CORTEX
BY PALO ALTO NETWORKS

CORTEX XDR

Extended detection and response

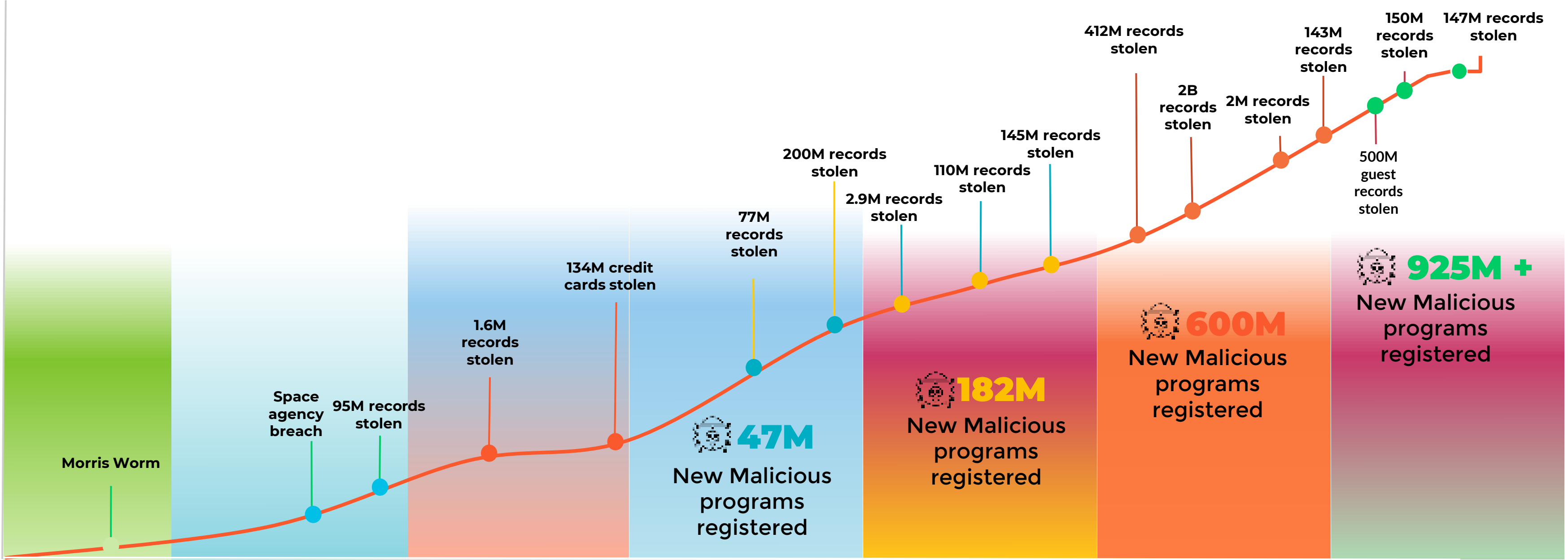
COHERENTIA
DIGITAL CYBERSECURITY

Luca.Bacchi@coherentia.it

paloalto NETWORKS

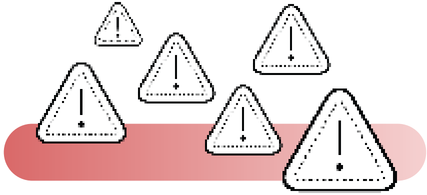
Emerging Challenges in Security Operations

As threats escalate, SecOps is more important than ever

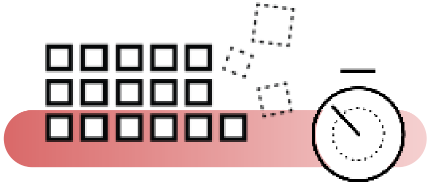


1998	2004	2007	2010	2013	2016	Present
Malicious code Trojans Worms Viruses	Identity theft Phishing Mobile viruses	DNS attacks Botnets Sabotage Anti-spam SQL attacks	Social engineering DDos attacks Malicious email Ransomware Botnets	Banking malware Keyloggers Ransomware Botnets	Ransomware Cryptominer Certificate attacks Bitcoin wallet Android hacks Insider threats	Cyberwarfare Fileless attacks Automated & AI attacks Cloud migration S3 buckets

Why do security teams struggle?



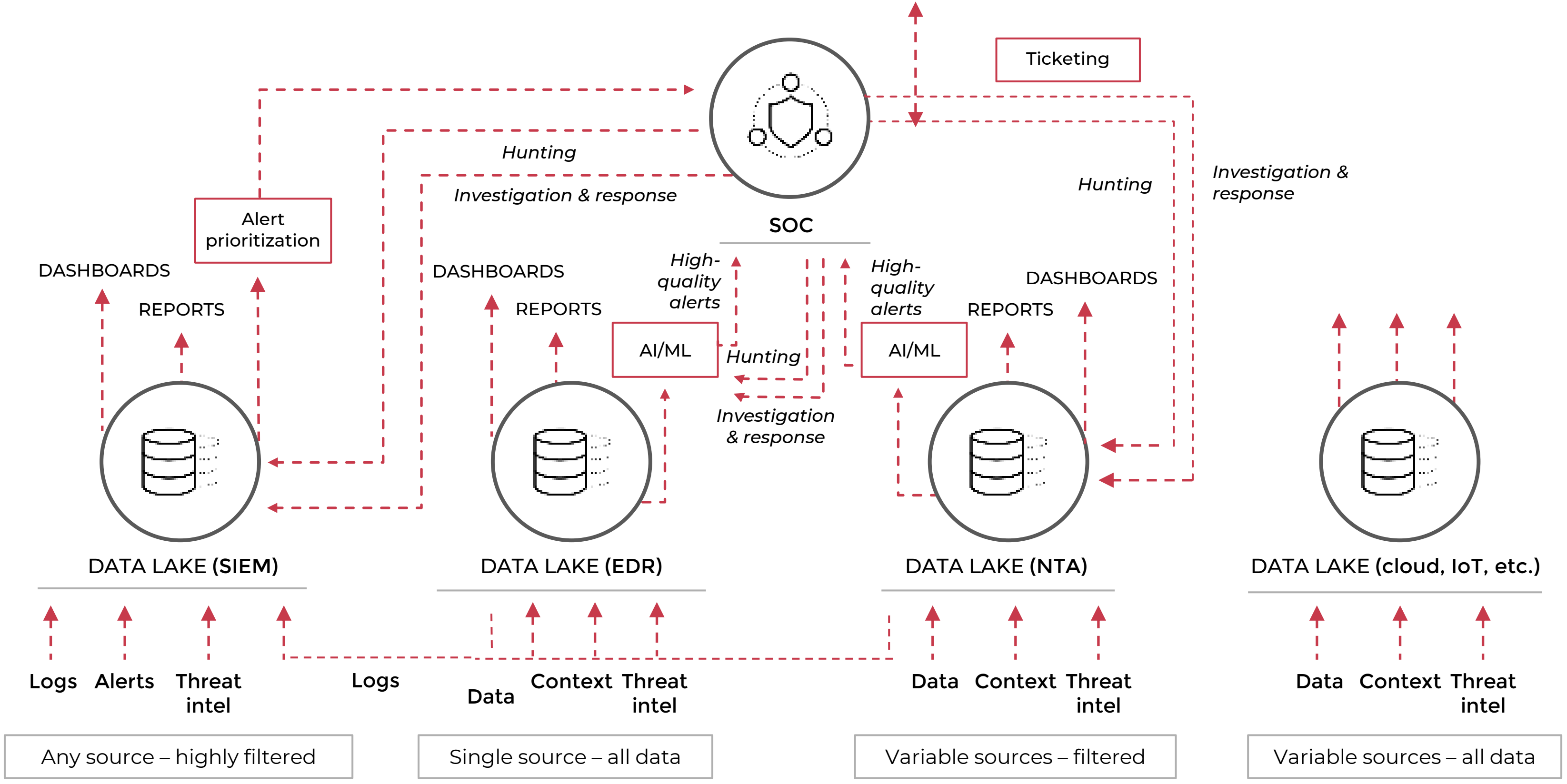
Too much noise, creating alert fatigue



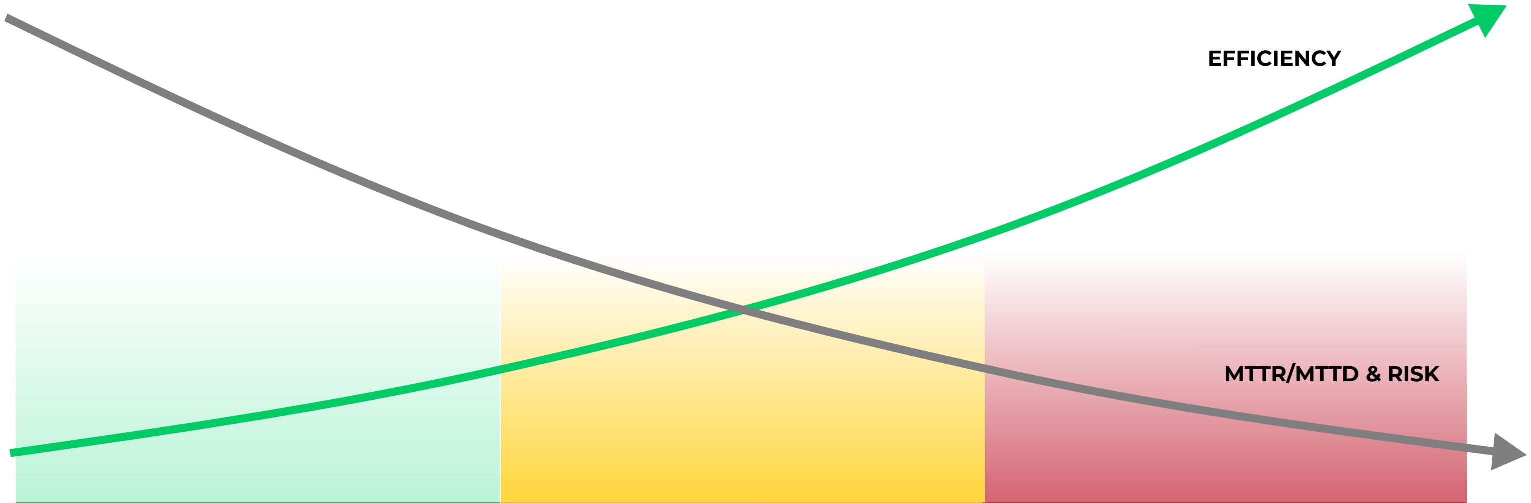
Too many products to piece together an incident

Too many manual, repetitive actions

Attempts to address gaps result in even more complexity



How SecOps must transform to reduce risk

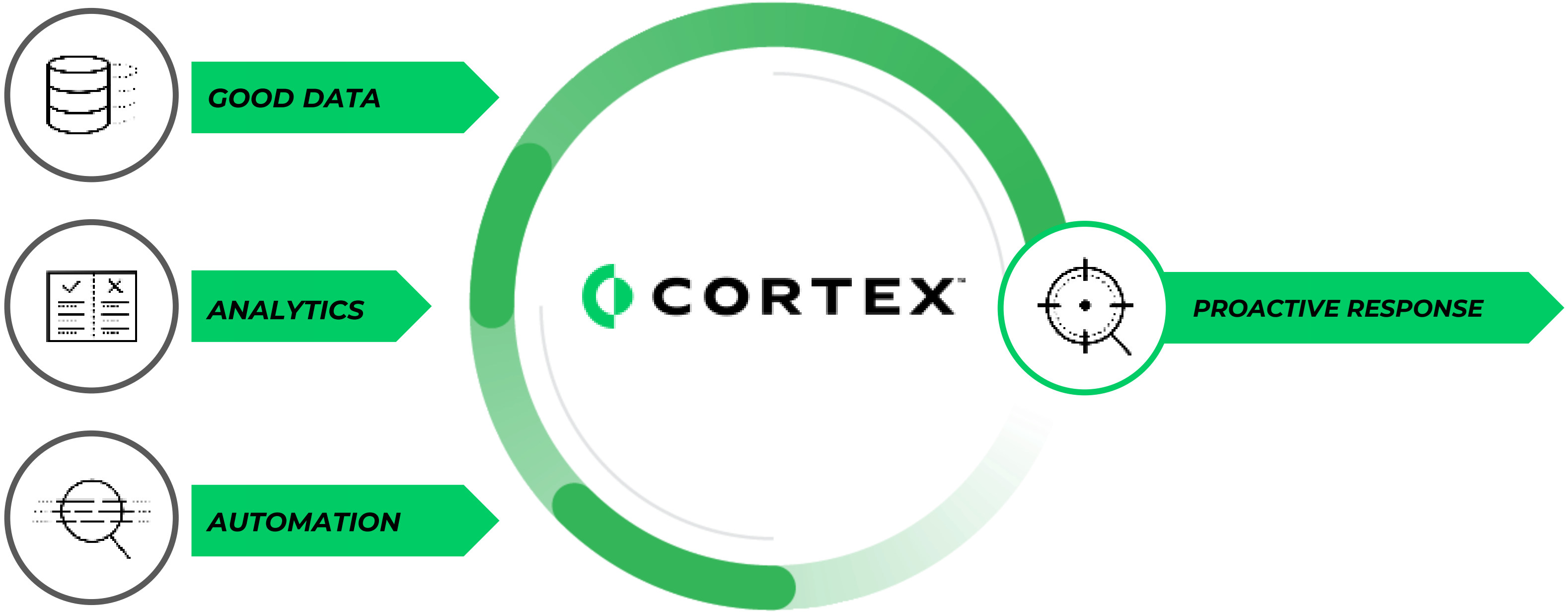


Maturity	**Low** (Reactive)	**Medium**	**High** (Proactive)
Detection	RULE-BASED	CORRELATED RULE-BASED	ANALYTICS-BASED
Context	LOG AGGREGATION	SILOED DATA COLLECTION	INTEGRATED RICH DATA
Automation	NONE	PARTIAL	FULL

Back to Cortex home >

Our Unique Approach

Our unique approach with Cortex



Rewiring SecOps with Cortex

Prevent everything you can

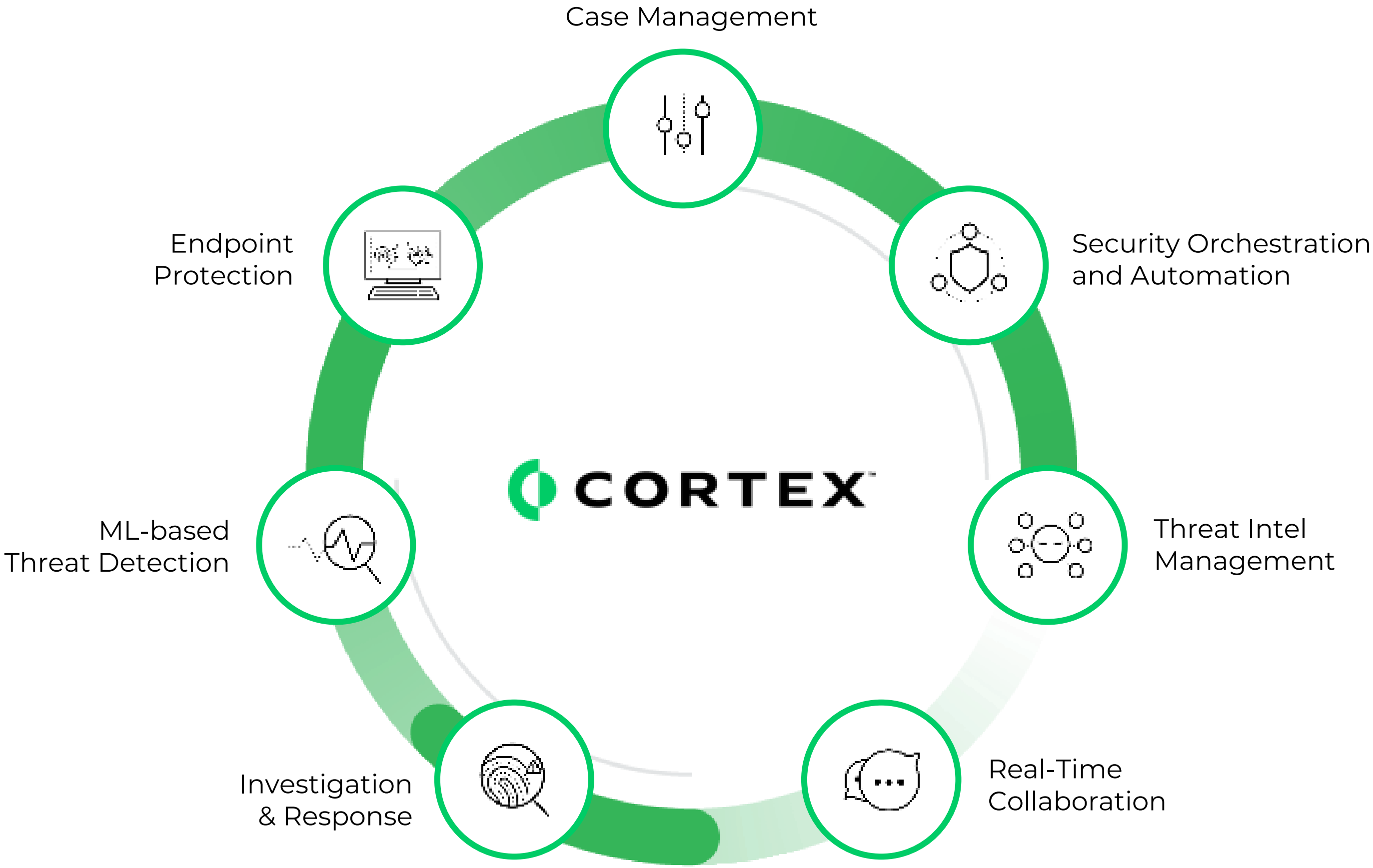
CORTEX XDR
BY PALO ALTO NETWORKS

Everything you can’t prevent, detect and investigate fast

CORTEX XDR
BY PALO ALTO NETWORKS

Automate response and get smarter with each incident

CORTEX XSOAR
BY PALO ALTO NETWORKS

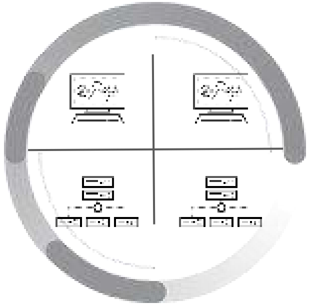

Case Management
Security Orchestration and Automation
Threat Intel Management
Real-Time Collaboration
Investigation & Response
ML-based Threat Detection
Endpoint Protection
CORTEX

