Extending Zero Trust from Network to the Endpoint

Jani Haapio

jhaapio@paloaltonetworks.com

Channel SE

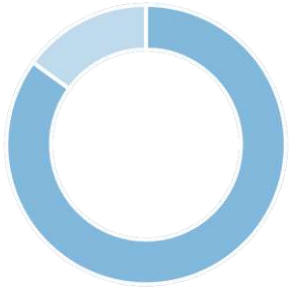
ZERO TRUST

paloalto NETWORKS

The world's leading cybersecurity company

85

of Fortune 100
rely on Palo Alto Networks

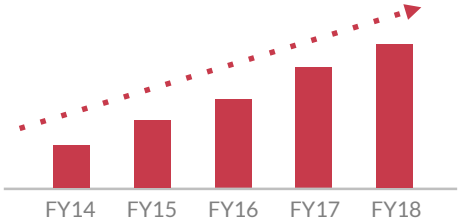


63% of the Global 2K
are Palo Alto Networks customers

#1

in enterprise security

Revenue trend 40% CAGR FY14 – FY18



28% year over year
revenue growth*

60,000+

customers
in 150+ countries

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

PRISMA BY PALO ALTO NETWORKS

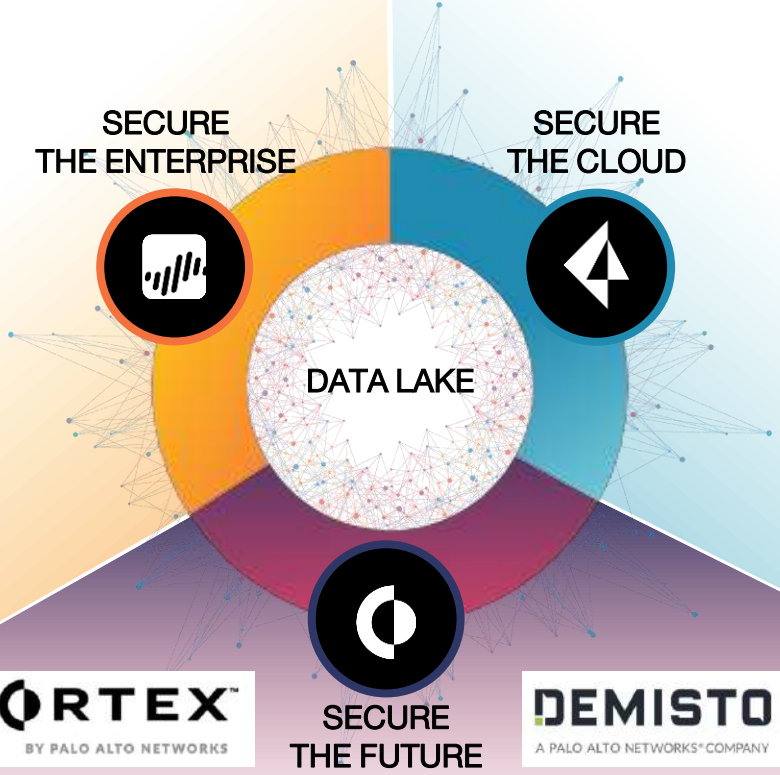
Hybrid data center

Internet Perimeter

Branch & mobile

5G & IoT

Endpoint



Secure access

SaaS

Public cloud

CORTEX BY PALO ALTO NETWORKS

DEMISTO A PALO ALTO NETWORKS® COMPANY

Detection & response

Automation & orchestration

Network traffic & behavioral analytics

Threat intelligence

paloalto NETWORKS

We Are a Leader Among ZTX Ecosystem Providers

We received the highest score in the strategy category

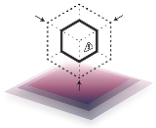
Our position validates the Security Operating Platform as an integrated platform that customers can use to implement Zero Trust and prevent successful cyberattacks

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

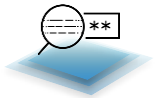


1. Define your Protect Surface

Next-Generation Firewall · VM Series · Cortex™ Data Lake · Cortex™ XDR · Transformation Services

2. Map the transaction flows

Next-Generation Firewall · VM Series · Cortex™ Data Lake · Cortex™ XDR · Traps · Transformation Services

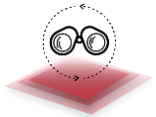


3. Build a Zero Trust architecture

Next-Generation Firewall · VM Series · 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

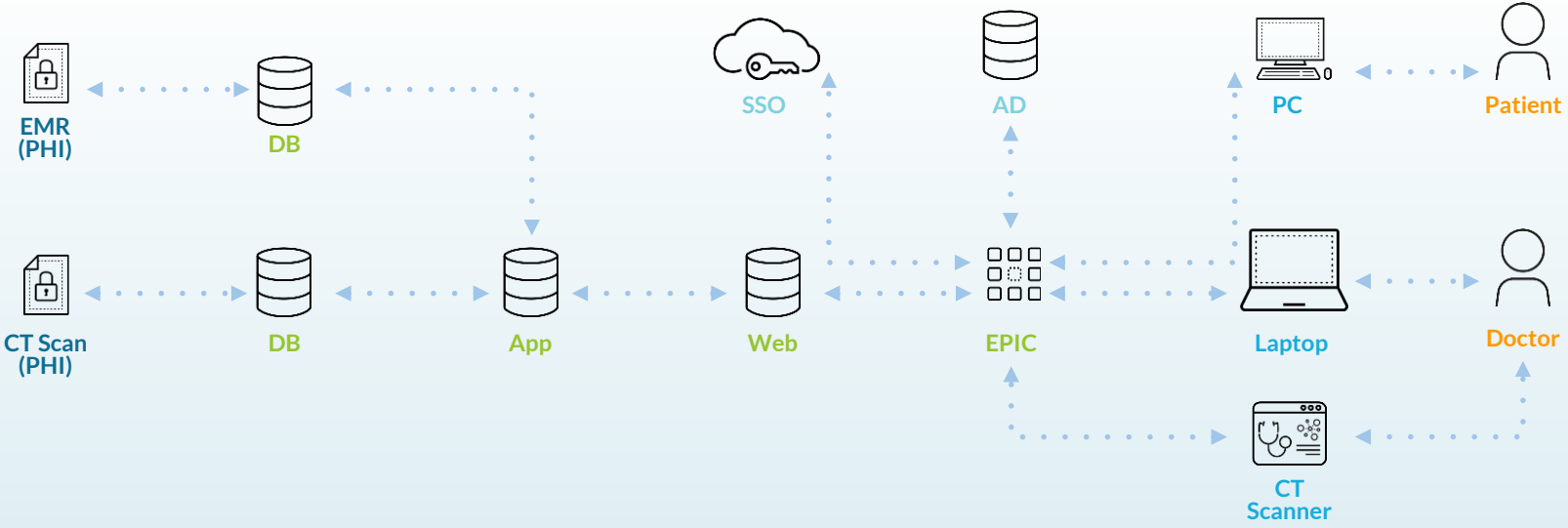
Step 1: Define Your Protect Surface

- 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

Data	Protect surface **Patient Info (PHI)**
Apps	Protect surface **EPIC**
Assets	Protect surface **Medical Equipment (CT Scanner)**
Services	Protect surface **Single Sign On (SSO), Active Directory (AD)**

