related alerts into one incident



Automated Root Cause Analysis

Reveal the root cause of attacks in one click



Integrated Response

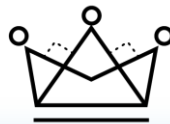
Quick actions to contain attacks or run custom forensics via live terminal

Cortex XDR Makes Detection & Response Accessible to All Analysts



Reduce risk of data
breach

Cut detection &
response times



Increase security
operations efficiency

Reduce alert
fatigue & turnover



Maximize detection
& response investments

Lower TCO by
44%

Cortex XDR breaks down silos to stop all attacks

CORTEX
XDR™



The new category for
detection & response

Best-in-class prevention

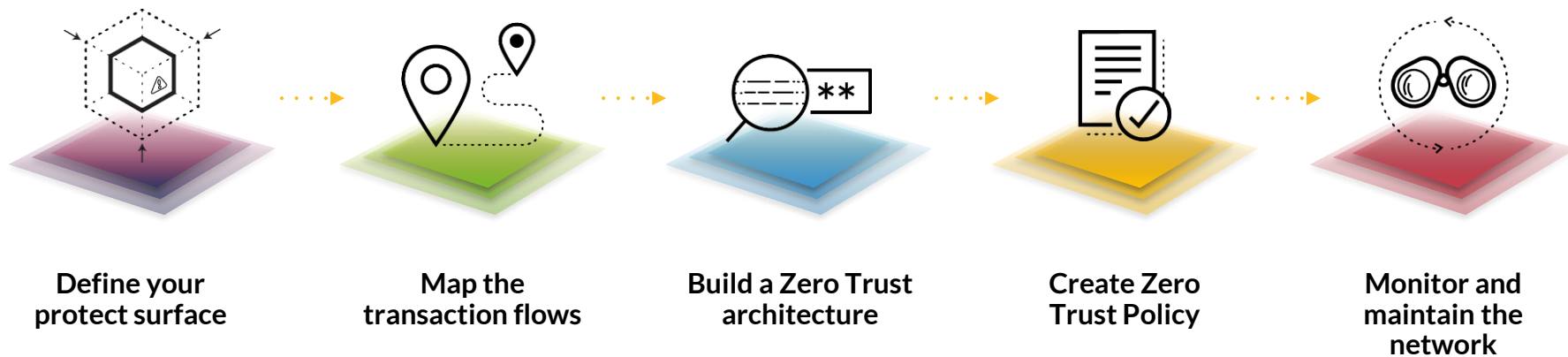
Most comprehensive security data asset

Continuous ML-based detection

Automated root-cause analysis

Integrated response for network and endpoint

The 5 Steps to Deploying Zero Trust



Prevention-Based Architecture Transformation

TRANSFORMATION LEVEL 1

VISIBILITY
INTO NON-ENCRYPTED TRAFFIC



TRANSFORMATION LEVEL 2

CONTROL
OF ALL TRAFFIC BY REDUCING
ATTACK SURFACE



TRANSFORMATION LEVEL 3

ENFORCEMENT
OF ADVANCED SECURITY POLICY



TRANSFORMATION LEVEL 4

INTEGRATION
ACROSS ALL DEPLOYMENT
SCENARIOS



OPERATIONAL TRANSFORMATION

Redefine process requirements



Apply automation



Formally document



Train and educate



Measure and revise

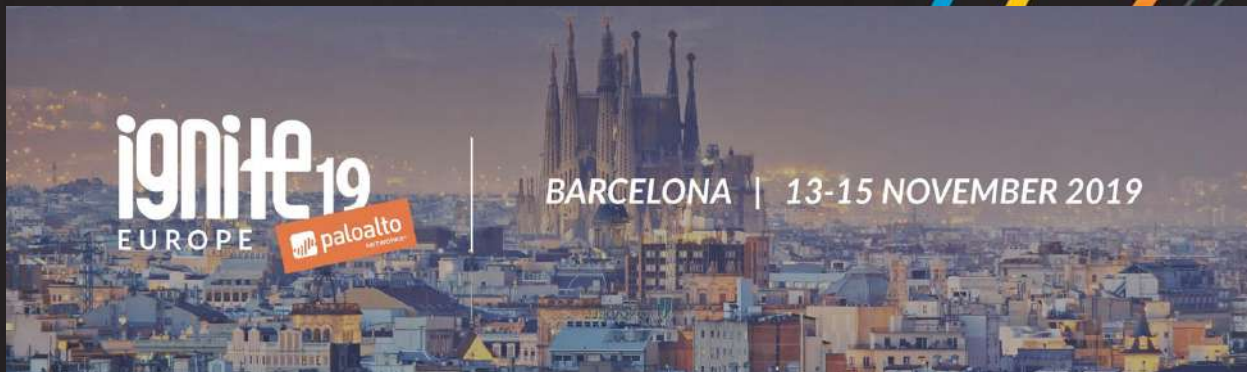


Thank You

paloaltonetworks.com

Email: jhaapio@paloaltonetworks.com

Twitter: [@PaloAltoNtwks](https://twitter.com/PaloAltoNtwks)



CORTEX™
BY PALO ALTO NETWORKS