Use Case: Endpoint Protection

The Problem: **Endpoint infections continue despite best efforts**

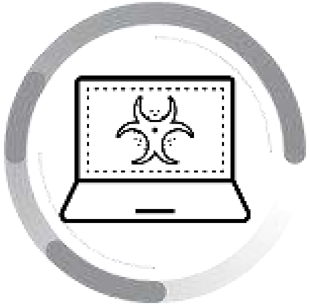
Legacy Endpoint Security Has Failed

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: Best-in-class endpoint protection

Before

- Open email attachment with malicious macros that launch PowerShell
- Download malware
- Run malware
- Infect local endpoint and prepare for exfiltration
- Lateral movement and data exfiltration

After

- Exploit prevention based on technique
- Malware protection trained by WildFire
- AI-based local analysis engine
- Behavioral Threat Protection (BTP)
- CORTEX XDR Investigate & respond

Key Differentiators: **Best-in-class prevention**

Prevent All Threats

Stop the advanced threats with machine learning, behavioral protection, and exploit mitigation

Shared Protections

Share protections across network, endpoint, and a global community of users

Enterprise-wide Detection & Response

Find, investigate and stop all attacks across network, endpoint and cloud assets

Use Case: Threat Detection

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

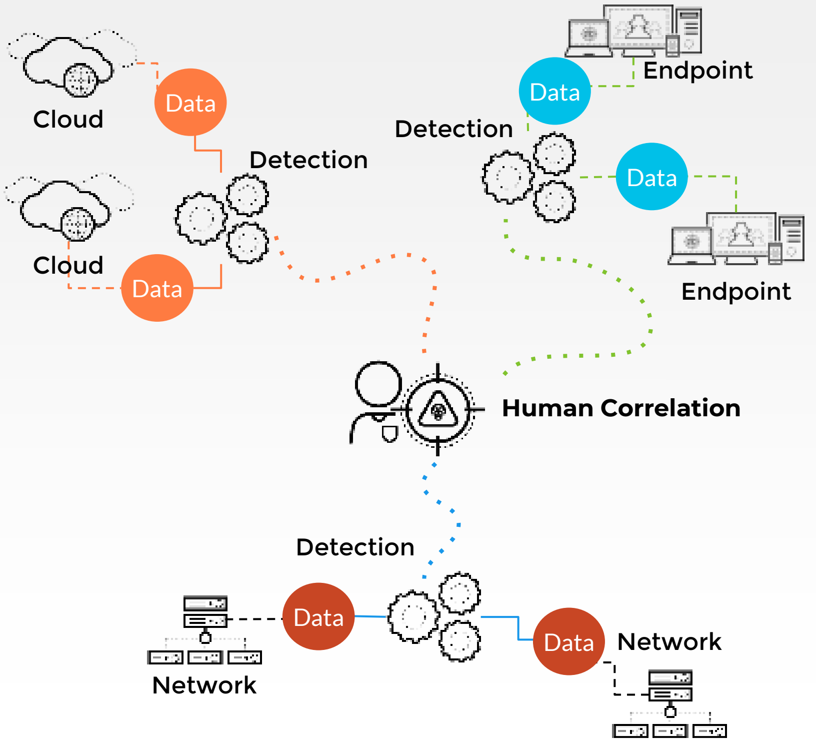
Teams waste time and miss threats chasing low-context false positive alerts

Anomaly Detection is not a "Human" Job

Detecting anomalies requires analyzing a comprehensive data set

Our Approach: **ML-based threat detection**

Before



Cloud

Data

Cloud

Data

Detection

Endpoint

Data

Detection

Data

Endpoint

Human Correlation

Detection

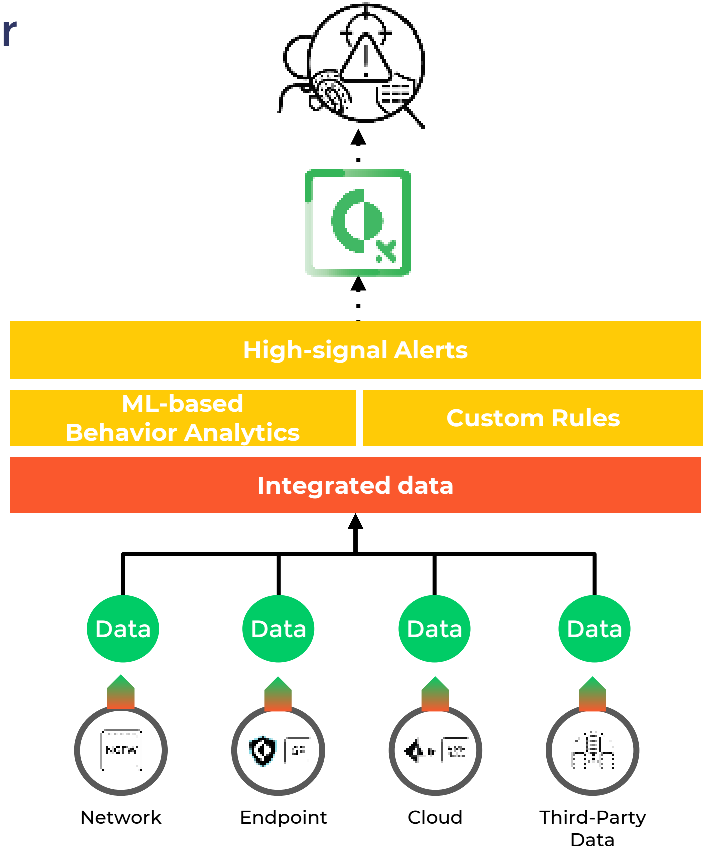
Network

Data

Data

Network

After



High-signal Alerts

ML-based Behavior Analytics

Custom Rules

Integrated data

Data

Data

Data

Data

Network

Endpoint

Cloud

Third-Party Data

Key differentiators: Find advanced attacks with analytics

Full Visibility To Detect Complex Threats

Eliminate blind spots across network, endpoint, and cloud

Patented Behavioral Analytics Technology

Find hidden threats with patented Machine Learning framework

Industry-leading Attack Coverage

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

Use Case: Investigation & Response

The Problem: Threat containment takes too long

Limited Context Across Multiple Alerts

Analysts have to review each alert individually

Investigations Are Highly Manual

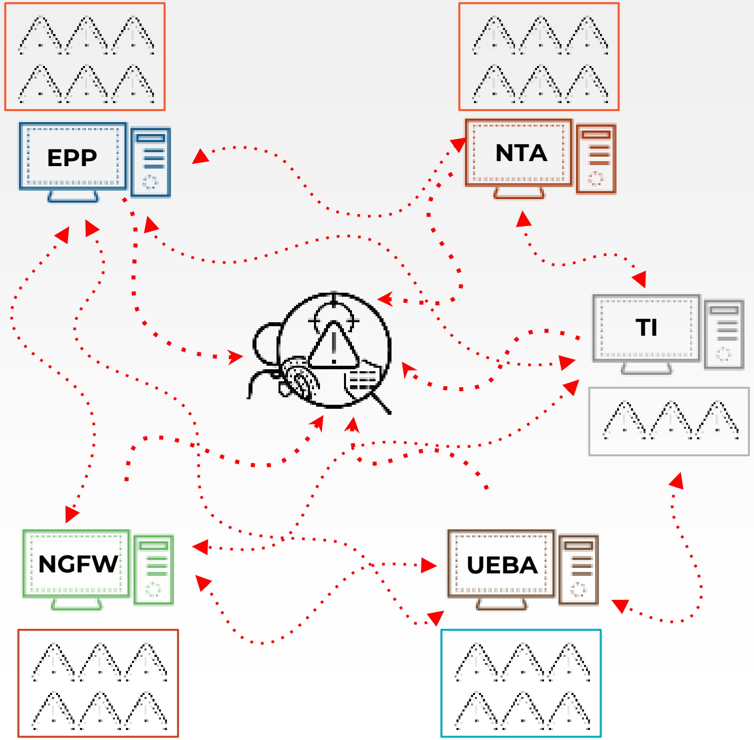
Teams must manually piece together data from siloed tools & data sources

Finding Root Cause Takes Too Long

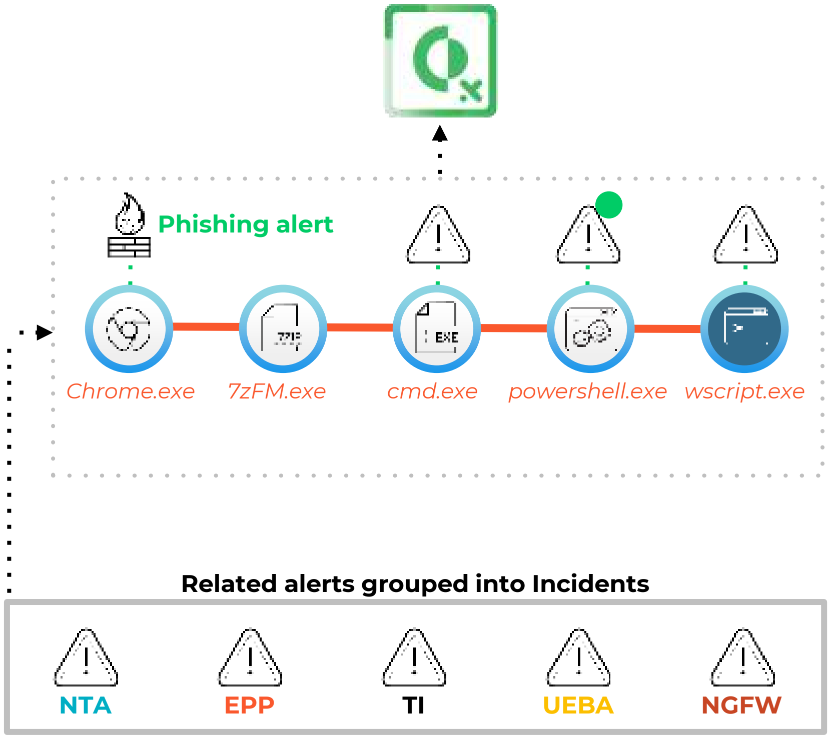
By the time you find root cause, the attack has progressed

Our Approach: Investigation & response with XDR

Before



After



Key Differentiators: Cut investigation & response time

Intelligent Alert Grouping

Turn multiple related alerts into one incident

Data Integration For Full Visibility

Unify network, endpoint, and cloud data to streamline analysis

Automated Root Cause Analysis

Easily understand the source and progression of attacks

Use Case: Managed Threat Hunting

The Problem: Proactive threat hunting is difficult

Lack of Time

Most teams don’t have the time to proactively hunt for threats

Lack of Resources

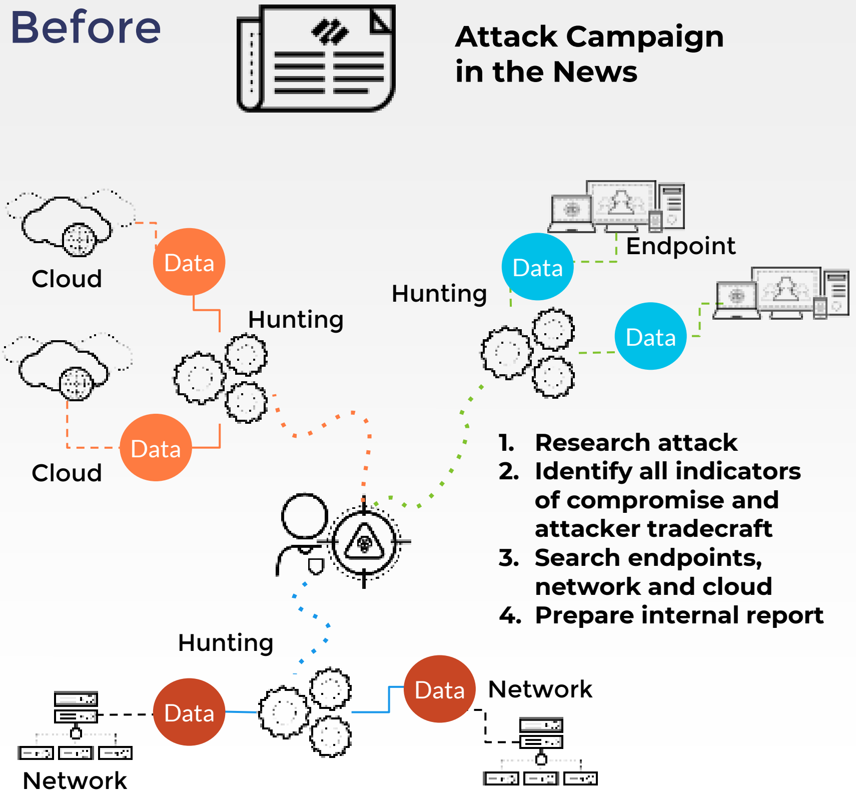
Teams rarely have advanced threat hunters dedicated to finding attacks

Missed Attacks

Without manual threat hunting, organizations may not find the stealthiest attacks

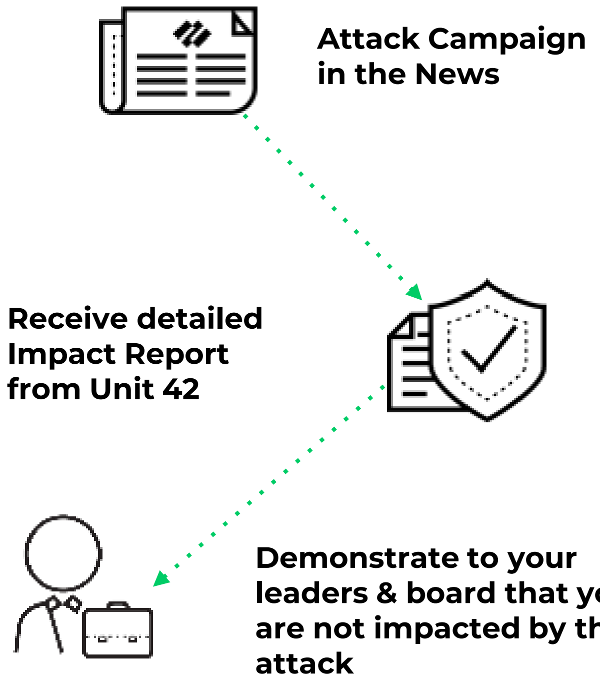
The Value of Impact Reports When a High-Profile Attack Strikes

Before



1. Research attack
2. Identify all indicators of compromise and attacker tradecraft
3. Search endpoints, network and cloud
4. Prepare internal report

After



Receive detailed Impact Report from Unit 42

Demonstrate to your leaders & board that you are not impacted by the attack

Get Peace of Mind with Cortex XDR Managed Threat Hunting

Built on Cortex XDR Data

Analytics on integrated endpoint, network, and cloud data for unrivaled threat hunting

Backed by Unit 42

World-renowned threat hunters continuously monitor your environment for attacks

Enriched with Context

High-fidelity threat intel informs Threat and Impact Reports

Use Case: Managed Detection & Response

The Problem: Security teams struggle to keep up on their own

Security operations is broken

The average security team can only handle 7% of alerts

Traditional security services are limited

The responsibility of investigation and response is on the security team

Vendor-based MDR services lack visibility

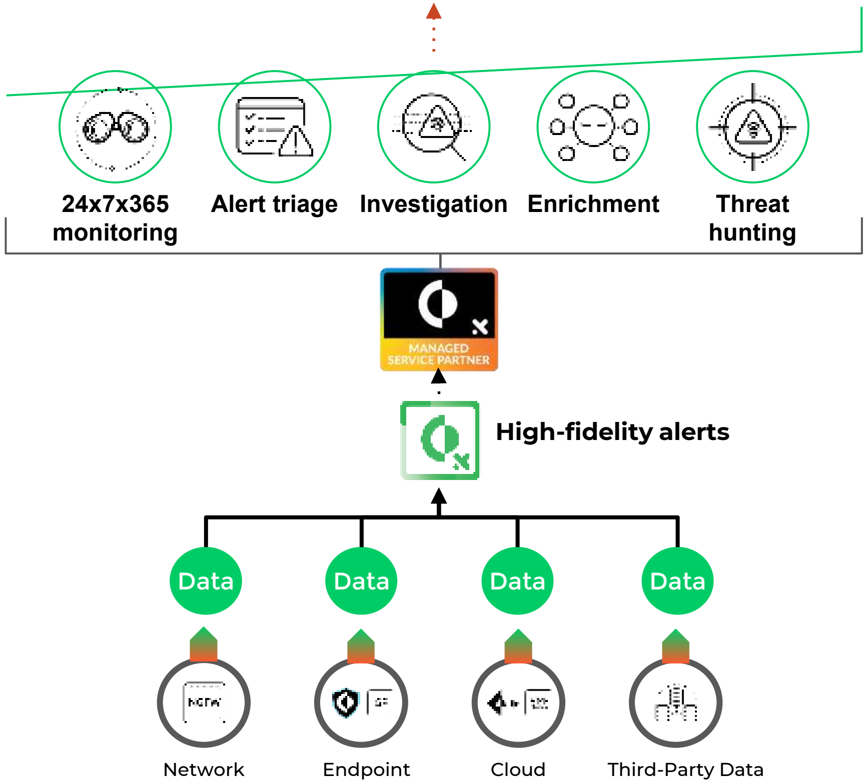
Siloed tools lack the visibility required to create time-based SLAs you can trust