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

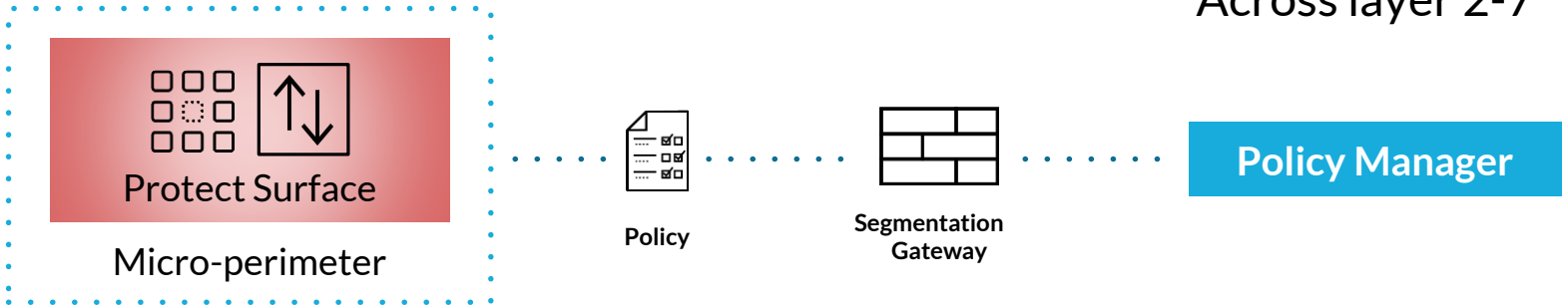


Step 3: Architect a Zero Trust Network

- 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

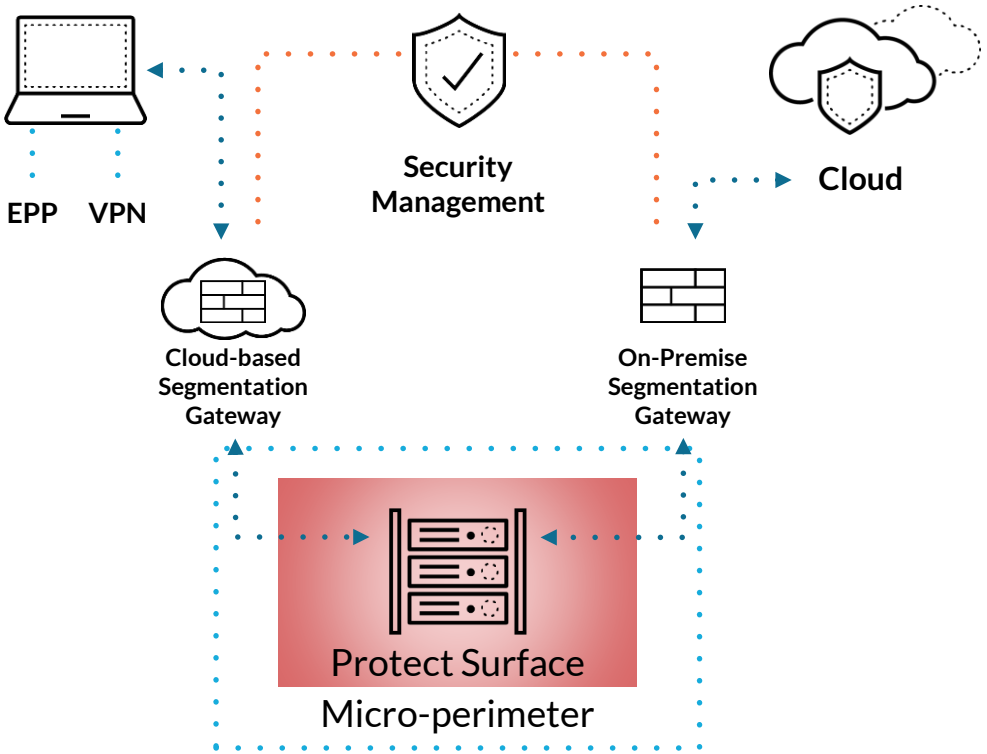
Why you're segmenting?
Define the protect surface

How you enforce segmentation?
Across layer 2-7



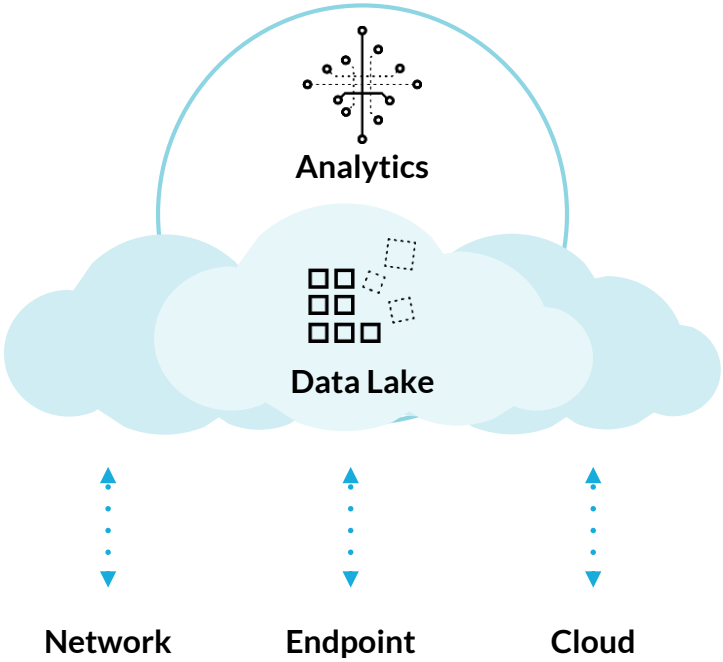
Step 4: Create a Trust Policy

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

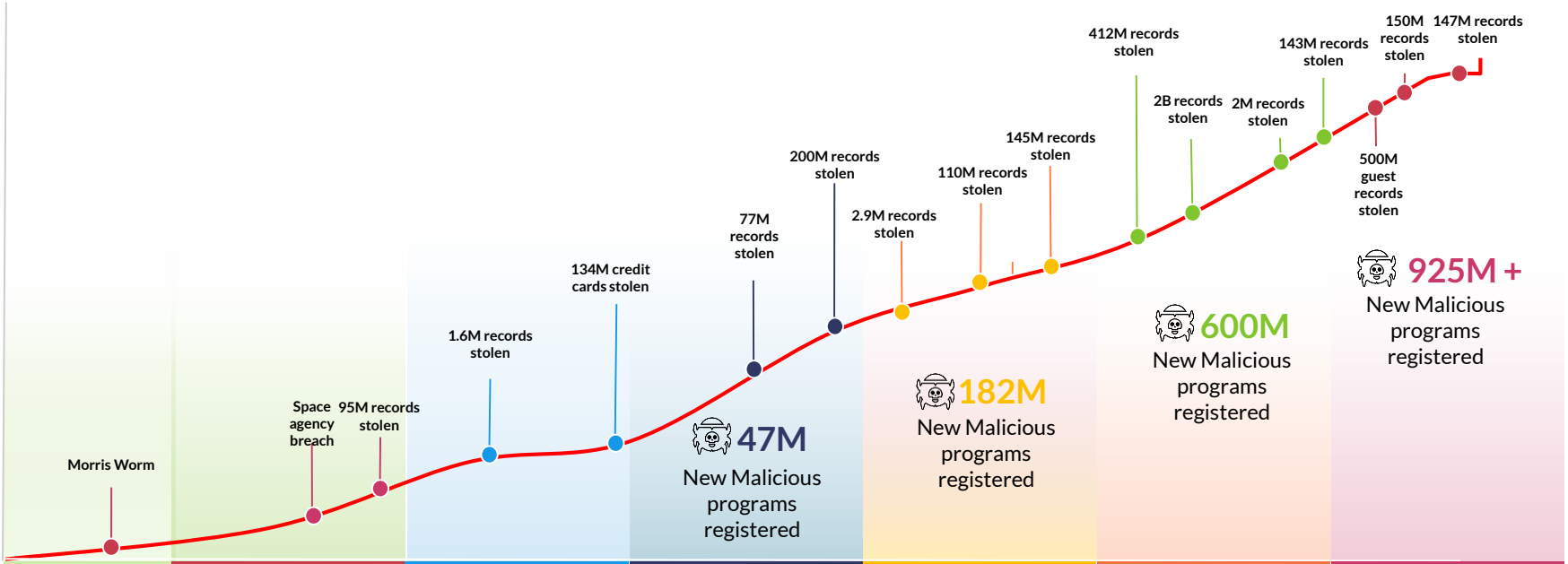


Step 5: Monitor and Maintain Your Environment with SecOps

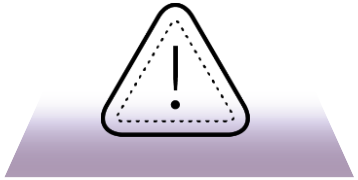
- Continuously monitor, enhance, and evolve your environment
- Use machine learning to quickly identify and respond to threats, and high priority alerts across the network, endpoint, and cloud