Our Approach: Partner with industry-leading MDR providers

Before

- Analysts bogged down by alert volume
- Point products produce high false-positive rates with little context
- Investigations are manual and complex
- Experts rarely have time to be proactive

After



Response to validated threats in <60 minutes

24x7x365 monitoring

Alert triage

Investigation

Enrichment

Threat hunting

High-fidelity alerts

Data

Data

Data

Data

Network

Endpoint

Cloud

Third-Party Data

Key Differentiators: Slash complexity & response times

accenture
pwc
BDO
on2it
CRITICALSTART
Trustwave

Accelerate time-to-value

Get deployed fast and shift to proactive security operations in weeks, not years

Put decades of security experience to work

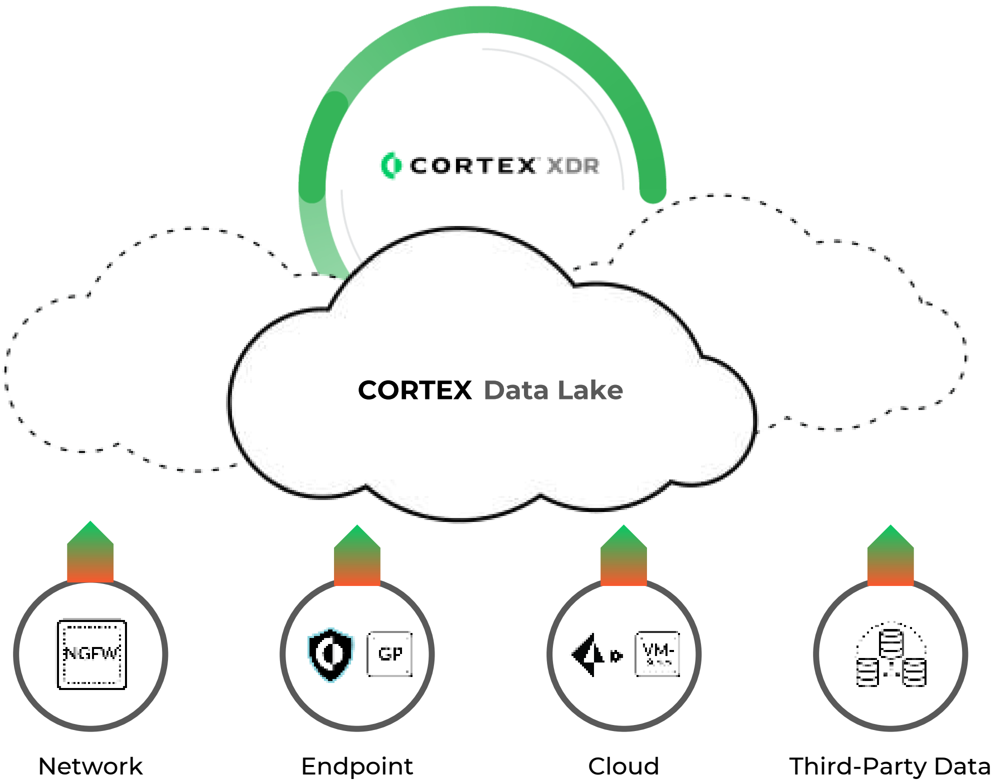
Gain unmatched forensic incident response experience from leading service providers

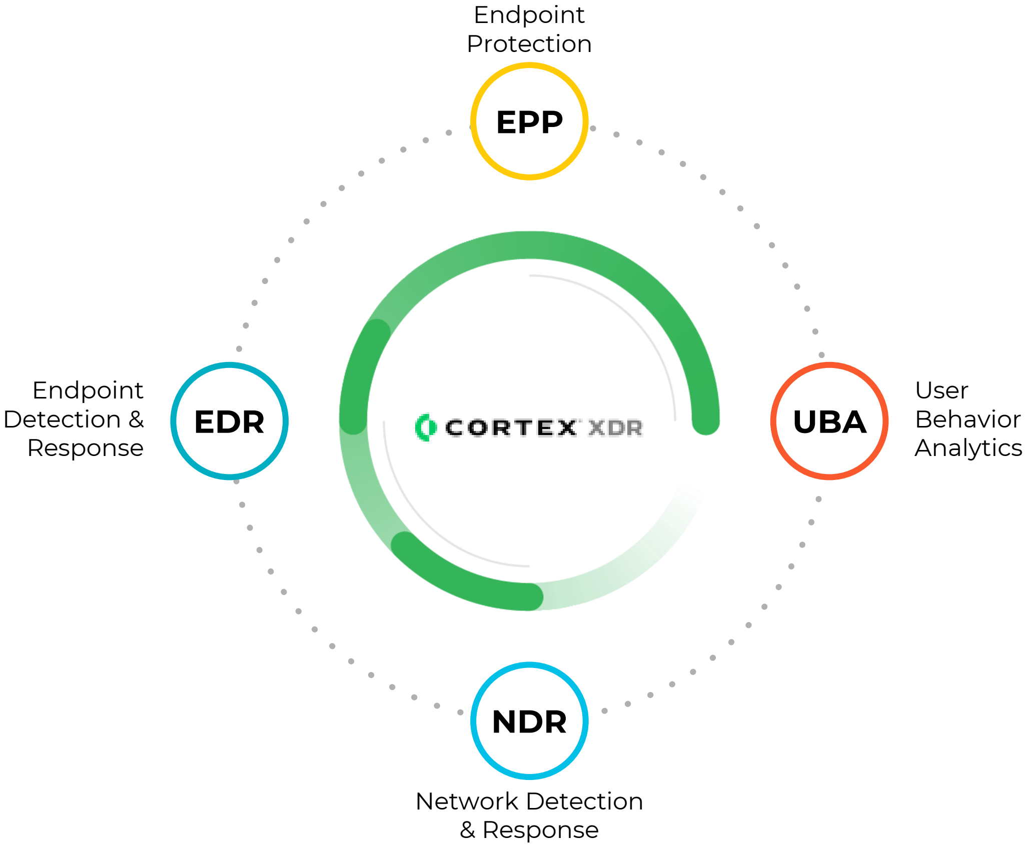
Budget to improve MTTD & MTTR

Achieve guaranteed <60 minute SLAs & ensure you are covered around the clock

CORTEX™ XDR

Key differentiators: **Gain enterprise-scale visibility**

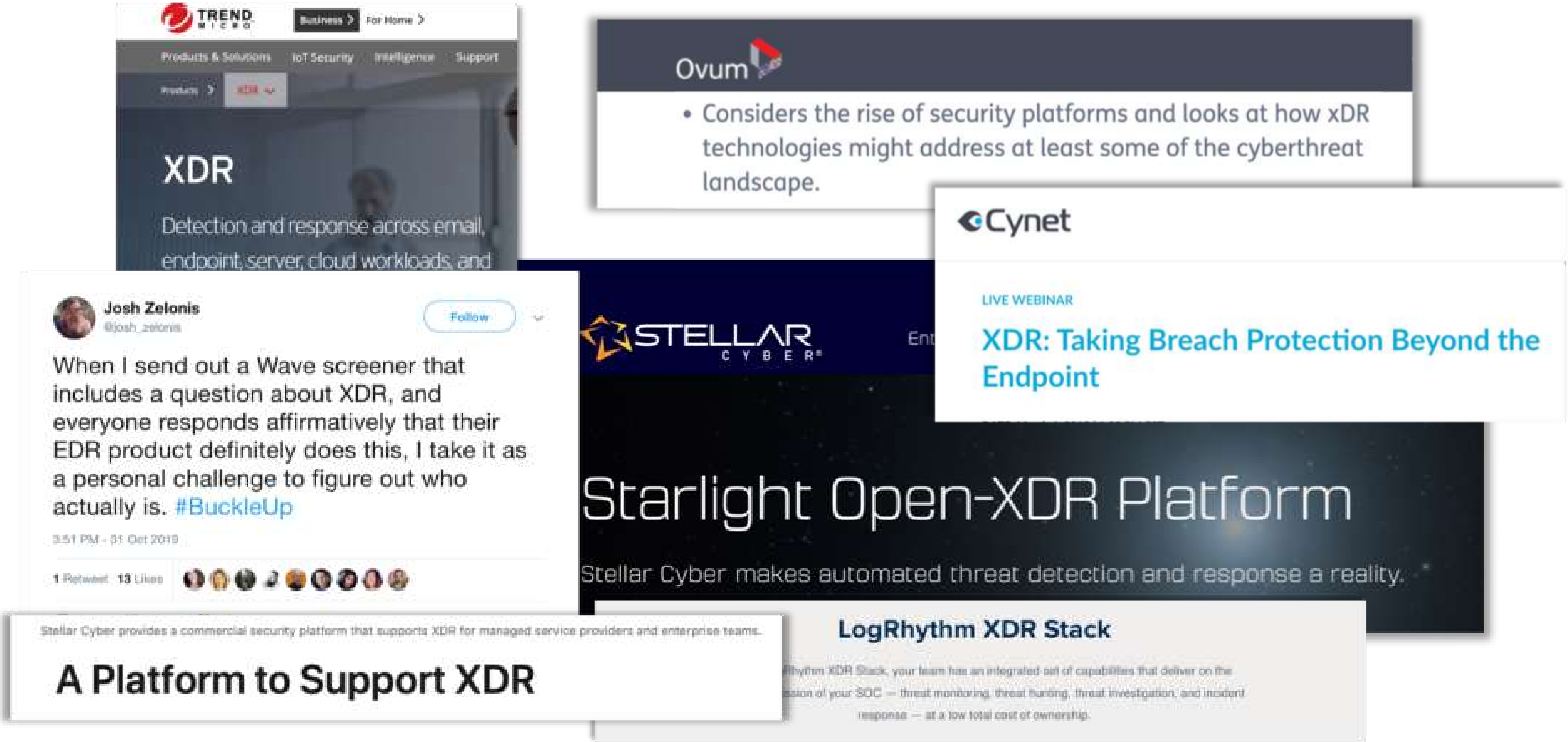




Our Approach: Breaking down data and product silos

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

XDR: Imitation is the Sincerest Form of Flattery



XDR

Detection and response across email, endpoint, server, cloud workloads, and

- Considers the rise of security platforms and looks at how xDR technologies might address at least some of the cyberthreat landscape.

LIVE WEBINAR

XDR: Taking Breach Protection Beyond the Endpoint

Starlight Open-XDR Platform

Stellar Cyber makes automated threat detection and response a reality.

Josh Zelonis
@josh_zelonis

When I send out a Wave screener that includes a question about XDR, and everyone responds affirmatively that their EDR product definitely does this, I take it as a personal challenge to figure out who actually is. #BuckleUp

3:51 PM - 31 Oct 2019

1 Retweet 13 Likes

Stellar Cyber provides a commercial security platform that supports XDR for managed service providers and enterprise teams.

A Platform to Support XDR

LogRhythm XDR Stack

Rhythm XDR Stack, your team has an integrated set of capabilities that deliver on the ssion of your SOC — threat monitoring, threat hunting, threat investigation, and incident response — at a low total cost of ownership.

Key differentiator: best-in-class prevention

Complete malware prevention

High fidelity local malware prevention trained by WildFire

Superior exploit protection

Stop attacks based on exploit techniques

Uncover and stop complex attacks

Analyzes multiple behaviors together to flag complex attacks

Key differentiator: find advanced attacks with analytics

Full visibility to detect complex threats

Eliminate blind spots across network, endpoint, and cloud

Patented behavioral analytics technology

Find hidden threats with a patented machine learning framework

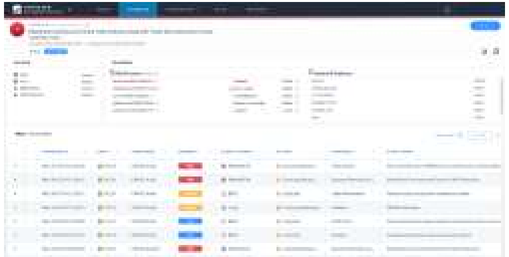
Industry-leading attack coverage

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

> “
>
> **The relief of knowing we are seeing actual viable data, information we could react to, and incidents we could follow up on. Now we can be ahead of the situation.**
>
> ”

Greg Biegen, Director of Information Security at Cherwell Software

Key differentiator: **supercharge investigation & response**

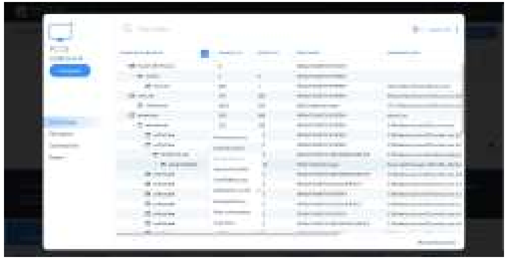


Unified Incident Engine

Intelligently group related alerts into one incident

Automated Root Cause Analysis

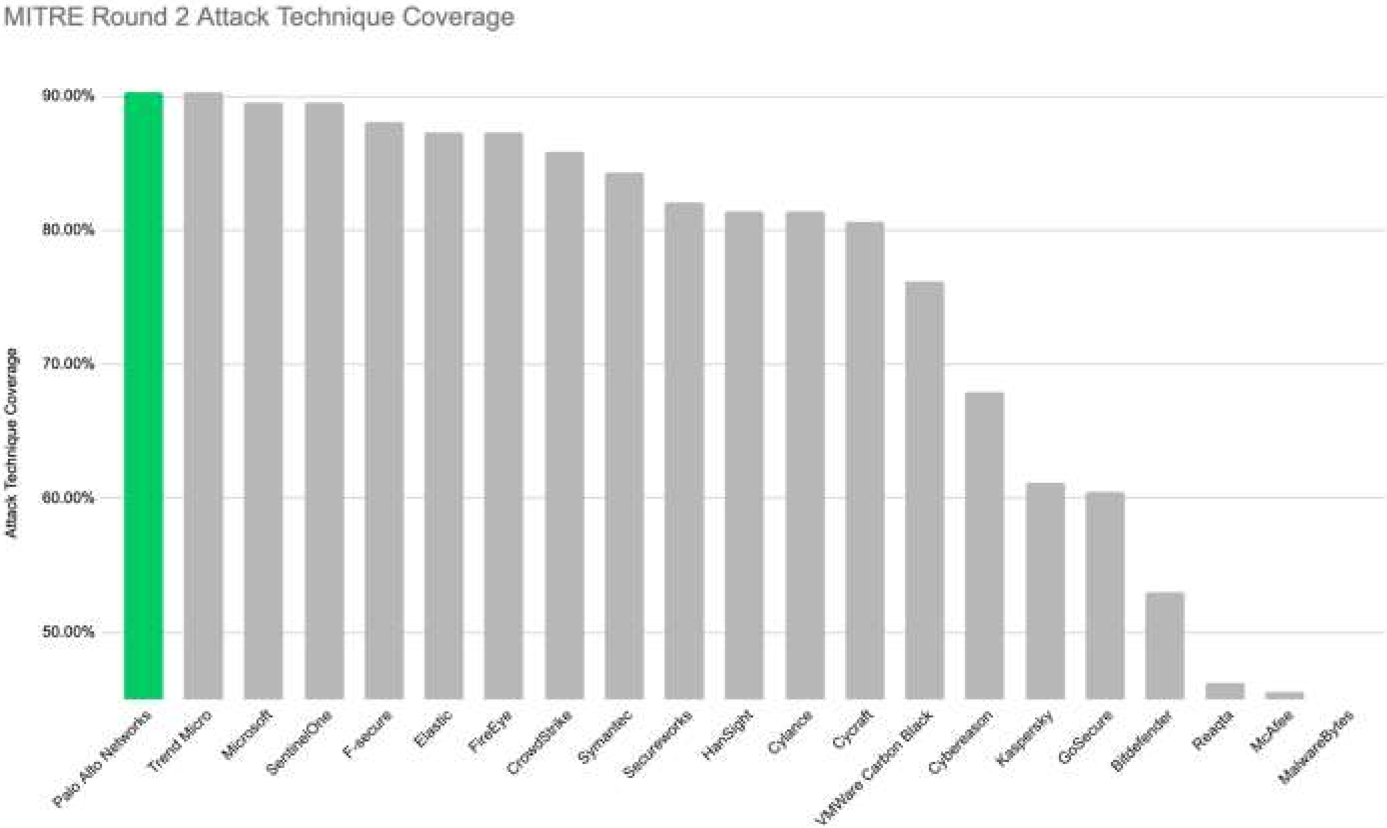
Reveal the root cause of attacks in one click



Integrated Response

Quick actions to contain attacks or run custom forensics

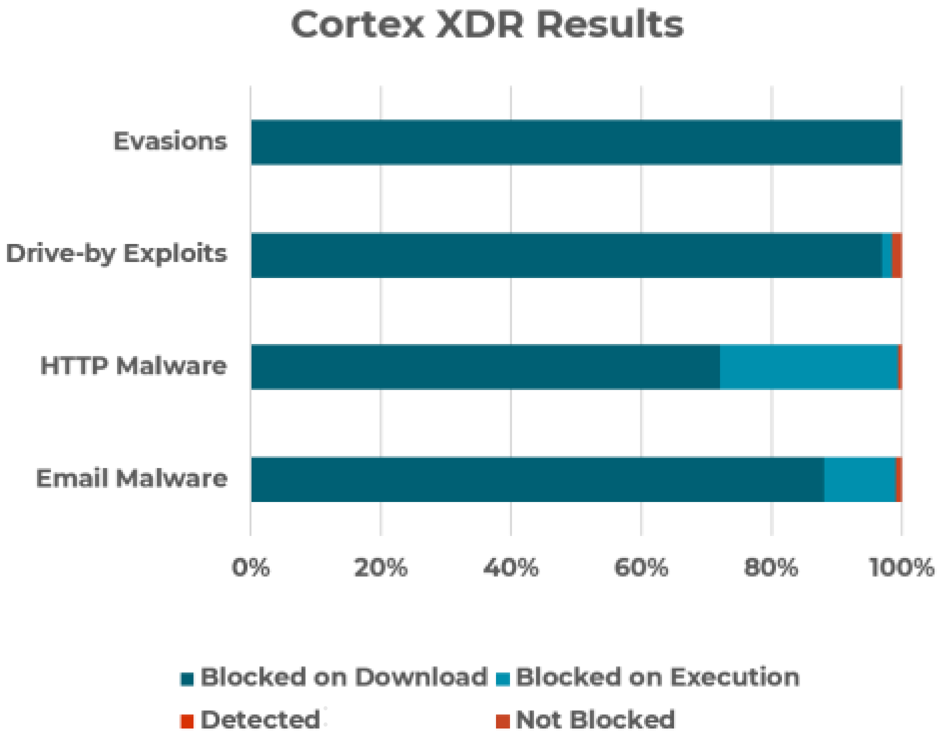
Cortex XDR MITRE ATT&CK coverage



Cortex XDR achieves "AA" rating in NSS Labs 2020 Test

NSS Labs assessment:

- Impressive overall protection with strong protection against malware, drive-by exploits, and offline infections.
- Excellent resistance to evasion.
- Low false positive rate.



Summary: Cortex XDR value

Reduce risk of a breach

Cut detection & response times 8x

Increase SecOps efficiency

Reduce alerts 50x with alert grouping

Maximize investments

Lower TCO by 44%

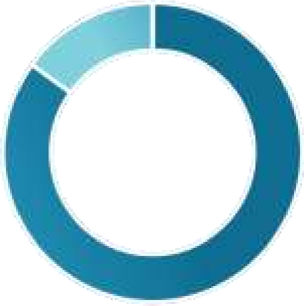
Palo Alto Networks: Better Together

The World’s Leading Cybersecurity Company

85

of Fortune 100

Rely on Palo Alto Networks



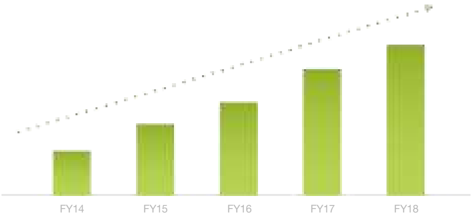
63% of the Global 2K

Are Palo Alto Networks Customers

#1

in Enterprise Security

Revenue trend 40% CAGR FY14 – FY18



29% Year-Over-Year

Revenue Growth

70,000

Customers

In 150+ Countries

J.D. POWER 2019 CERTIFIED ASSISTED TECHNICAL SUPPORT

tsia 2019 RATED OUTSTANDING PALO ALTO NETWORKS | GLOBAL ASSISTED SUPPORT

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

CORTEX
BY PALO ALTO NETWORKS

Thank you

paloaltonetworks.com

Email:

name@paloaltonetworks.com

Twitter: @PaloAltoNtwks

Additional Product Details

Cortex XDR 2.0: Raising the Bar for XDR

Third Party Data

Now analyzing Check Point, Cisco, and Fortinet, Logs

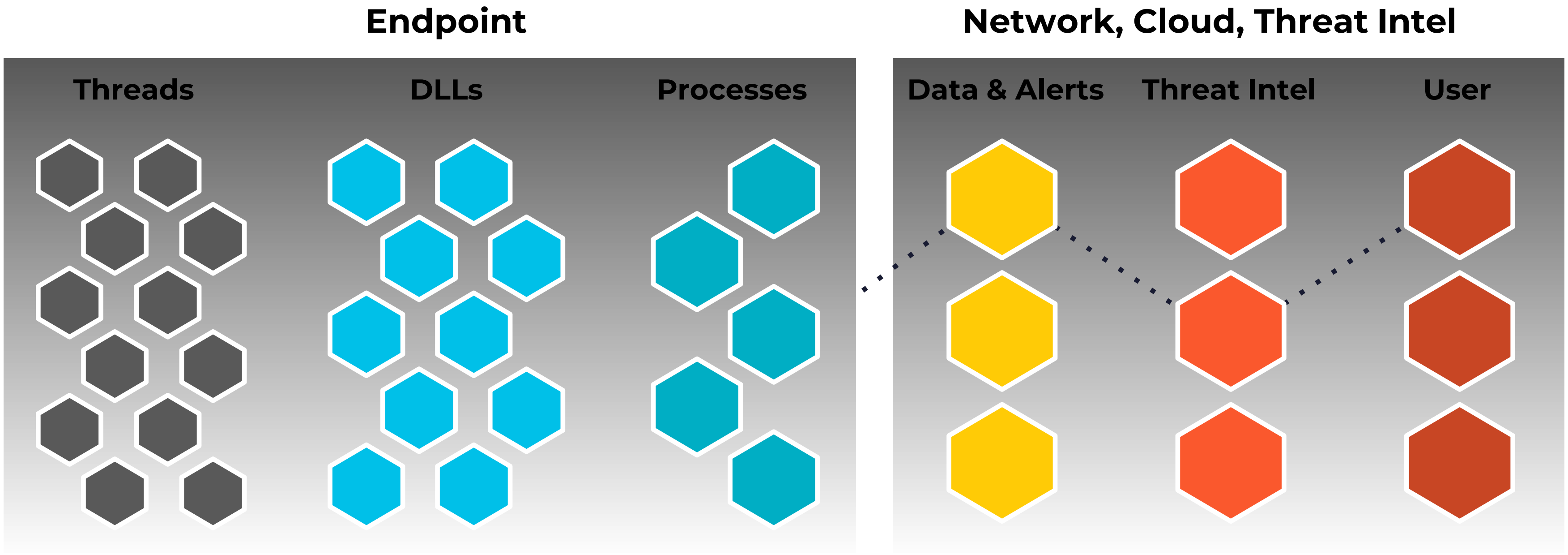
Fully Integrated Solution

Endpoint Protection now seamlessly integrated into XDR

ML-Driven Local Analysis

Delivered new local analysis engine 10X accuracy improvement

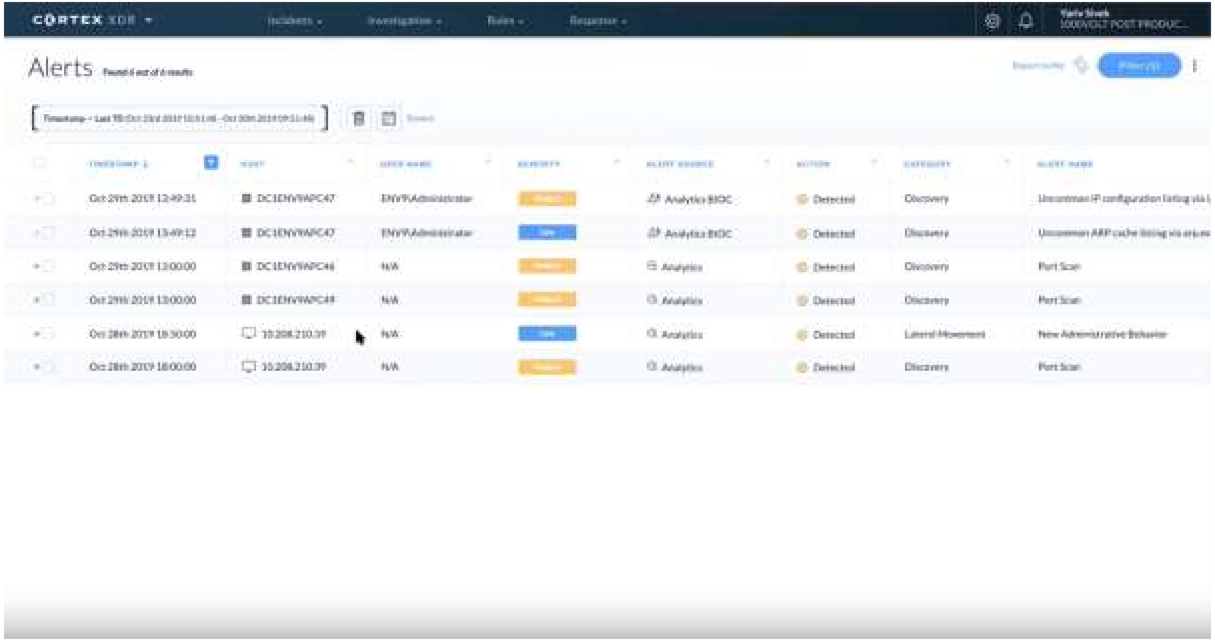
Integrate rich data for analytics & investigations



Identify the sequence of events with patented thread-level visibility

Integrate data to detect stealthy attacks and provide complete context

Opened up to third-party firewall logs



Alerts Found 6 out of 6 results

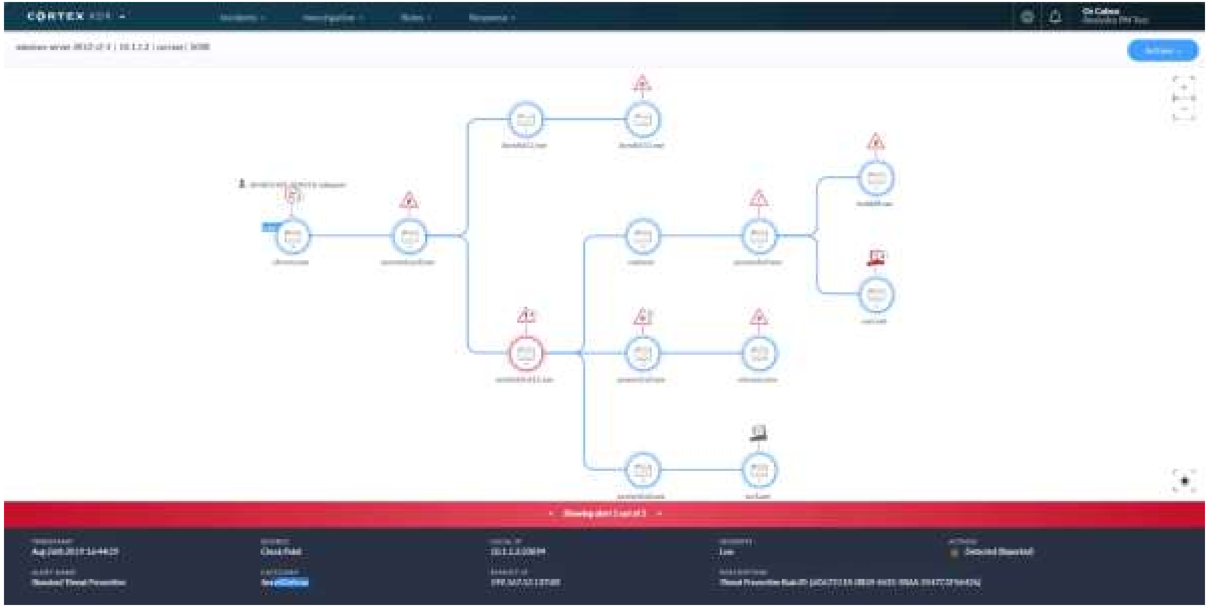
	TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY	ALERT NAME
□	Oct 29th 2019 12:49:21	DC1ENV9APC47	ENV9\Administrator	[illegible]	Analytics BIOC	Detected	Discovery	Uncommon IP configuration listing via i
□	Oct 29th 2019 13:49:12	DC1ENV9APC47	ENV9\Administrator	[illegible]	Analytics BIOC	Detected	Discovery	Uncommon ARP cache listing via arp.ex
□	Oct 29th 2019 13:00:00	DC1ENV9APC46	N/A	[illegible]	Analytics	Detected	Discovery	Port Scan
□	Oct 29th 2019 13:00:00	DC1ENV9APC48	N/A	[illegible]	Analytics	Detected	Discovery	Port Scan
□	Oct 28th 2019 18:30:00	10.208.210.39	N/A	[illegible]	Analytics	Detected	Lateral Movement	New Administrative Behavior
□	Oct 28th 2019 18:00:00	10.208.210.39	N/A	[illegible]	Analytics	Detected	Discovery	Port Scan

Check Point

CISCO

FORTINET

Opened up to third-party alerts



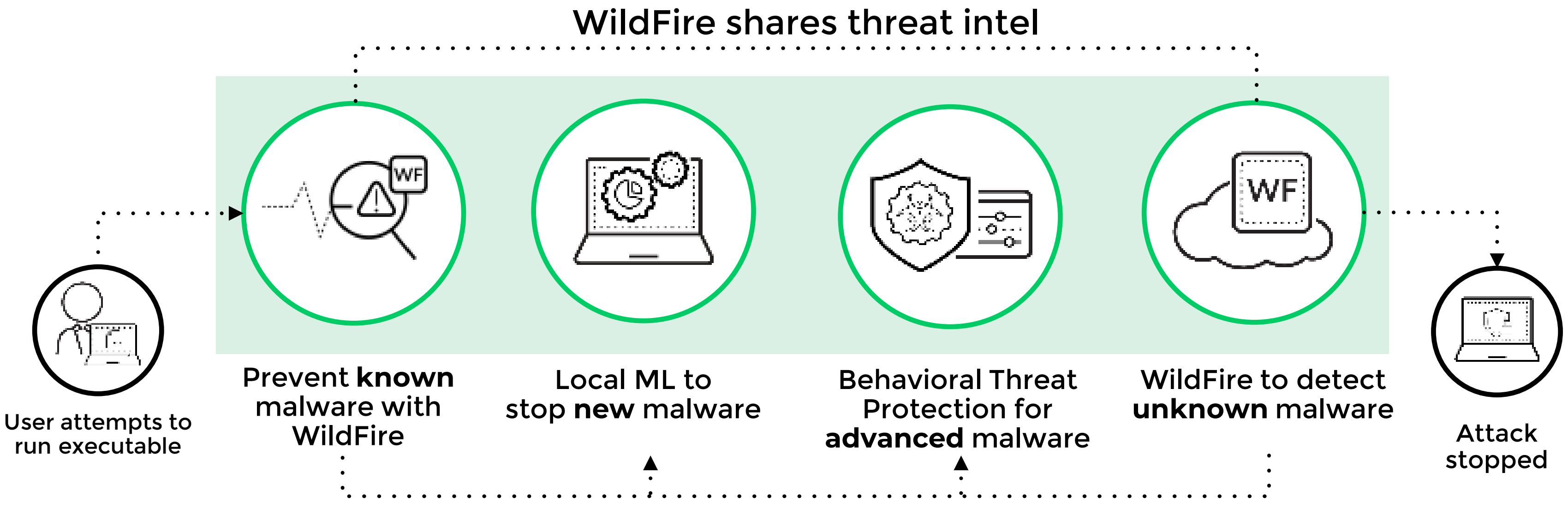
Any third-party firewall
Syslog CEF

Any network data in SIEM
Cortex XDR API

One attack story
Integrate alerts with deep endpoint and network data

Reduce alerts
Intelligently group all alerts into incidents

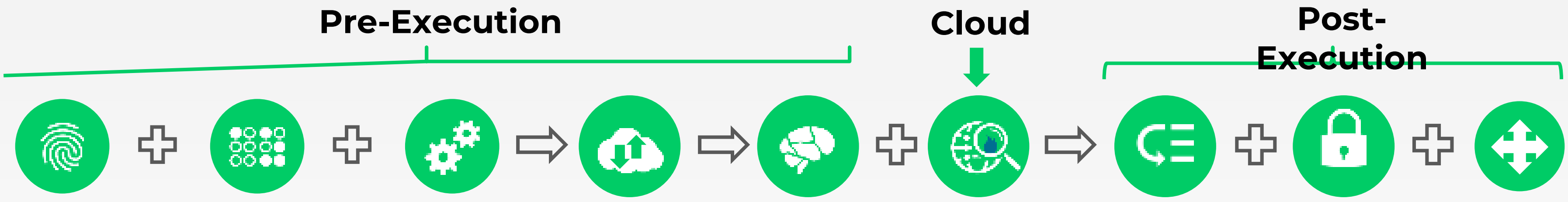
Prevent threats with the Cortex XDR agent