As threats escalate, SecOps is more important than ever



Why security teams struggle

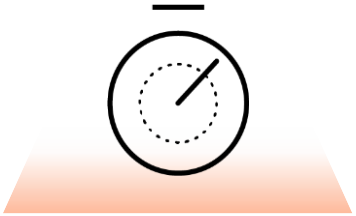


Gaps in Prevention

Legacy tools generate too many alerts

174k

alerts per week



Lack of Time

Manual tasks across siloed tools take too long

30+

point products

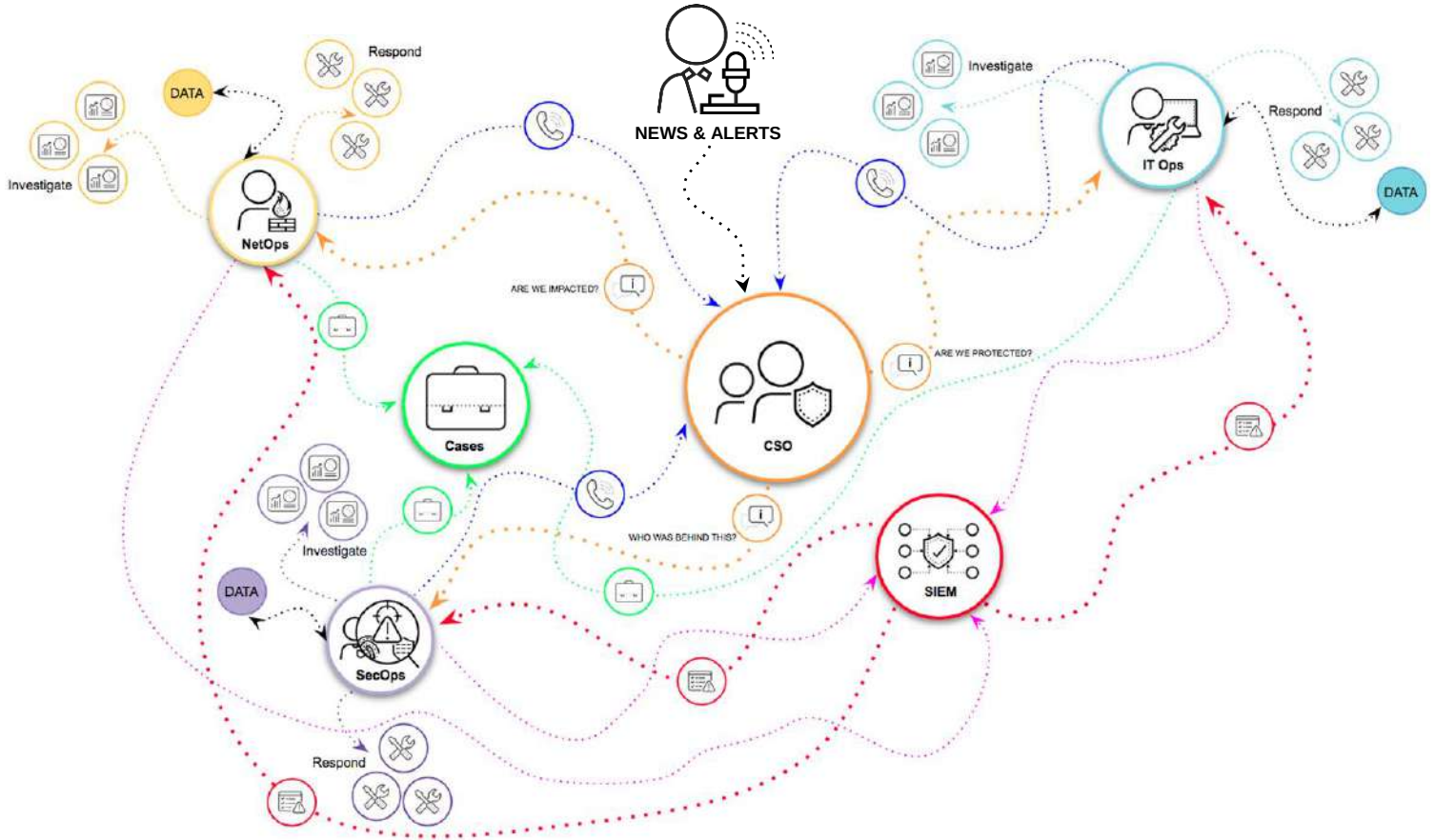
Limited Context

It takes days to investigate threats

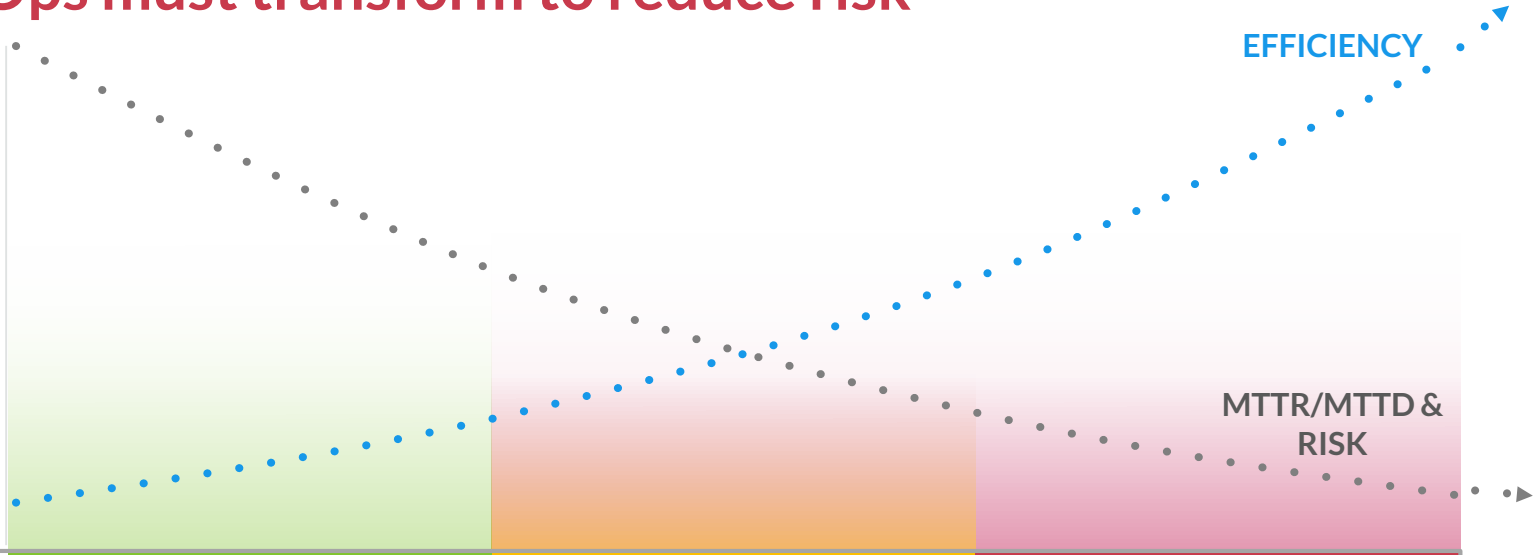
4+ days

to complete an investigation

The reality (and complexity) of security operations



How SecOps must transform to reduce risk



Maturity	Low (Reactive)	Medium	High (Proactive)
Detection	RULE-BASED	CORRELATED RULE-BASED	ANALYTICS-BASED
Context	LOG AGGREGATION	SILOED DATA COLLECTION	INTEGRATED RICH DATA
Automation	NONE	PARTIAL	FULL

Reinventing SecOps with Cortex

Prevent everything you can

Traps & Next-Generation Firewall

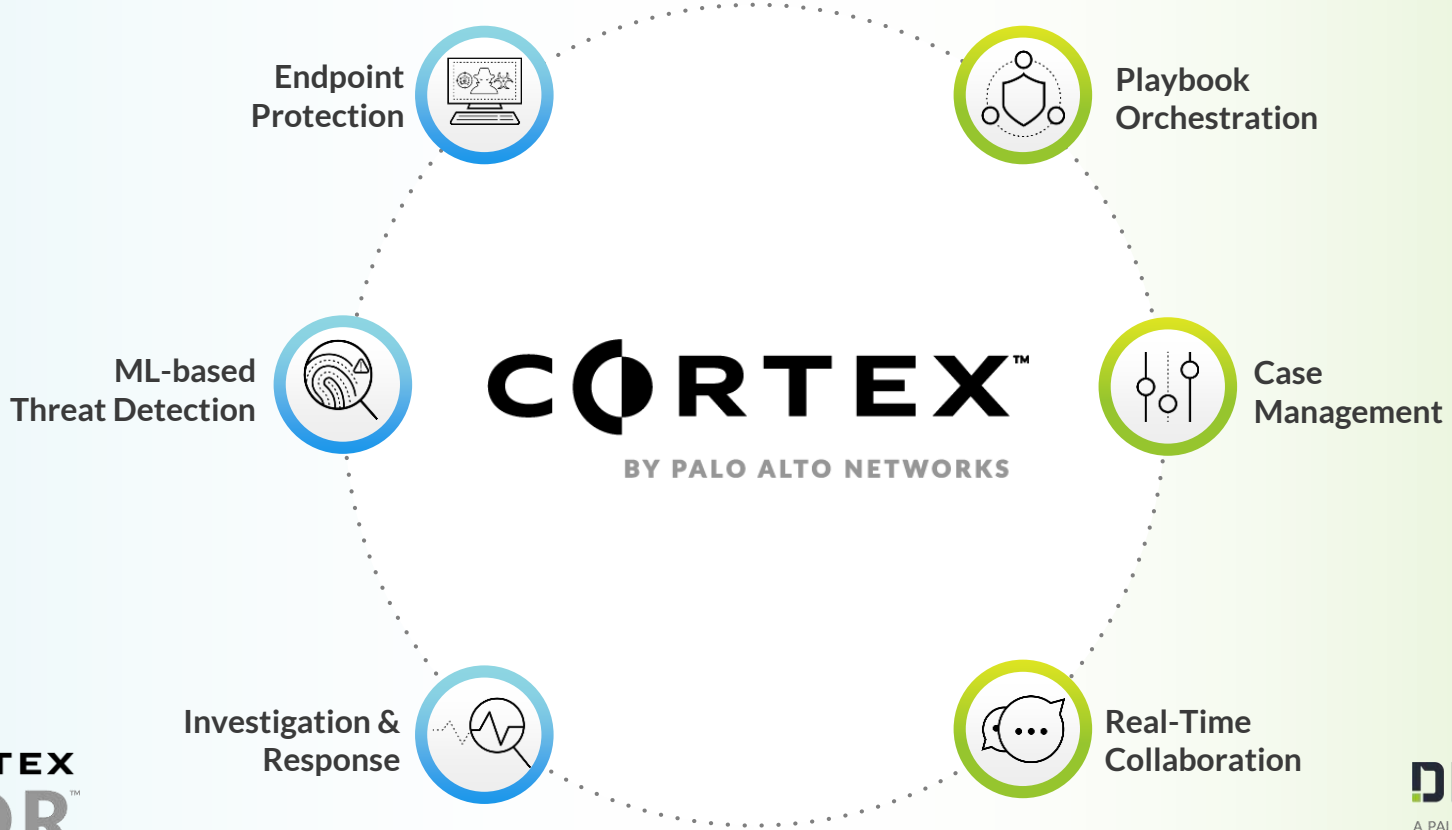
Everything you can't prevent, detection and investigate fast

Cortex XDR & Autofocus

Automate response and get smarter with each incident

Demisto

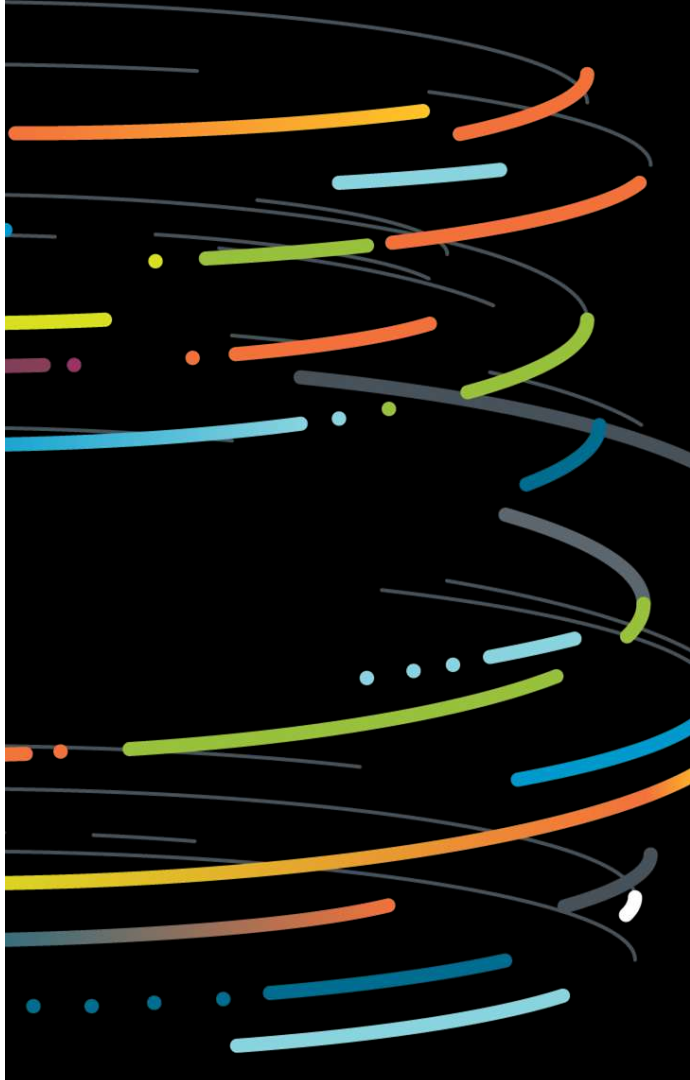
Reinventing SecOps with Cortex



CORTEX XDR™

DEMISTO
A PALO ALTO NETWORKS® COMPANY

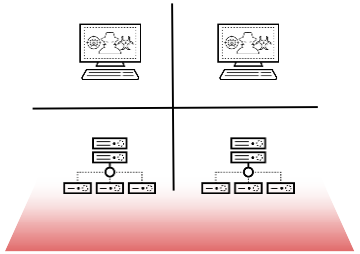
Use Case: Endpoint Protection



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

Phishing email and credentials stolen

Login using RPC and download malware

Exploit local vulnerabilities

Infect local endpoint and prepare for exfiltration

Lateral movement and data exfiltration

After

TR Exploit prevention based on technique

TR Malware protection trained by WildFire

TR Exploit prevention based on technique

TR Traps Behavior Threat Protection (BTP)

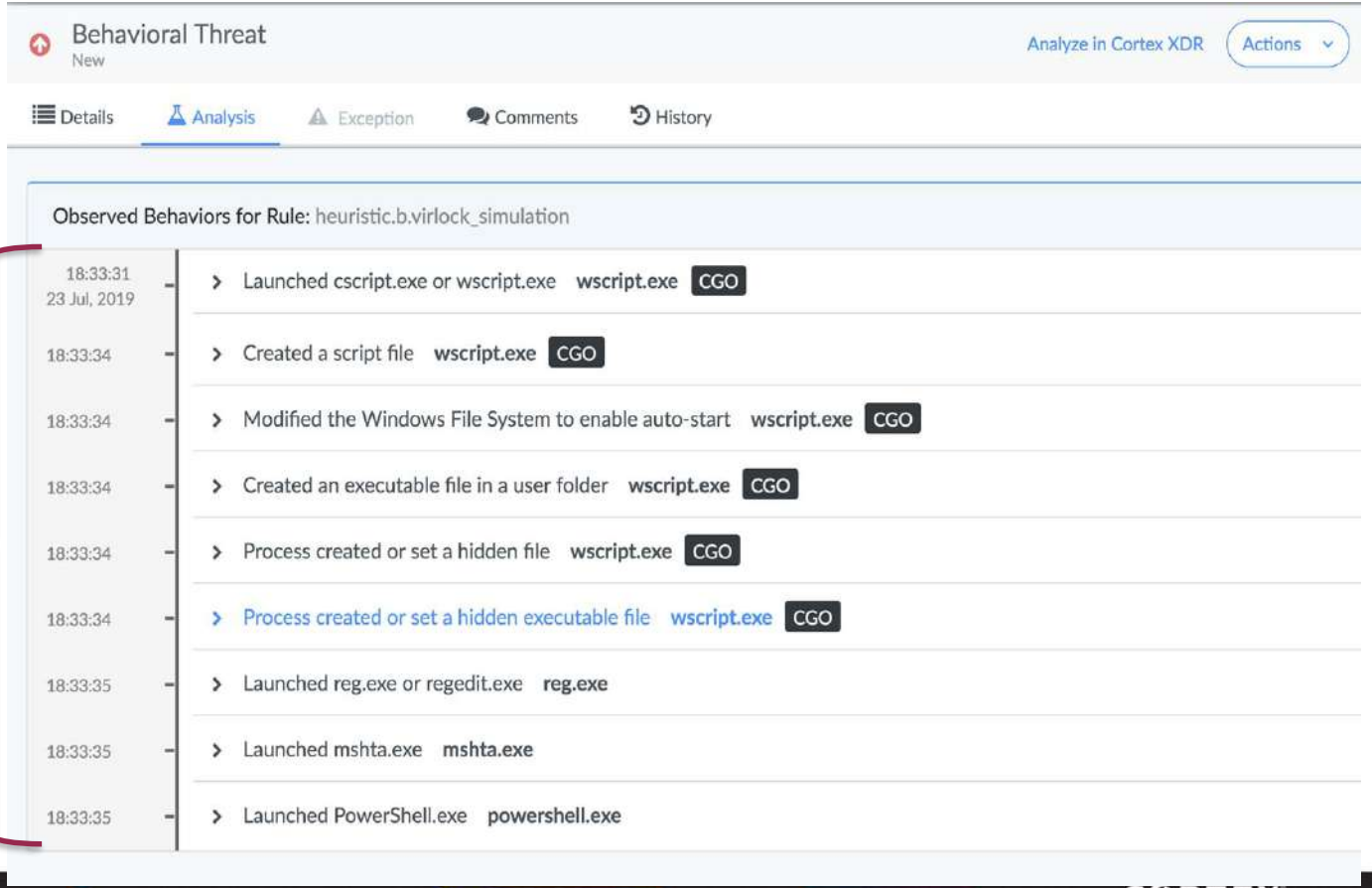
CORTEX XDR Investigate & respond with Cortex XDR

Sample Traps Security Event (BTP)

Endpoint behaviors that triggered the rule.

Can you determine the root cause:

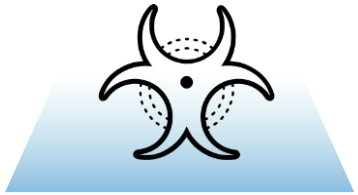
1. Drive by download?
2. USB installation?
3. Phishing?