WildFire shares threat intel
WF
User attempts to run executable
Prevent **known** malware with WildFire
Local ML to stop **new** malware
Behavioral Threat Protection for **advanced** malware
WildFire to detect **unknown** malware
Attack stopped

Stop malware with local and cloud-based analysis

Block exploits by technique to prevent script-based & fileless attacks

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

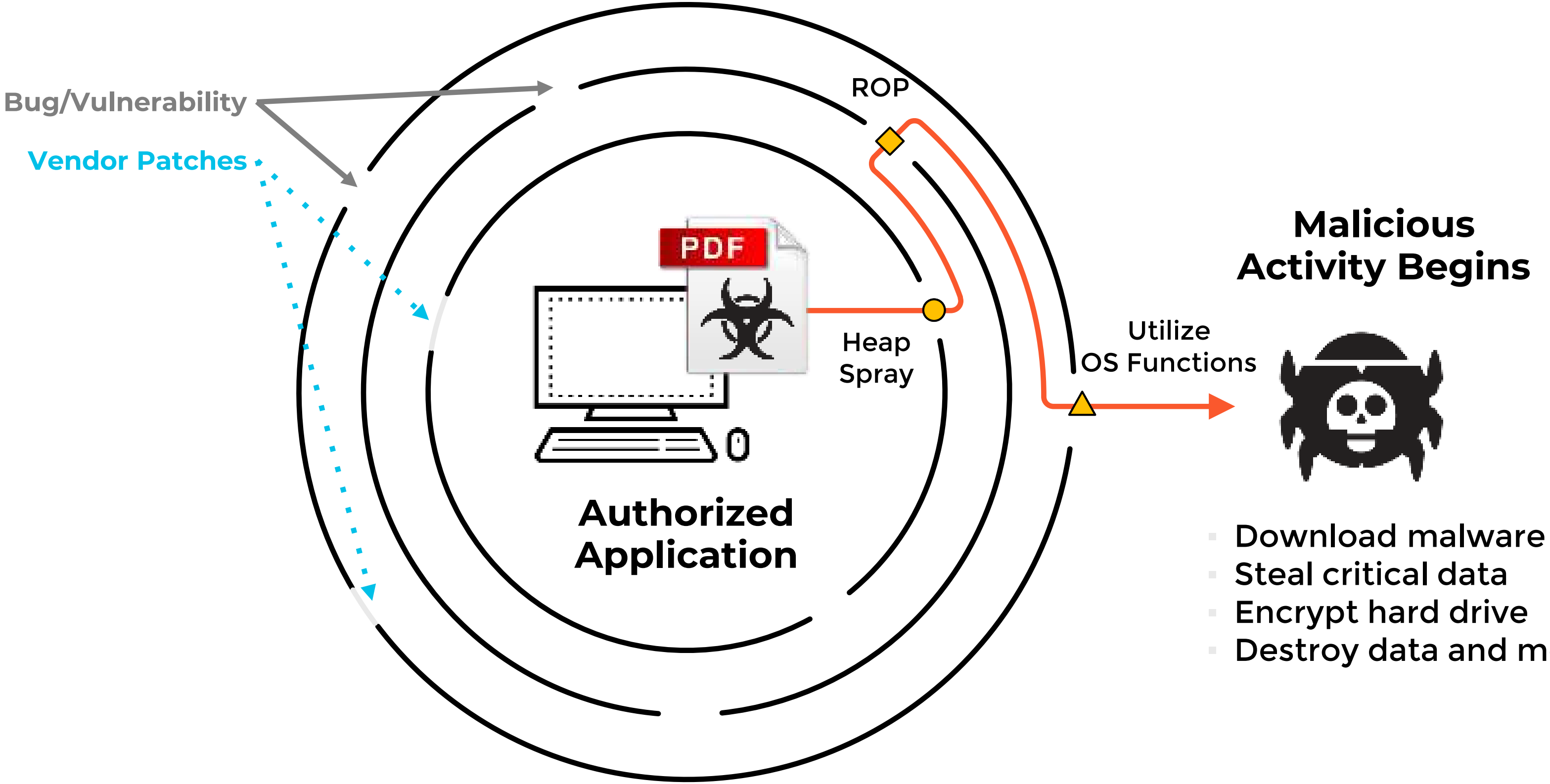
Stops attacks by analyzing chains of endpoint events

On and Offline Protection

Scheduled and On-Demand Scanning

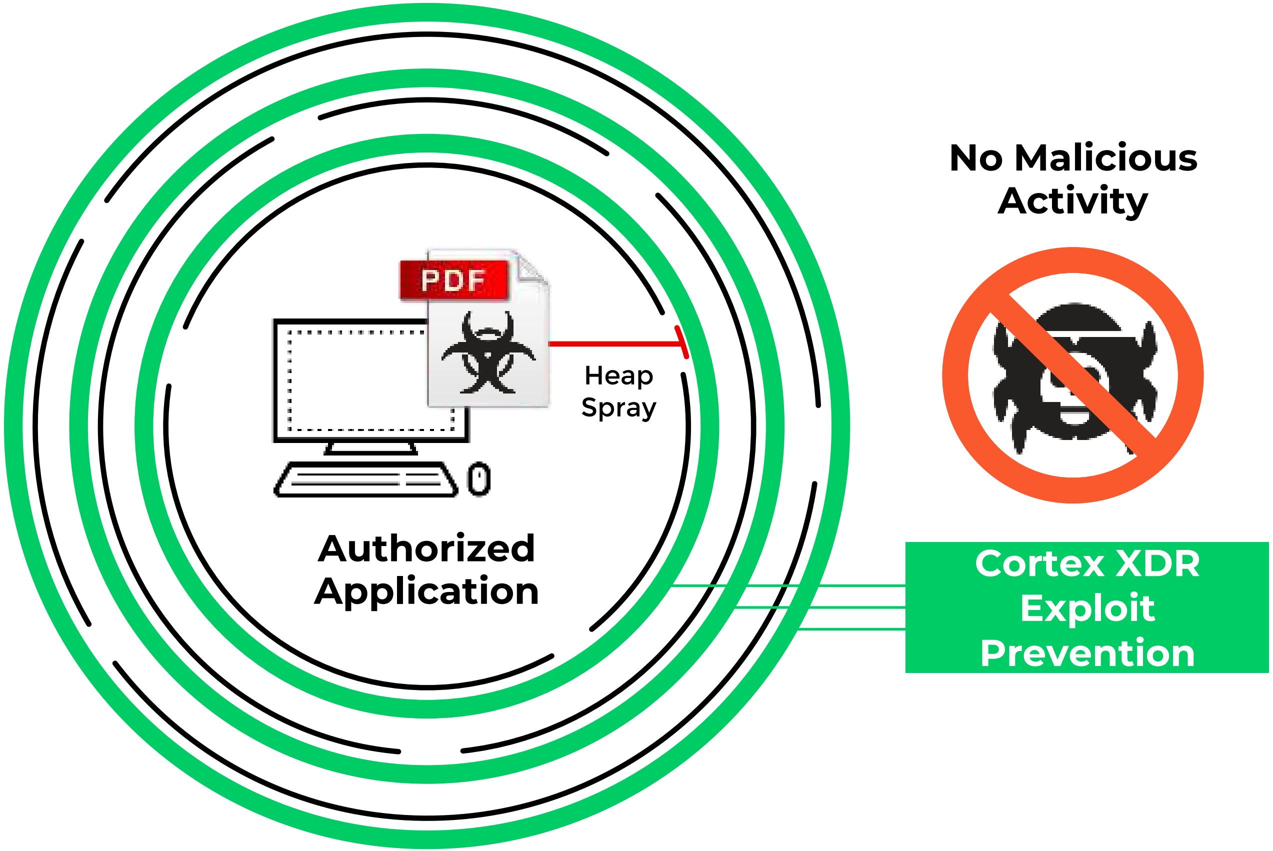
Cross-Platform Protection

Exploits Subvert Authorized Applications



- Download malware
- Steal critical data
- Encrypt hard drive
- Destroy data and more

Cortex XDR Blocks Exploits by Exploit Technique



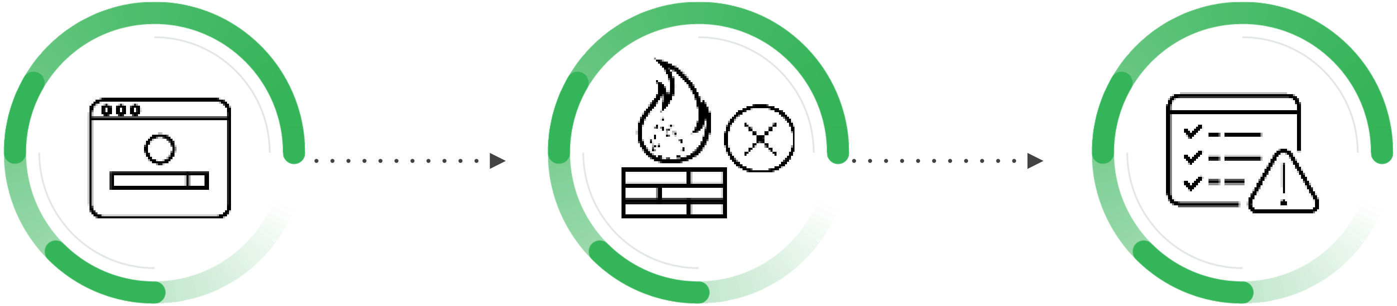
Authorized Application

No Malicious Activity

Cortex XDR Exploit Prevention

Behavioral Threat Protection: analyzing behaviors in context

Malicious sequence of events



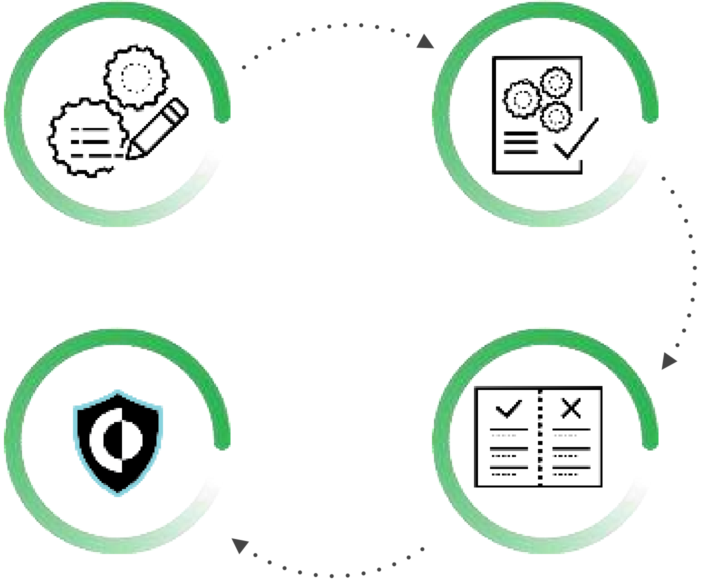
Process creates unsigned executable in "temp" directory

Process updates Windows firewall to allow malware to connect to the internet

New malware updates registry to disable a warning message

Analyze multiple behaviors together to uncover threats

Behavioral Threat Protection stops advanced attacks



BIOCs

Identify targeted attack on customer's endpoints

Silent BTP rules

Create new rules, collect telemetry and verify accuracy

BTP PREVENTION RULES

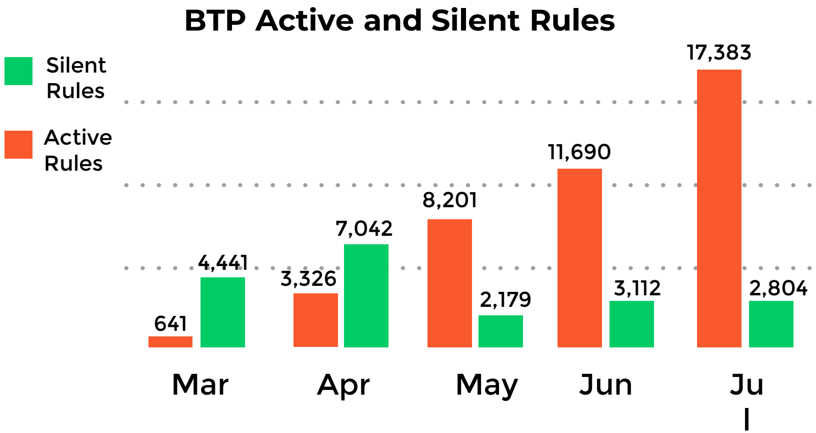
Stop active attacks with verified, automated new rules