Best-in-class prevention with Traps

Prevent all malware

High fidelity local detection trained by WildFire



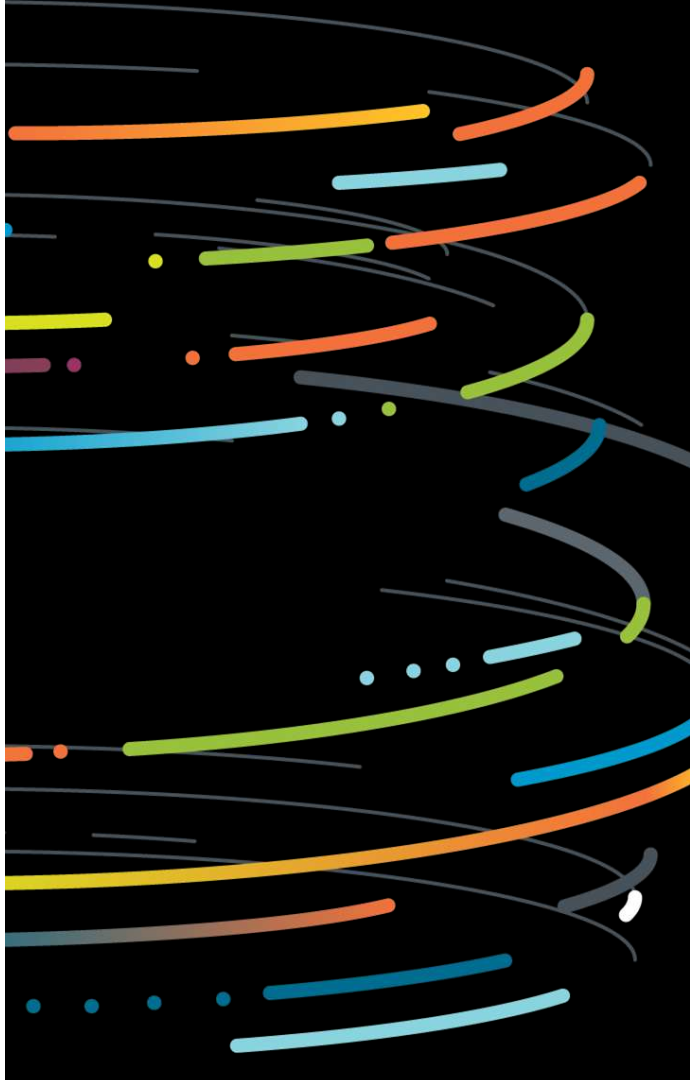
Block exploits

Block exploits based on techniques

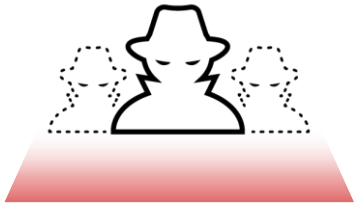
Analyze suspicious patterns

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

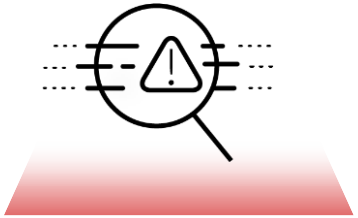


You Can't Prevent All Attacks

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

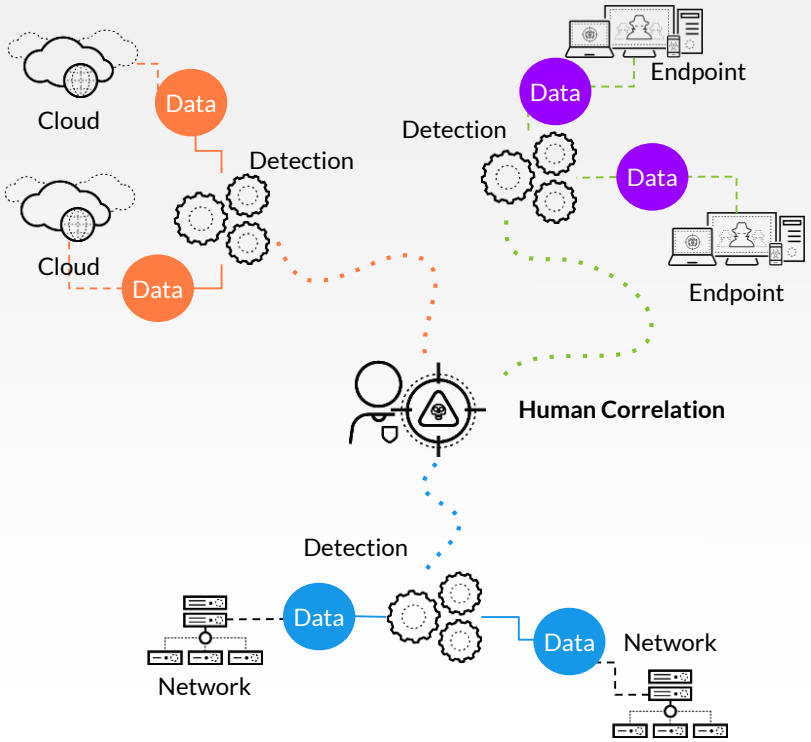


Anomaly Detection is not a "Human" Job

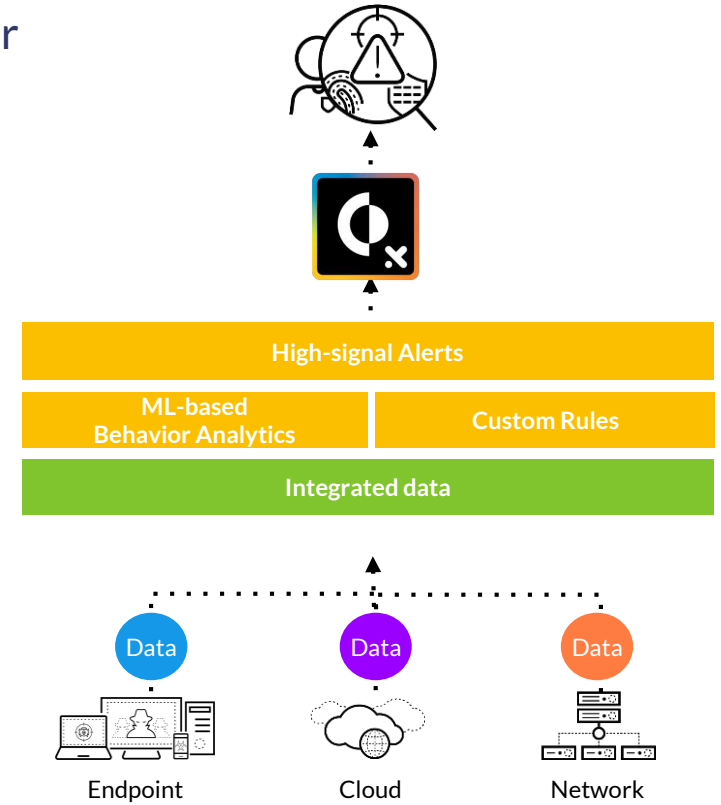
Detecting anomalies requires analyzing a comprehensive data set

Our Approach: Threat detection

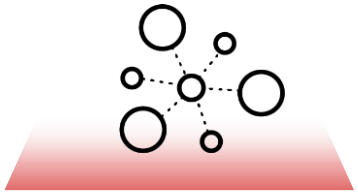
Before



After



The Problem: Threat containment takes too long

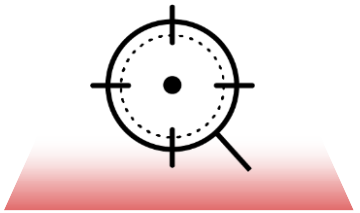


Limited Context Across Multiple Alerts

Analysts have to review each alert individually

Investigations Are Highly Manual

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

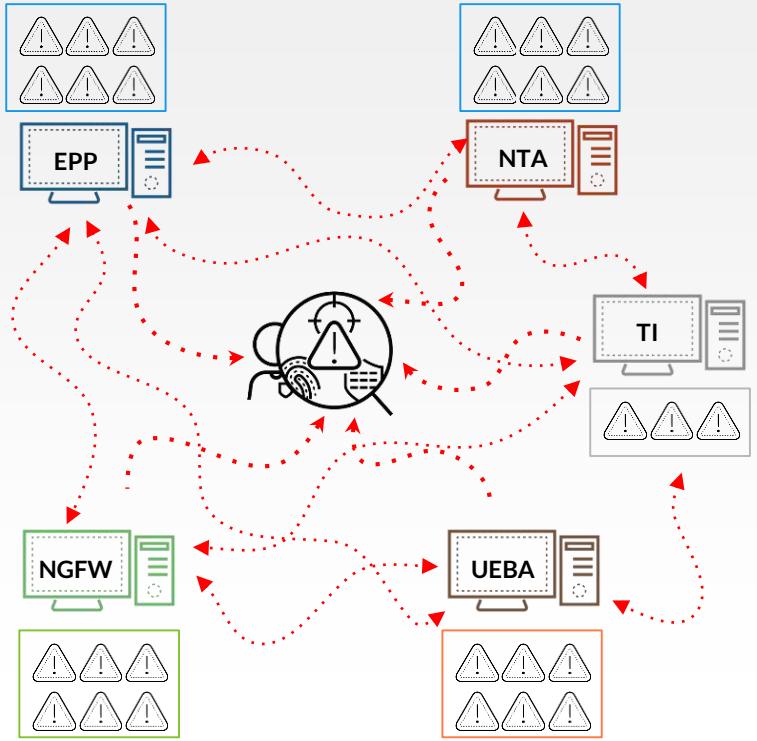


Finding Root Cause Takes Too Long

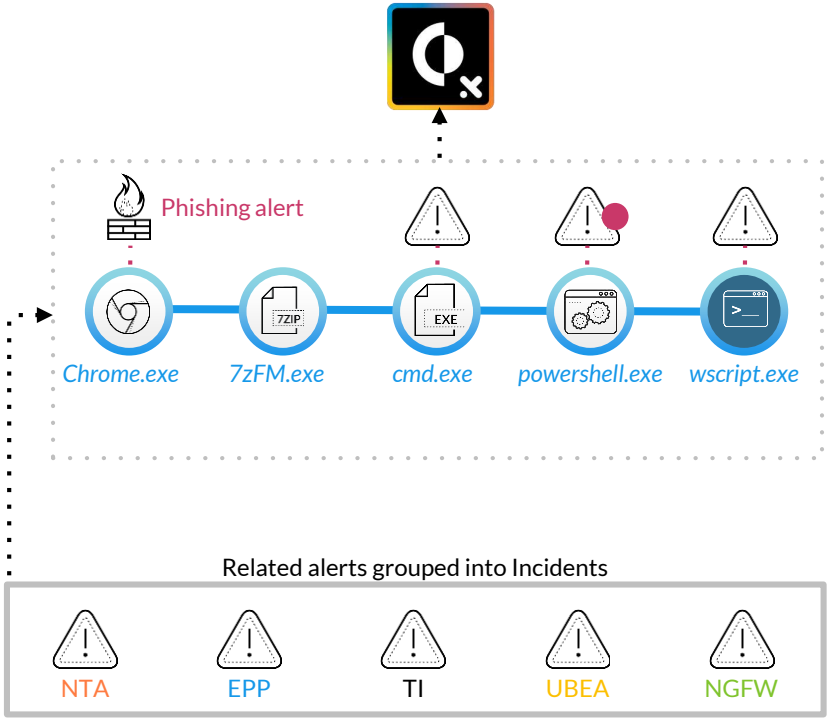
By the time you find root cause, the attack has progressed