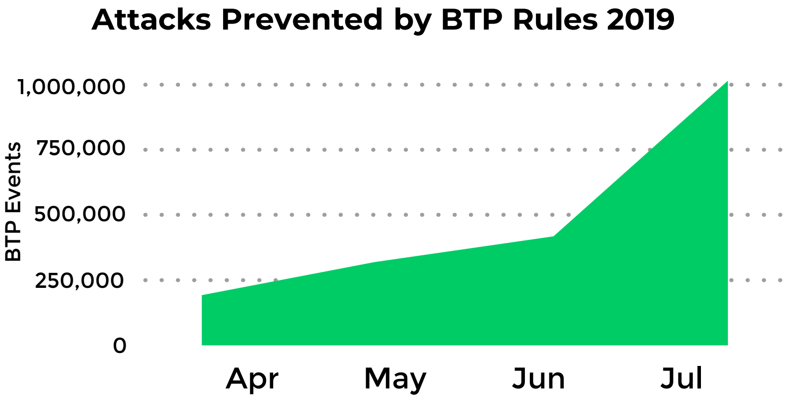
Cortex XDR Agent

Block threats on all globally deployed endpoints with shared protections

Detection to global prevention in less than 24 hours

Behavioral Threat Protection by the numbers





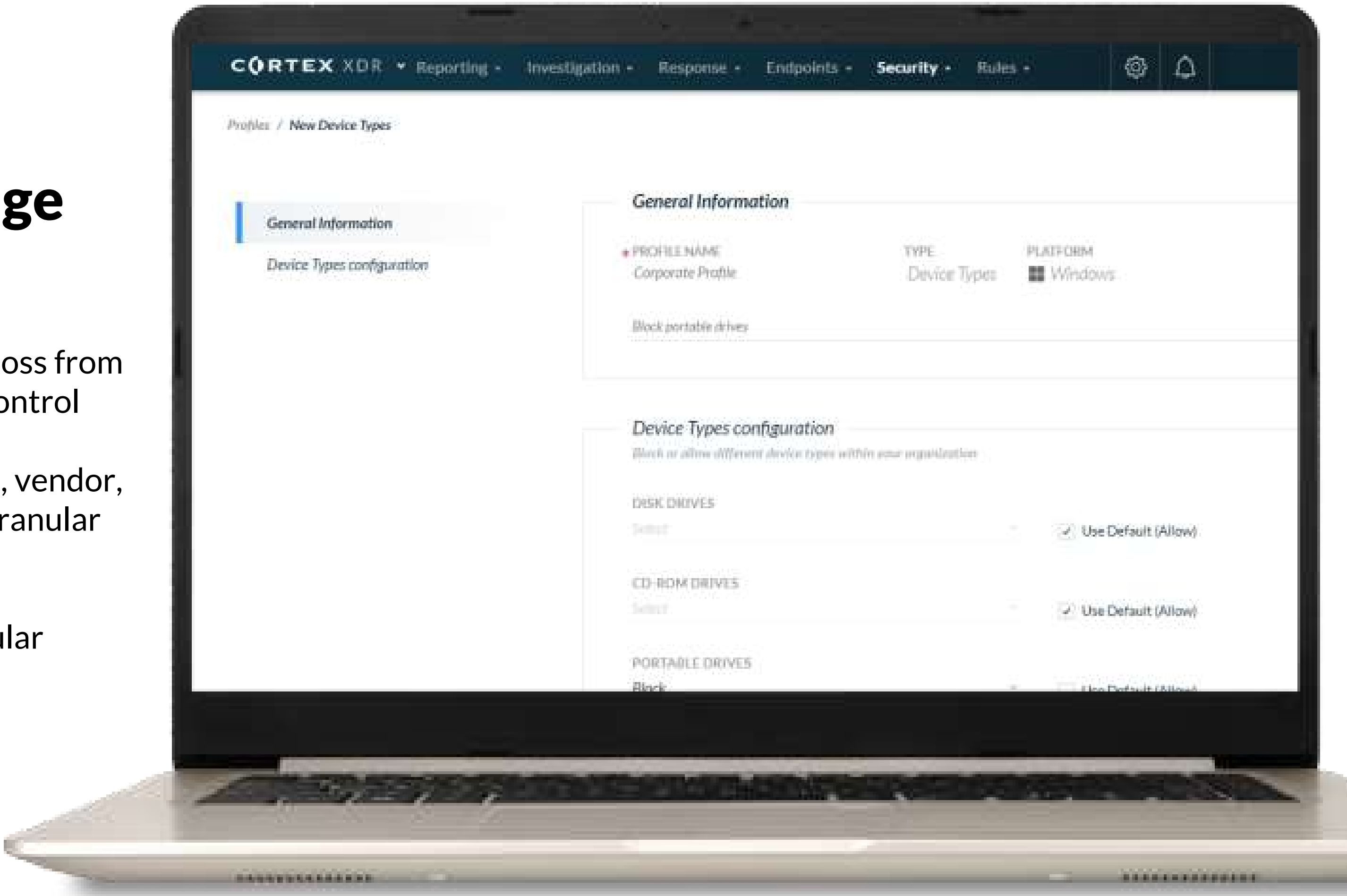
End-to-end automated process

Securely Manage USB Devices

Prevent malware and data loss from USB devices with Device Control

Restrict access by endpoint, vendor, and USB device type with granular control

Built on an extensible modular framework



General Information

* PROFILE NAME: Corporate Profile
TYPE: Device Types
PLATFORM: Windows

Block portable drives

Device Types configuration

Block or allow different device types within your organization

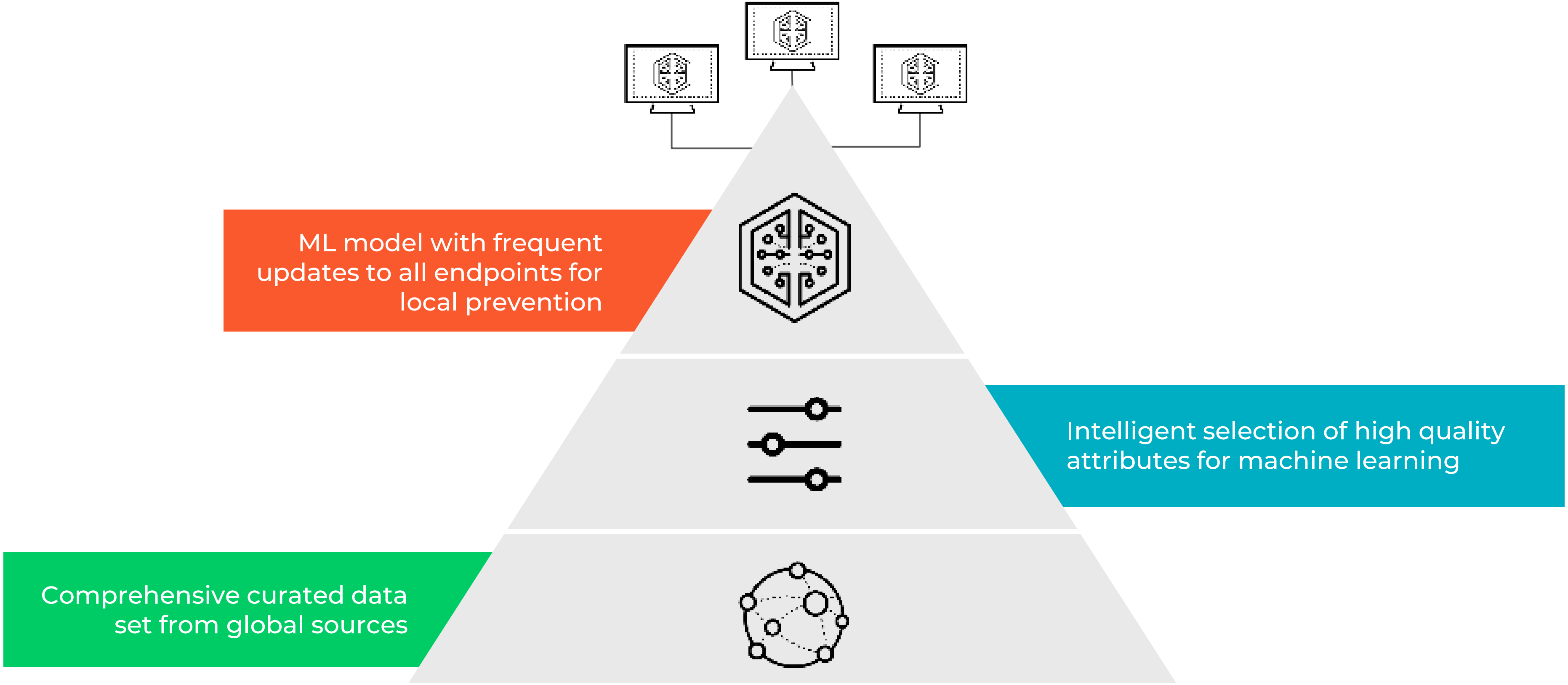
DISK DRIVES: Select — ✓ Use Default (Allow)

CD-ROM DRIVES: Select — ✓ Use Default (Allow)

PORTABLE DRIVES: Block — □ Use Default (Allow)

Learn globally, prevent locally

Best-in-class malware prevention rebuilt from the ground-up



ML model with frequent updates to all endpoints for local prevention

Intelligent selection of high quality attributes for machine learning

Comprehensive curated data set from global sources

Powerful Capabilities Introduced in Cortex XDR Agent 7.1

Script Execution

Host Firewall for Windows

Disk Encryption for Windows

File Scanning for MacOS

Improved Coverage for macOS in Cortex XDR Agent 7.2

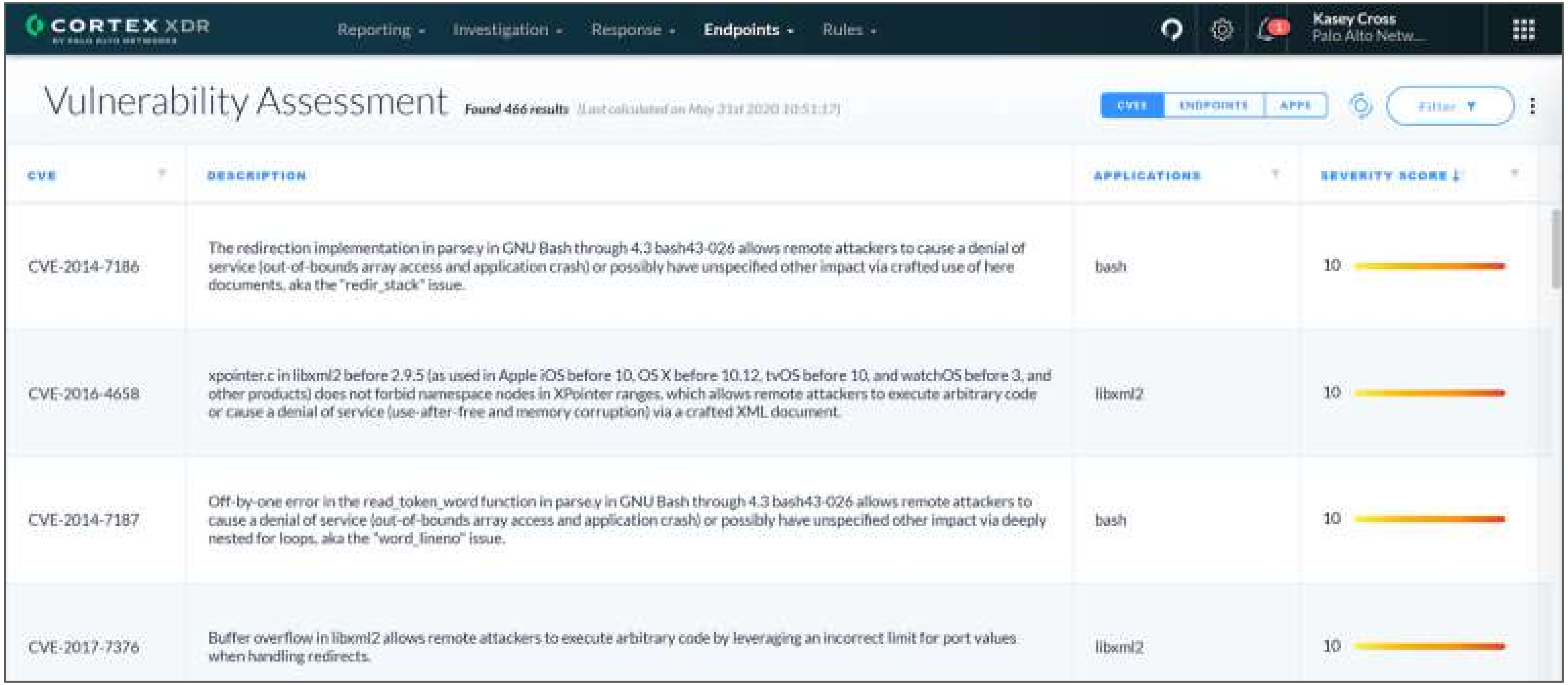
Device Control for macOS

Host Firewall for macOS

Disk Encryption for macOS via FileVault

DMG File Analysis

Vulnerability Assessment identifies and prioritizes your risks

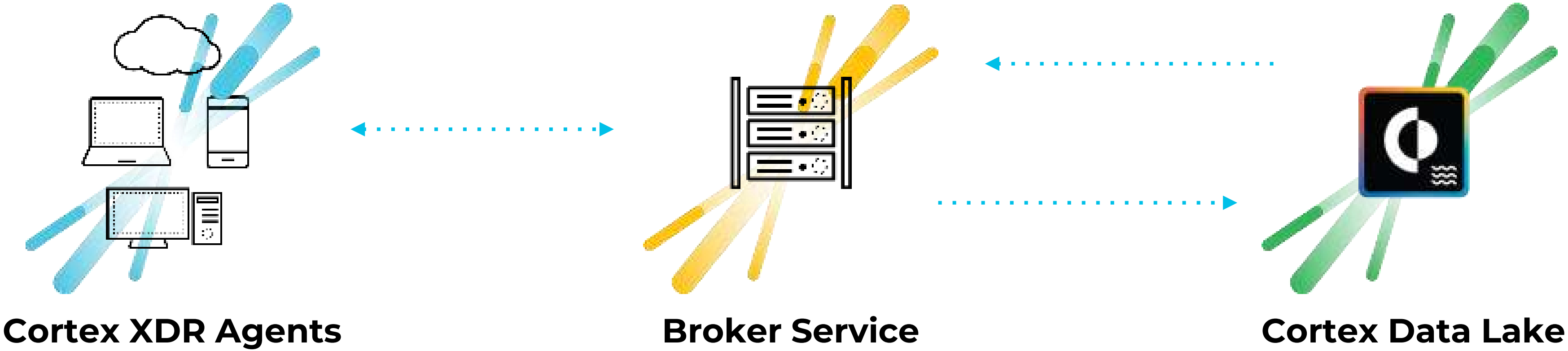


Vulnerability Assessment Found 466 results (Last calculated on May 31st 2020 10:51:17)

CVE	DESCRIPTION	APPLICATIONS	SEVERITY SCORE
CVE-2014-7186	The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the "redir_stack" issue.	bash	10
CVE-2016-4658	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.	libxml2	10
CVE-2014-7187	Off-by-one error in the read_token_word function in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via deeply nested for loops, aka the "word_lineno" issue.	bash	10
CVE-2017-7376	Buffer overflow in libxml2 allows remote attackers to execute arbitrary code by leveraging an incorrect limit for port values when handling redirects.	libxml2	10

- View all the vulnerabilities detected on your Linux endpoints by CVE or by host.
- Get up-to-date vulnerability data from the NIST National Vulnerability Database.

On-premises Broker Service for the Cortex XDR agent



Protect endpoints that can’t directly connect to the internet

Cortex XDR 2.0 product tiers

Cortex XDR Prevent

Complete endpoint protection

Cortex XDR Pro

Comprehensive prevention, detection, investigation, and response

30 days Cortex Data Lake retention included

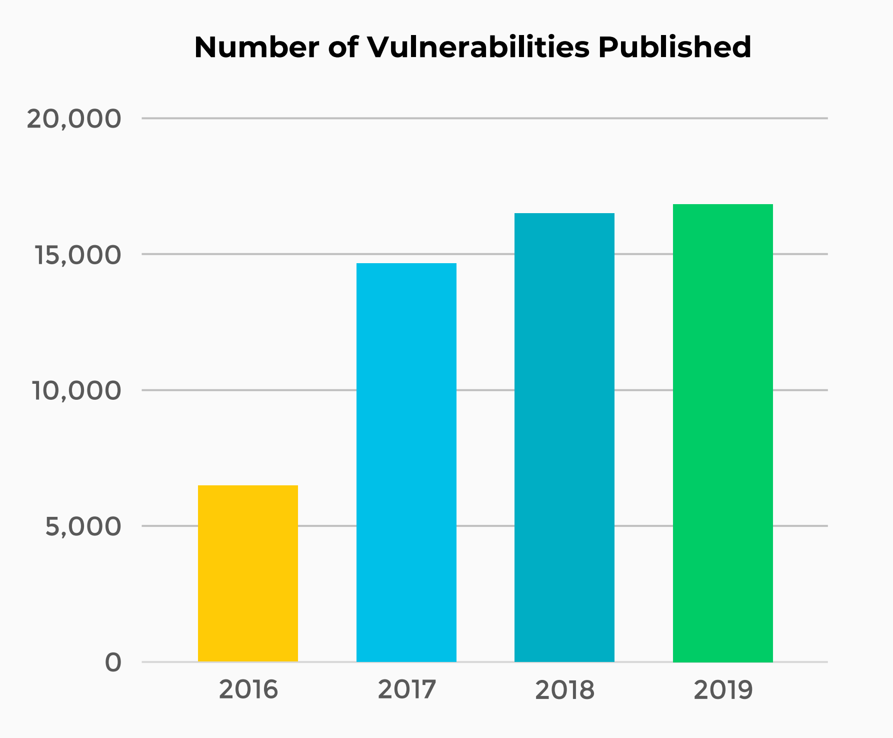
Cortex XDR Tiers

	Cortex XDR Prevent	Cortex XDR Pro
Data sources Get extended visibility across data sources	Endpoint	Endpoint, network, cloud and third-party products
Endpoint protection Stop malware, exploits, and fileless attacks	√	√
Device control Prevent data loss and USB-based malware infections	√	√
Disk encryption Directly manage BitLocker from the Cortex XDR console	√	√
Host firewall Reduce the attack surface on Windows endpoints	√	√
Vulnerability assessment Identify and prioritize risk and get application visibility	–	√
Behavioral analytics Detect emerging attacks with patented analytics and machine learning	–	√
Rule-based detection Find threats with out-of-the-box and custom rules	–	√
Accelerated investigation Cut investigation time 88% with root cause analysis and data stitching	–	√
Managed threat hunting Let Unit 42 experts uncover the most complex threats across data sources	–	Optional
Unified incident engine Reduce alert fatigue 50x by intelligently grouping alerts	Endpoint alerts	All alert sources
Integrated response Contain threats with multiple, flexible response options	Endpoint only	Endpoint and network response, script execution
Threat intelligence feed Enrich investigations with rich context from tens of thousands of customers	Optional	Optional
Alert retention	30 days	30 days
XDR data retention	–	Endpoint and network, 30 days
Extended data retention	Optional	Optional

How Cortex XDR Stops Emerging Attacks

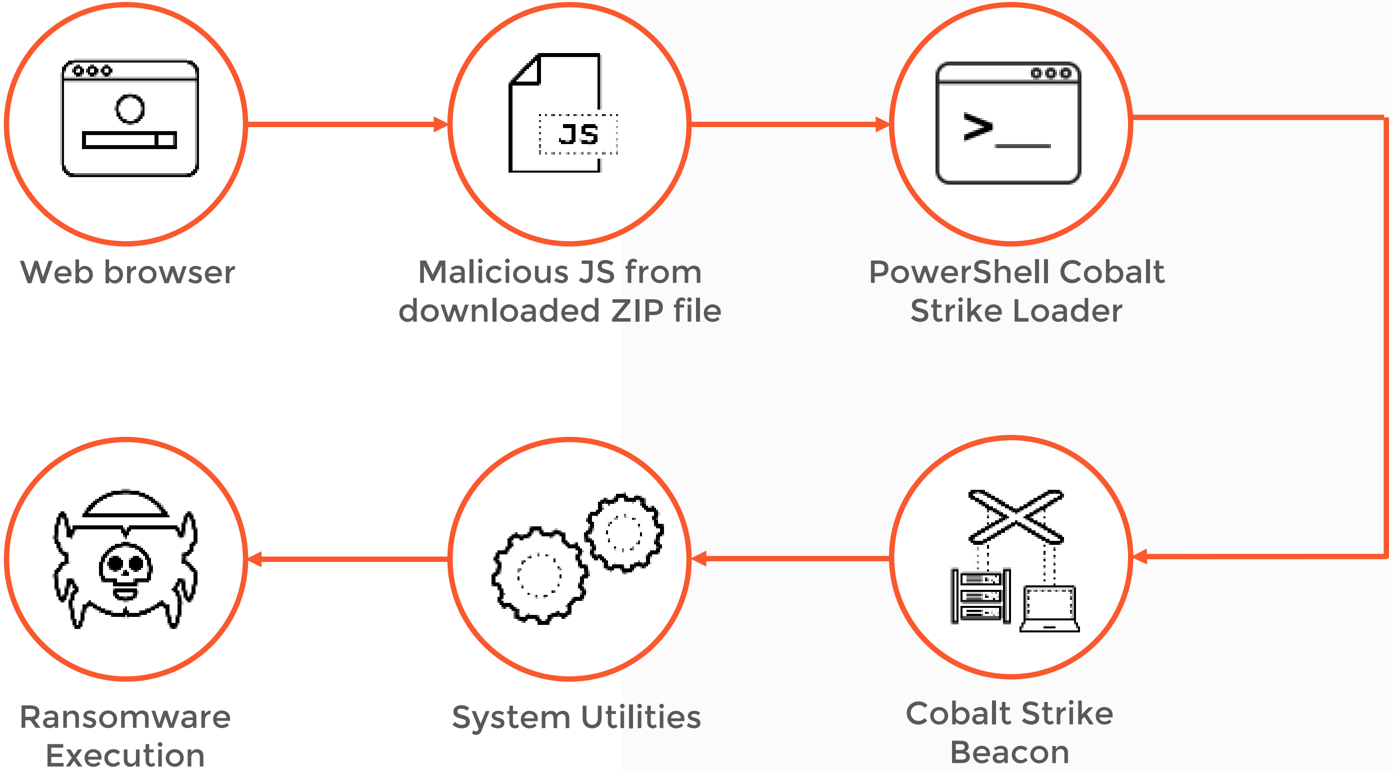
Trends in cyber attacks

- Number of vulnerabilities discovered per year is increasing x3 times compared to 3 years ago, despite Microsoft tightening the security in Windows 10
- Cross-platform (Go-based) malware–3x increase over last year
- Infected Word/Excel documents running PowerShell–5X compared to last year
- Continued investment in targeting POS machines for either credit card stealing or ransomware
- Increased focus on containerized environments



Sources: https://unit42.paloaltonetworks.com/the-gopher-in-the-room-analysis-of-golang-malware-in-the-wild/ Palo Alto Networks GSRT annual threat report, 2019

WastedLocker Attack Lifecycle



Web browser

Malicious JS from downloaded ZIP file

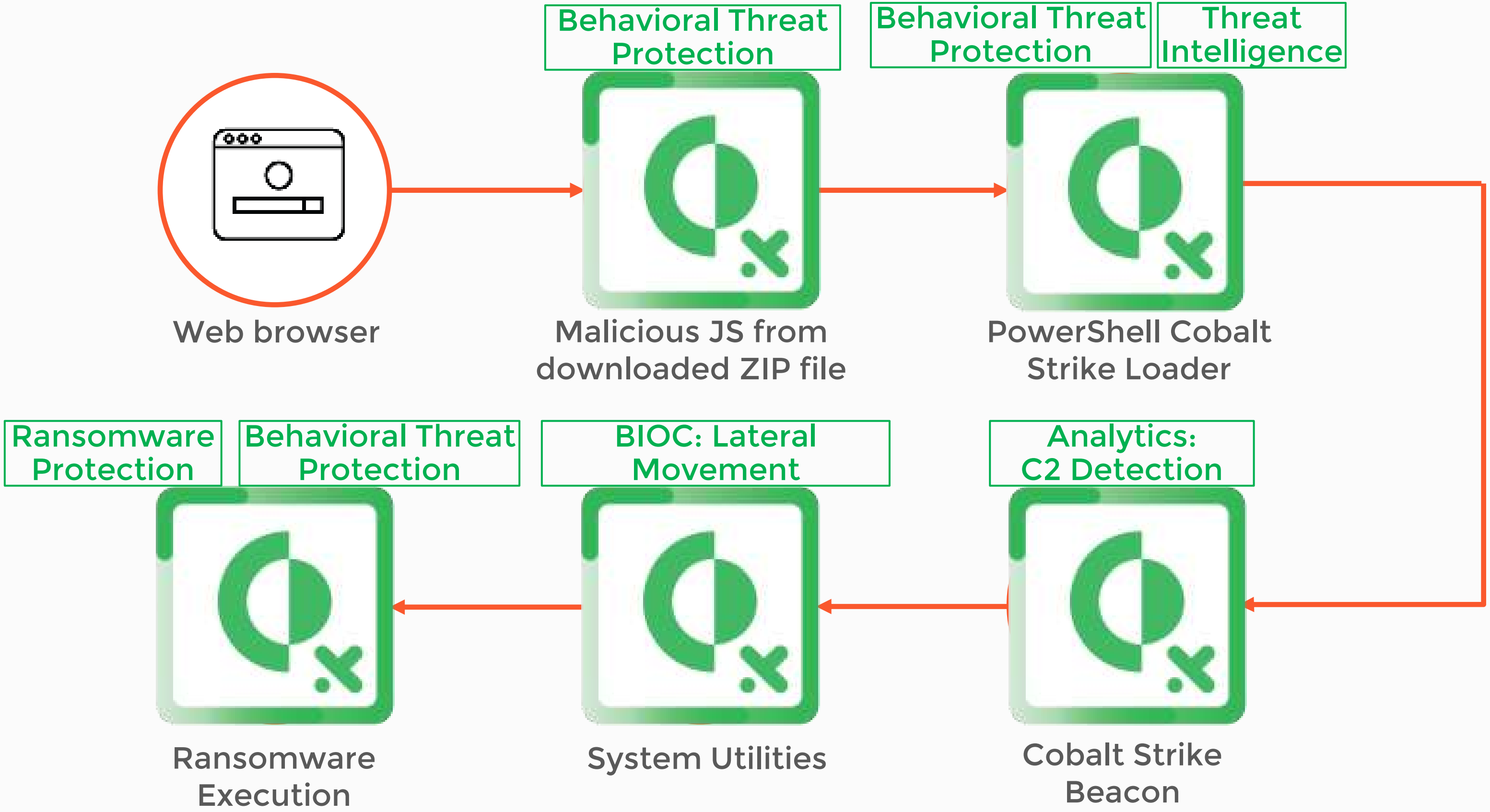
PowerShell Cobalt Strike Loader

Cobalt Strike Beacon

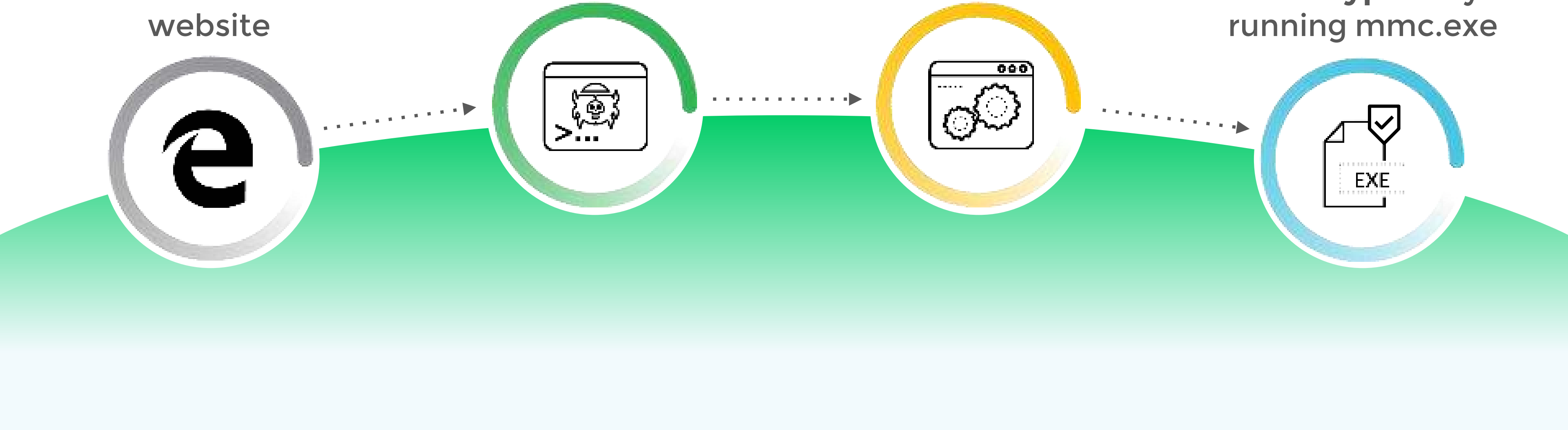
System Utilities

Ransomware Execution

Cortex XDR Stops WastedLocker at Every Step


Web browser
Behavioral Threat Protection
Malicious JS from downloaded ZIP file
Behavioral Threat Protection
Threat Intelligence
PowerShell Cobalt Strike Loader
Analytics: C2 Detection
Cobalt Strike Beacon
BIOC: Lateral Movement
System Utilities
Ransomware Protection
Behavioral Threat Protection
Ransomware Execution

North Korea-linked DarkHotel APT leverages zero-day exploit



Specific targeted users are directed to a malicious website

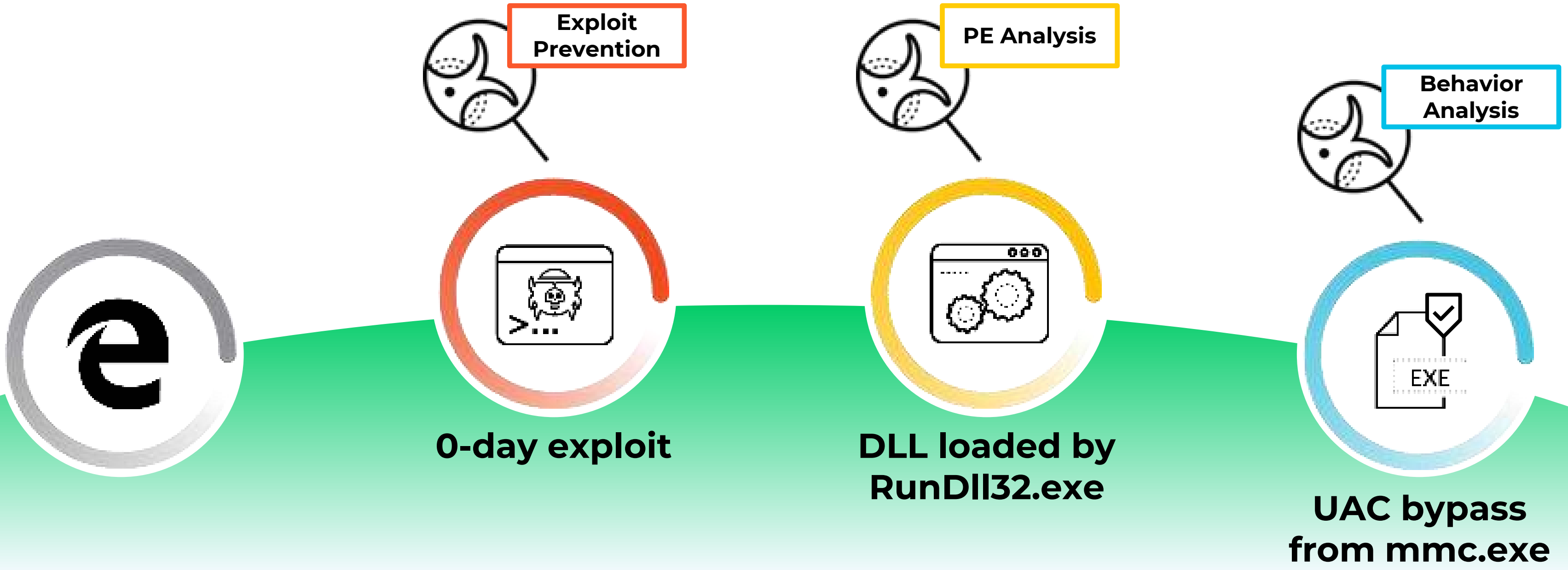
The returned webpage contains a **0-day exploits** in Adobe Flash

The exploits runs a **shellcode** that is used to download and run a DLL using RunDLL32.exe

The DLL runs a **UAC bypass** by running mmc.exe

explorer/

How does the Cortex XDR agent prevent this?



Exploit Prevention

PE Analysis

Behavior Analysis

0-day exploit

DLL loaded by RunDll32.exe

UAC bypass from mmc.exe

Sources: https://unit42.paloaltonetworks.com/unit42-traps-prevents-wild-vbscript-zero-day-exploit-internet-explorer/

COVID-19 Threat Landscape

What are we seeing?

Phishing and malware distributed using COVID-19 related themes

Advisories, Tips, Cures, Etc.

Fake COVID-19 apps for Android

COVID-19 related domains and websites for scams and phishing

Fake stores selling masks and other supplied.

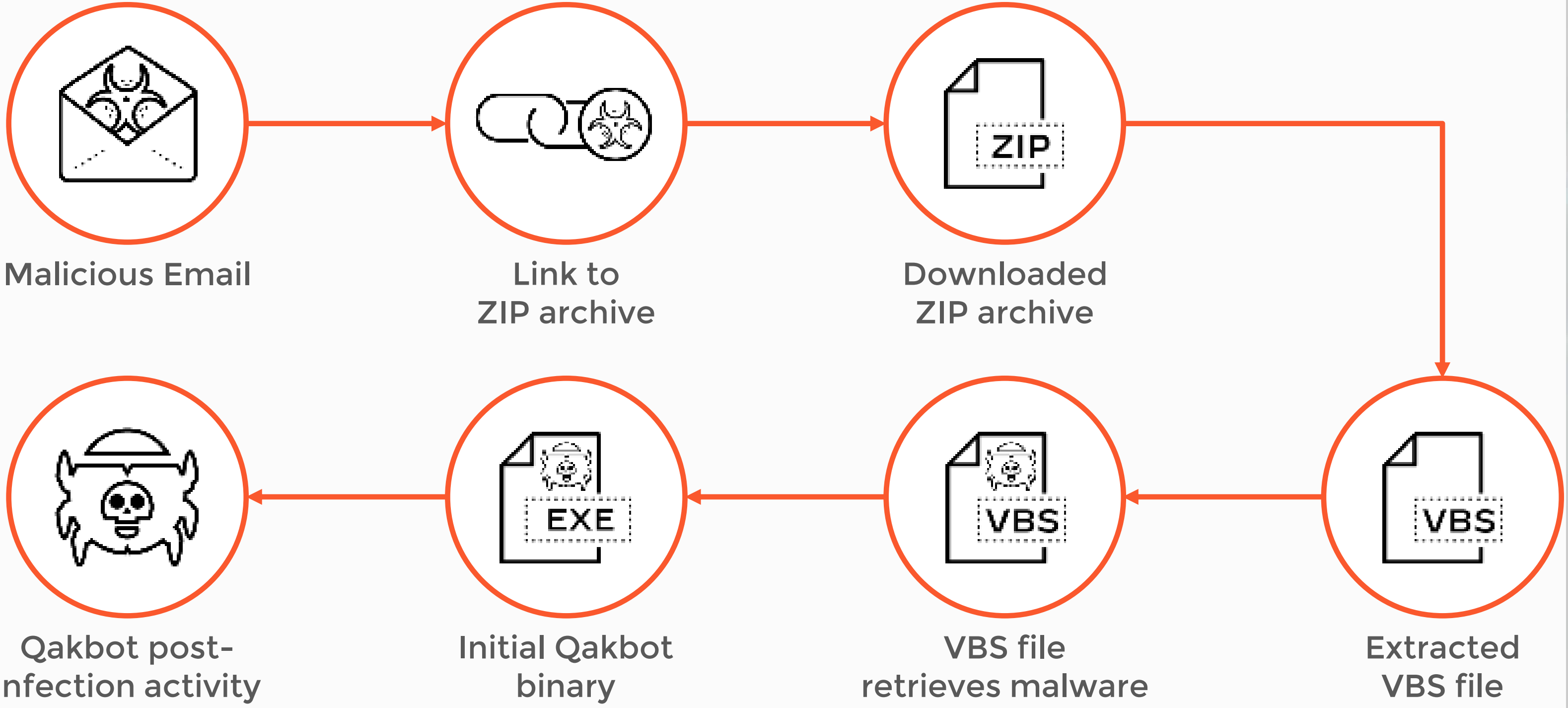
Illicit pharmacy websites selling remedies

Attempted ransomware attacks

Canadian Universities and Hospitals

“The biggest opportunity for cyber attackers with this outbreak has nothing to do with technology, but with **how humans change their behavior** and patterns in response to the crisis.”