Our Approach: Investigation & response

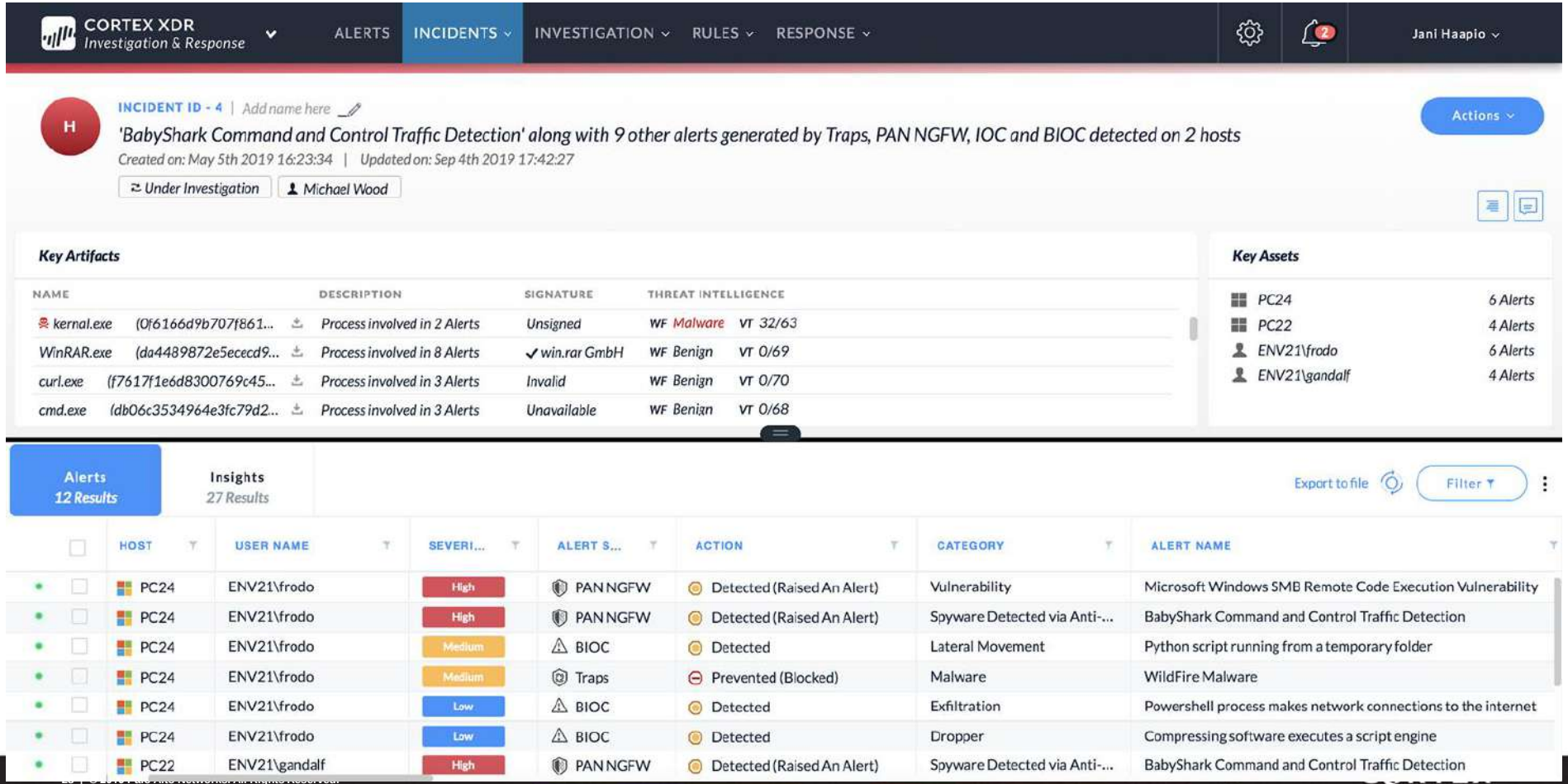
Before



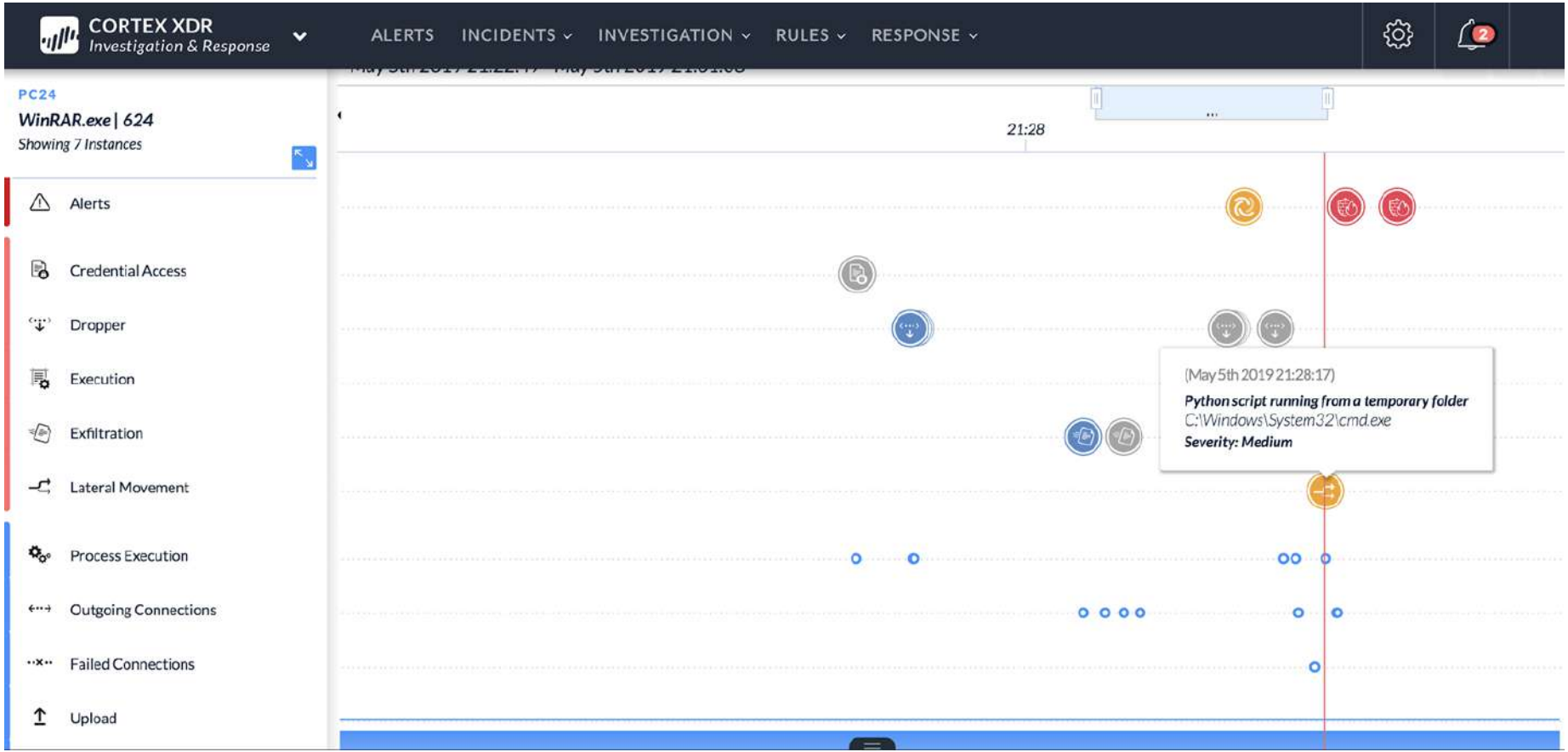
After



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

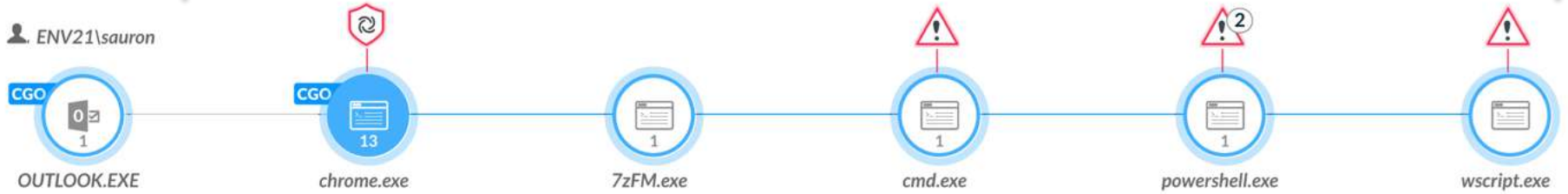


Investigate in timeline



Determining Root Cause of Security Events

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



Clicks on URL in phishing email

Default browser is opened

Downloads 7zip file

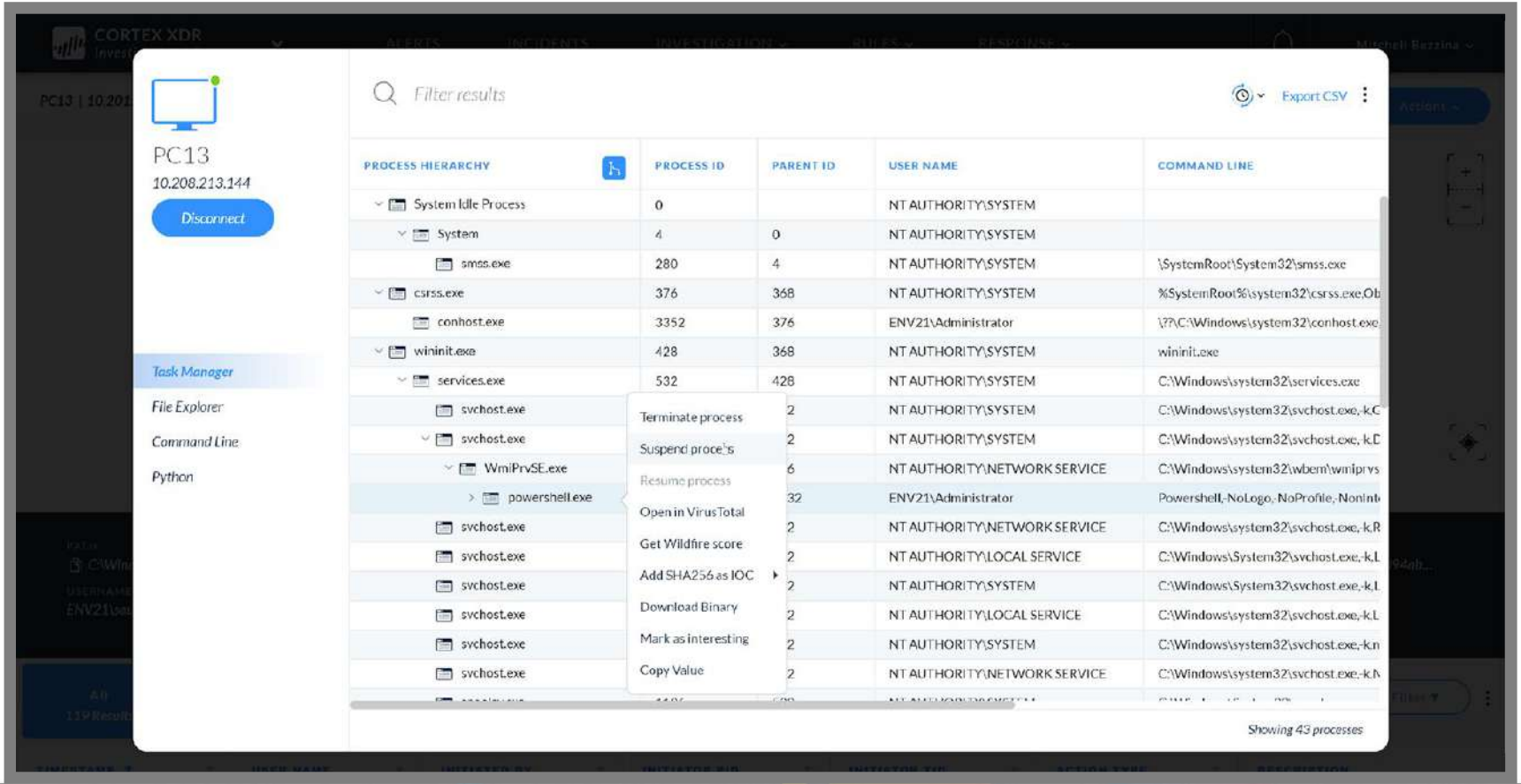
7zip runs *.pdf.bat file in zip

*pdf.bat file creates Virtual basic script for Windows script engine

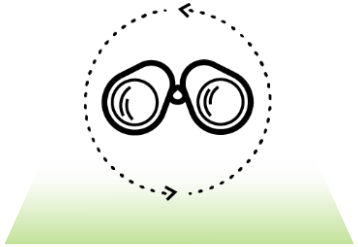
Attempts C2 connection

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

Integrated response via live terminal

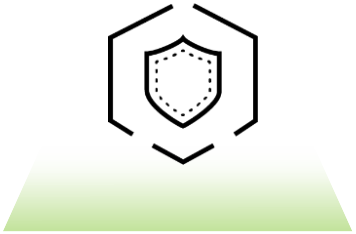


Key Differentiators: Find advanced attacks with analytics



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

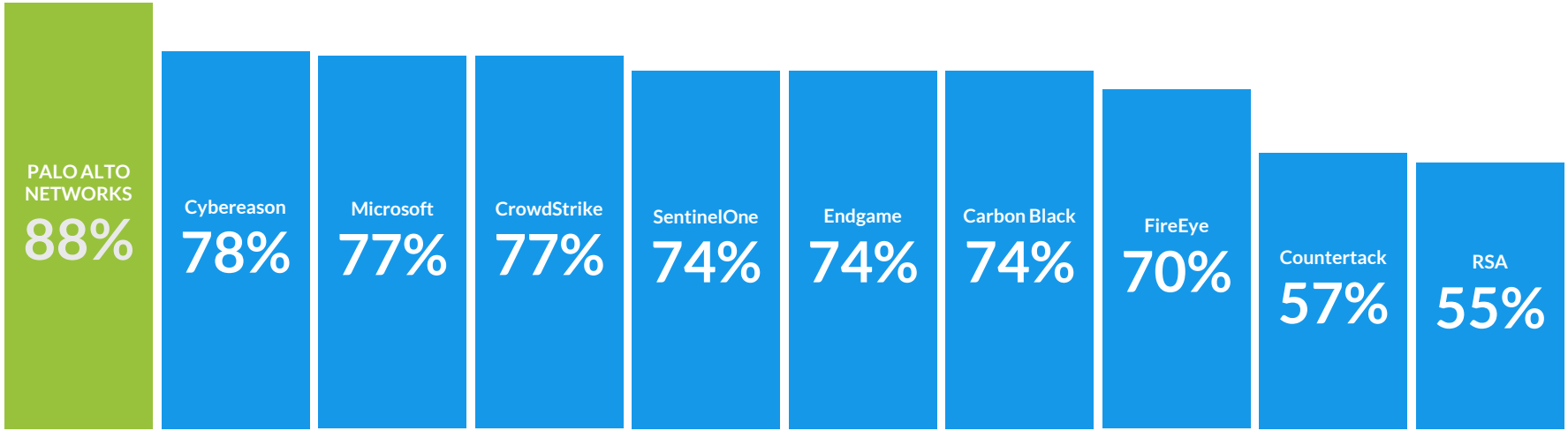
Patented Behavioral Analytics Technology

Find hidden threats with Machine Learning running across all data

Cortex XDR achieves best MITRE ATT&CK coverage

MITRE | ATT&CK™

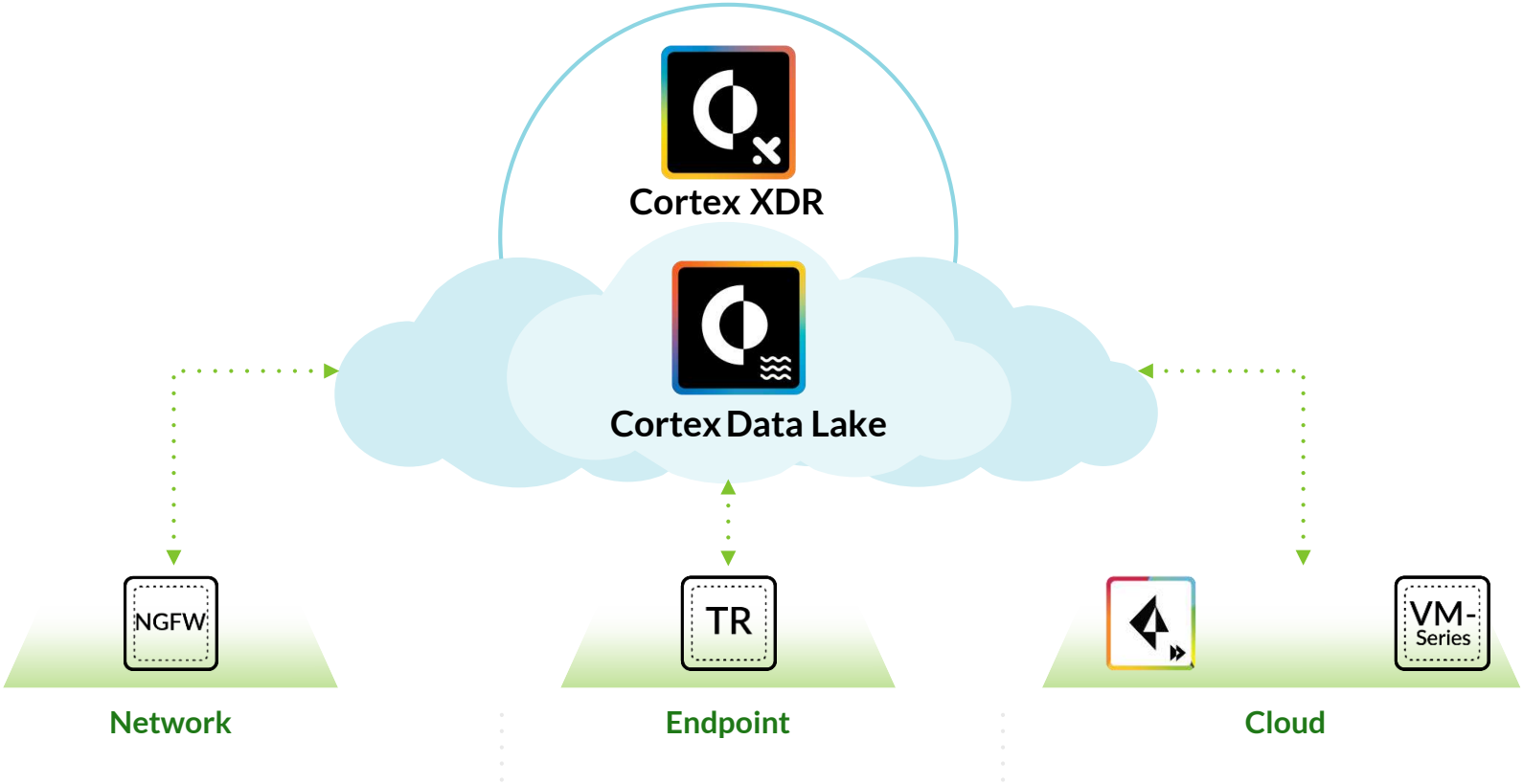
Scored higher than all other vendors with 93% fewer misses



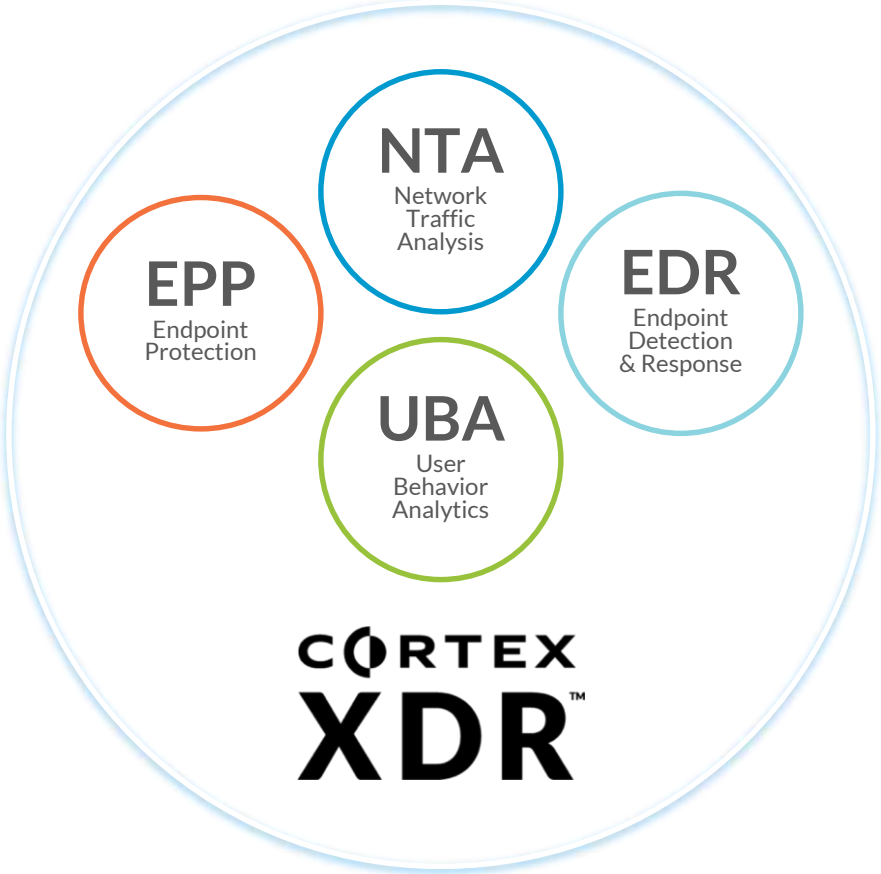
Attack technique coverage

CORTEX

The industry's best security data asset

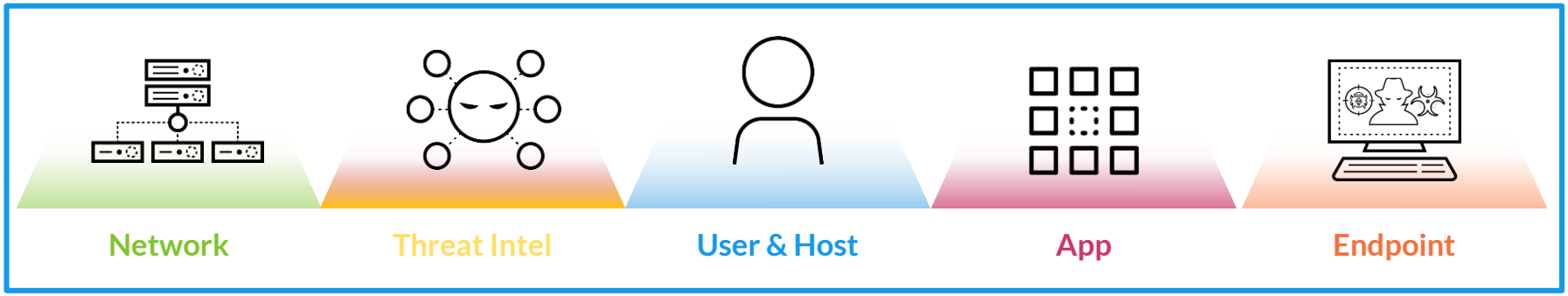


Breaking down point products operating in silos



Why is it critical we break down data silos?

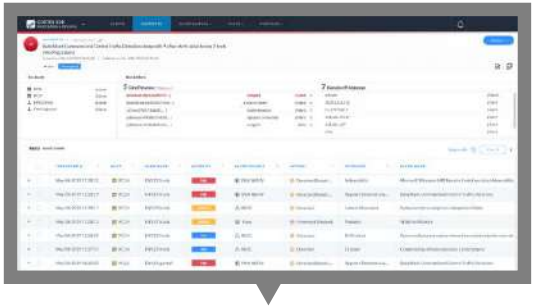
Cortex XDR provides an integrated view into all your data



Collect the right data for ML and behavioral analytics

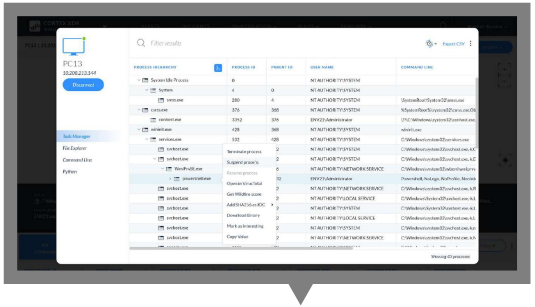
Automatically integrate data to gain context for investigations

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%

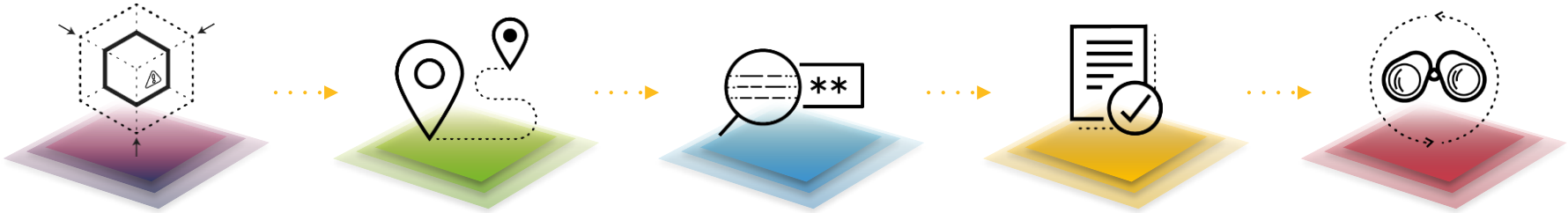
Cortex XDR breaks down silos to stop all attacks

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



Define your protect surface

Map the transaction flows

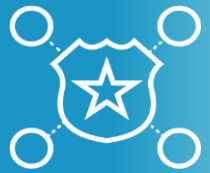
Build a Zero Trust architecture

Create Zero Trust Policy

Monitor and maintain the network

Prevention-Based Architecture Transformation

TRANSFORMATION LEVEL 1	TRANSFORMATION LEVEL 2	TRANSFORMATION LEVEL 3	TRANSFORMATION LEVEL 4
VISIBILITY INTO NON-ENCRYPTED TRAFFIC	**CONTROL** OF ALL TRAFFIC BY REDUCING ATTACK SURFACE	**ENFORCEMENT** OF ADVANCED SECURITY POLICY	**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

CORTEX™
BY PALO ALTO NETWORKS