Qakbot Infection Delivery



Malicious Email

Link to ZIP archive

Downloaded ZIP archive

Extracted VBS file

VBS file retrieves malware

Initial Qakbot binary

Qakbot post-infection activity

Behavioral Analytics

Why You Need Network Traffic Analysis

Lack of visibility into internal network traffic

Limited monitoring of east-west traffic, VPN users, unmanaged devices & IoT

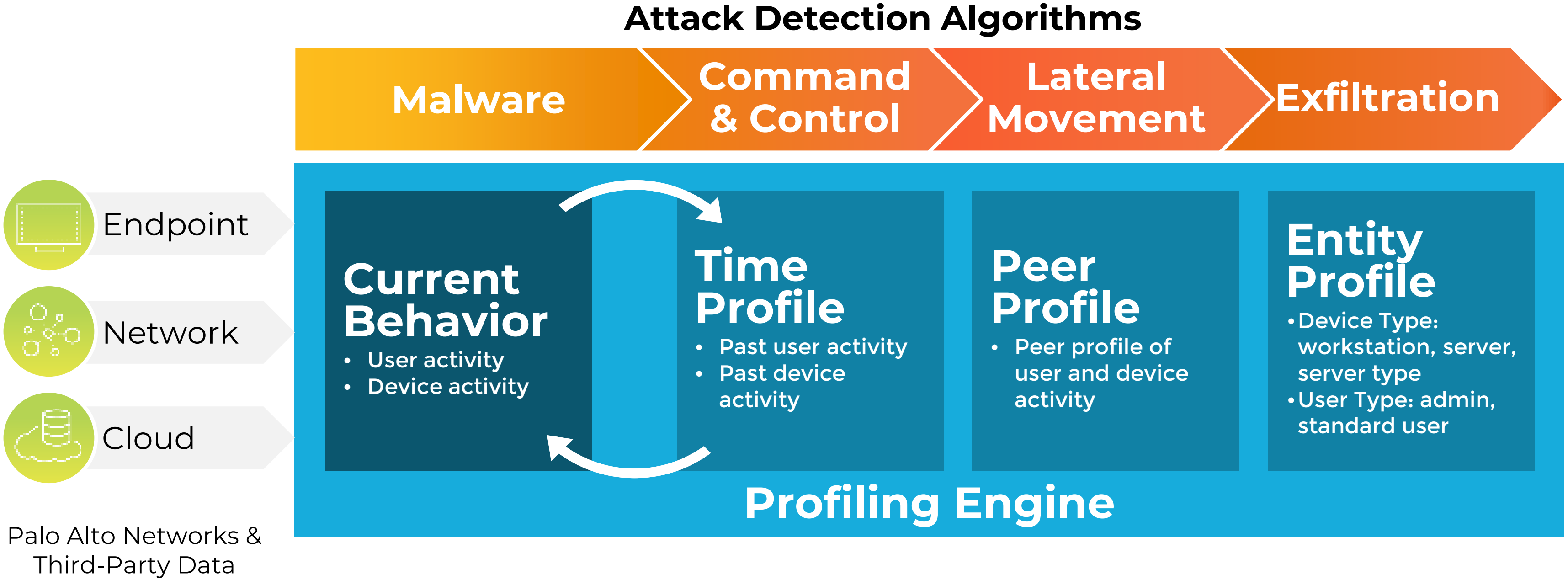
Inability to find active attacks

No AI or behavioral analytics to find low and slow attacks & lateral movement

Limited hunting based on network data

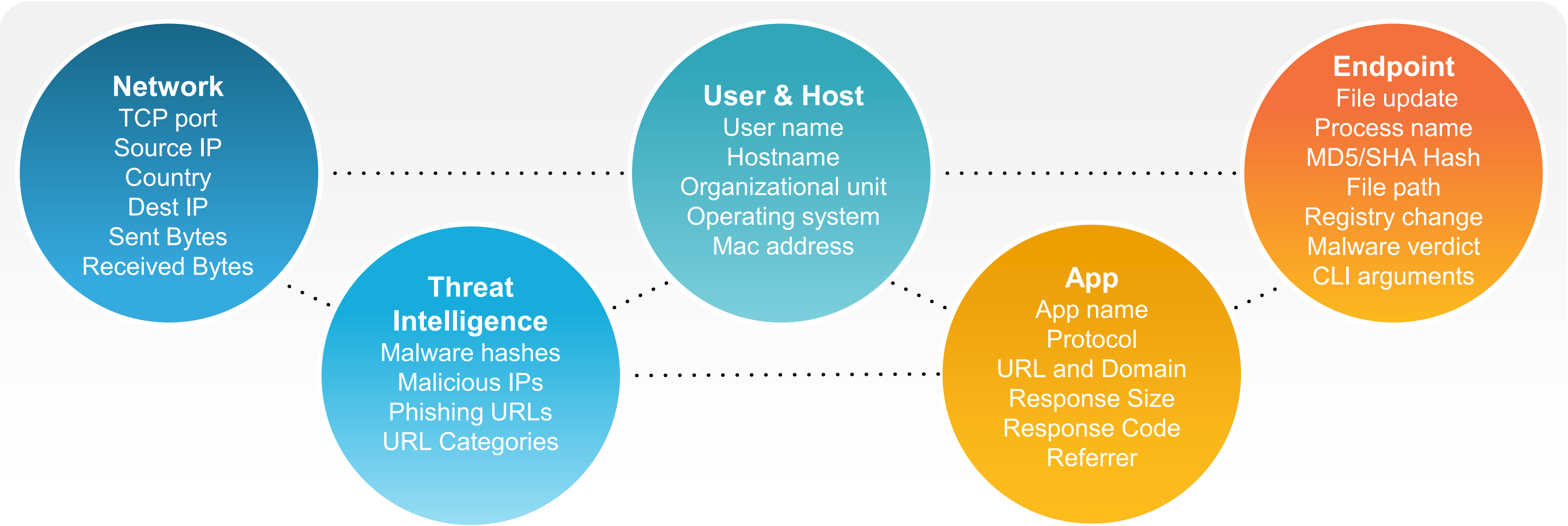
Cannot use network data for detection or searches

Automatically Detect Attacks with Machine Learning



Profile behavior & detect anomalies indicative of an attack

Collect and Correlate Data



Network
TCP port
Source IP
Country
Dest IP
Sent Bytes
Received Bytes

Threat Intelligence
Malware hashes
Malicious IPs
Phishing URLs
URL Categories

User & Host
User name
Hostname
Organizational unit
Operating system
Mac address

App
App name
Protocol
URL and Domain
Response Size
Response Code
Referrer

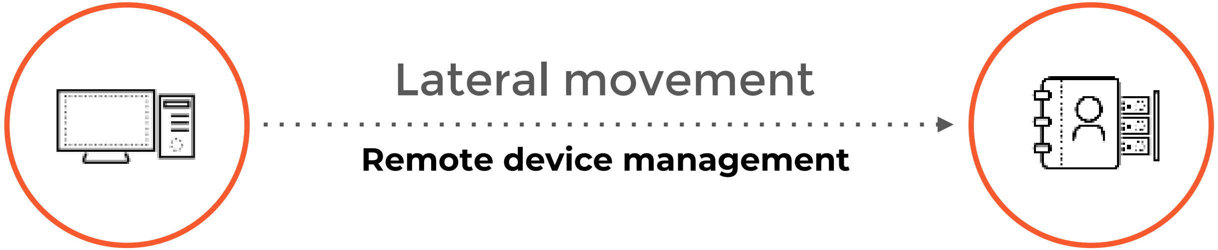
Endpoint
File update
Process name
MD5/SHA Hash
File path
Registry change
Malware verdict
CLI arguments

Collect rich data for behavioral analytics & AI

Automatically correlate data to gain context for investigations

Uncover stealthy threats with AI & machine learning

High Signal Alert



Lateral movement

Remote device management

- Windows PC, standard user (not IT admin)
- 2 GB traffic a day, 30 destinations, no admin protocols

- Active Directory server
- 25 GB traffic a day, 500 destinations

1

Automatically classify all devices and users

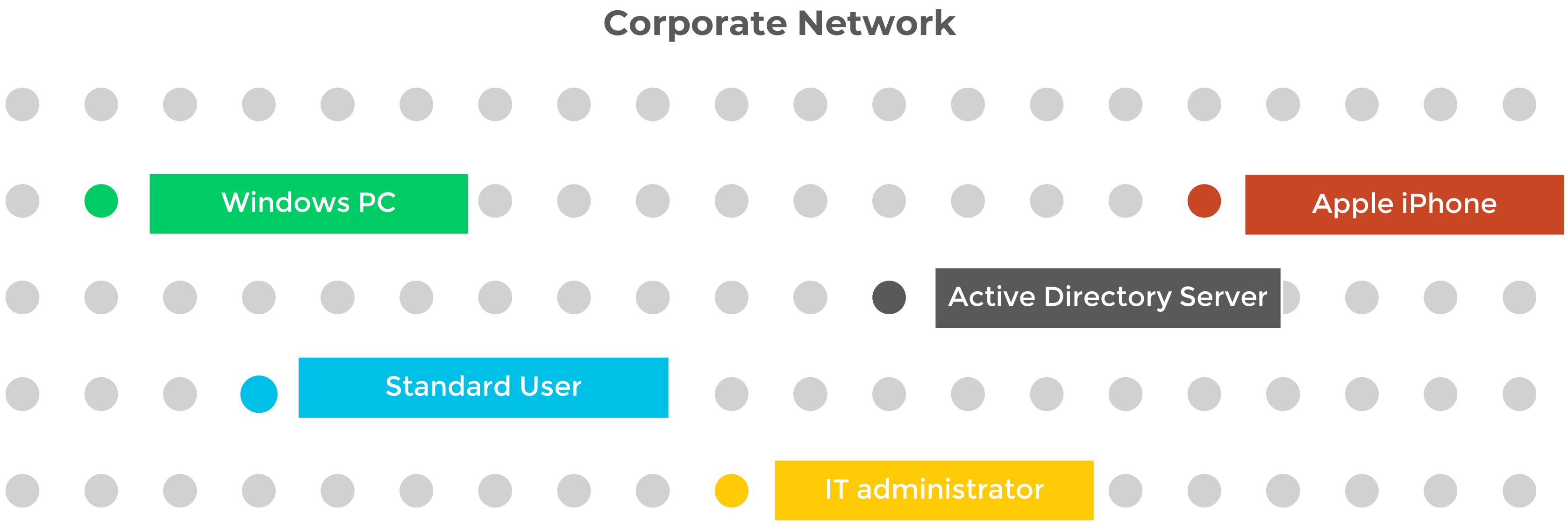
2

Profile 100s of types of behaviors over days & weeks

3

Accurately detect anomalies indicative of attack

Automatically detect attacks with behavioral analytics

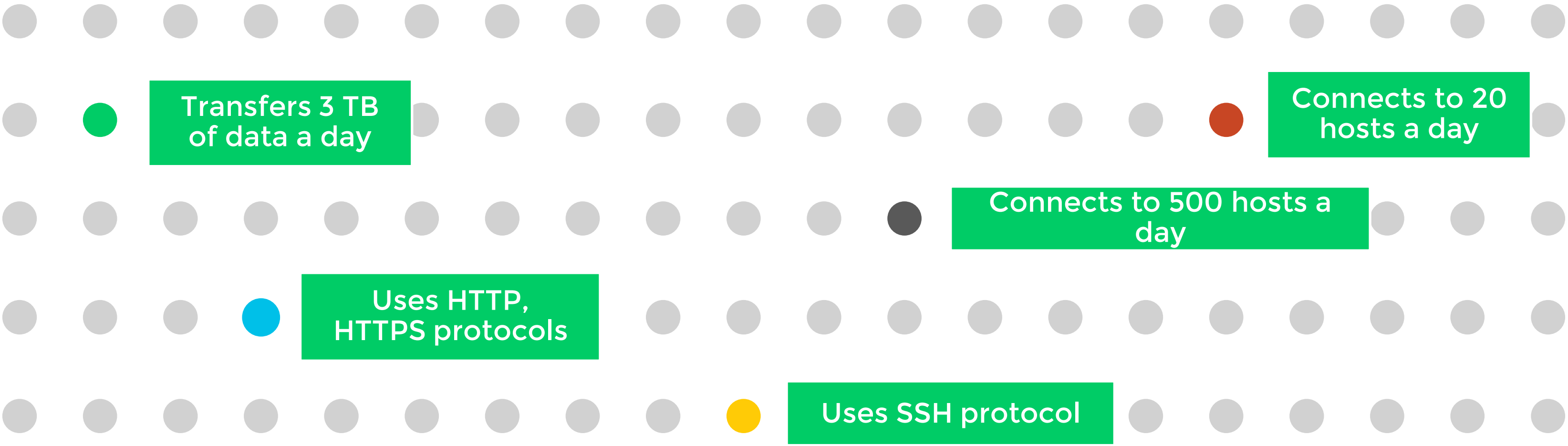


1

Identify types of users & devices by analyzing activity

Automatically detect attacks with behavioral analytics

Corporate Network



Transfers 3 TB of data a day

Connects to 20 hosts a day

Connects to 500 hosts a day

Uses HTTP, HTTPS protocols

Uses SSH protocol

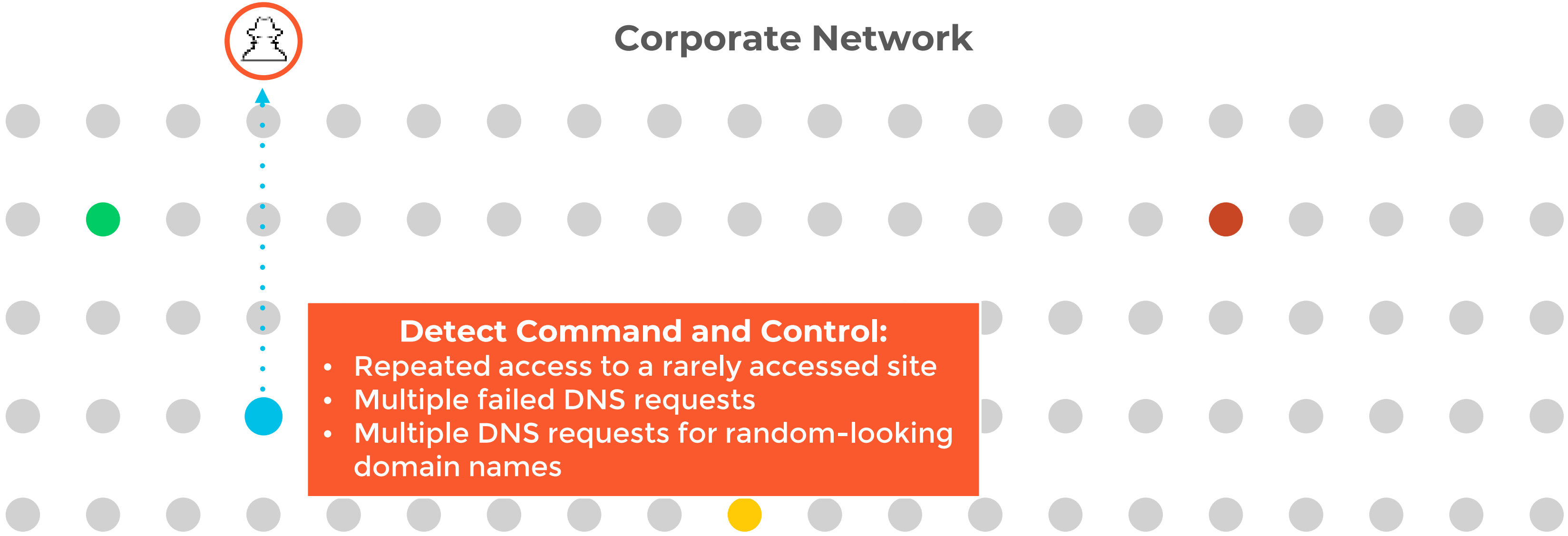
1

Identify types of users & devices by analyzing activity

2

Profile behavior of devices, users and groups over time

Automatically detect attacks with behavioral analytics



Detect Command and Control:

- Repeated access to a rarely accessed site
- Multiple failed DNS requests
- Multiple DNS requests for random-looking domain names

1 Identify types of users & devices by analyzing activity

2 Profile behavior of devices, users and groups over time

3 Detect anomalies indicative of C&C, lateral movement, exfiltration and malware

Why Cortex XDR for Network Traffic Analysis?

Deep Analytics

- AI-powered analytics
- Better data:
  - Threat, URL logs, User-ID, EAL
  - Agent or dissolvable agent (Pathfinder) for endpoint data
  - Windows event logs
  - Okta and Active Directory logs

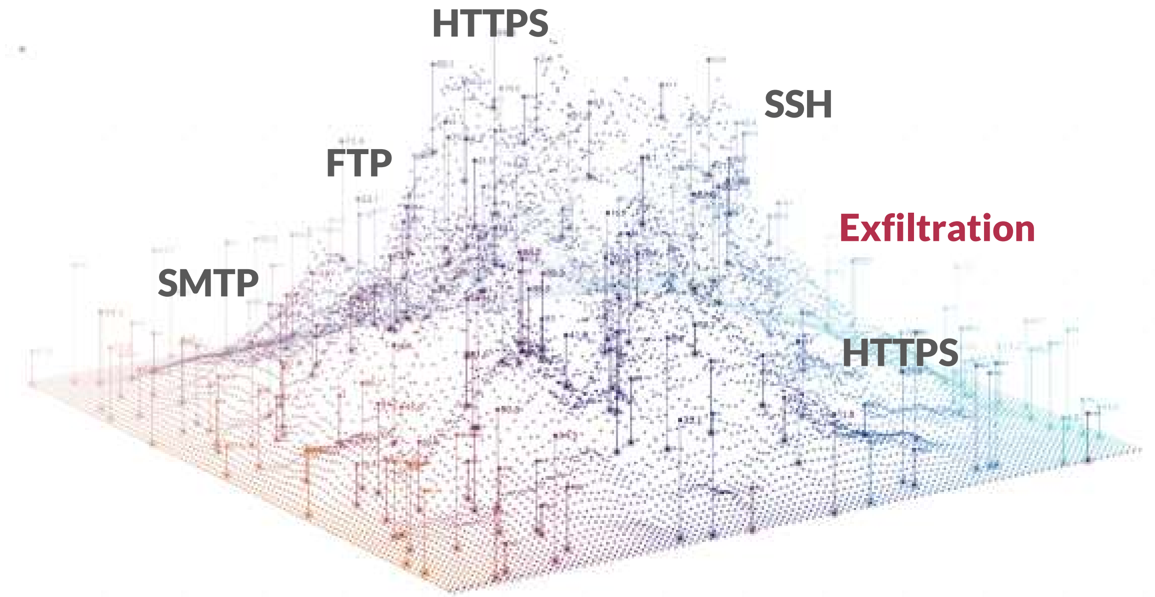
Flexible Log Exploration

- Threat hunting and custom rules (BIOCs) based on network data

Easy Deployment

- Seamless cloud-native deployment
- Existing NGFWs act as network sensors

The Most Complete Analytics Compared to NTA, UBA, or EDR Vendors

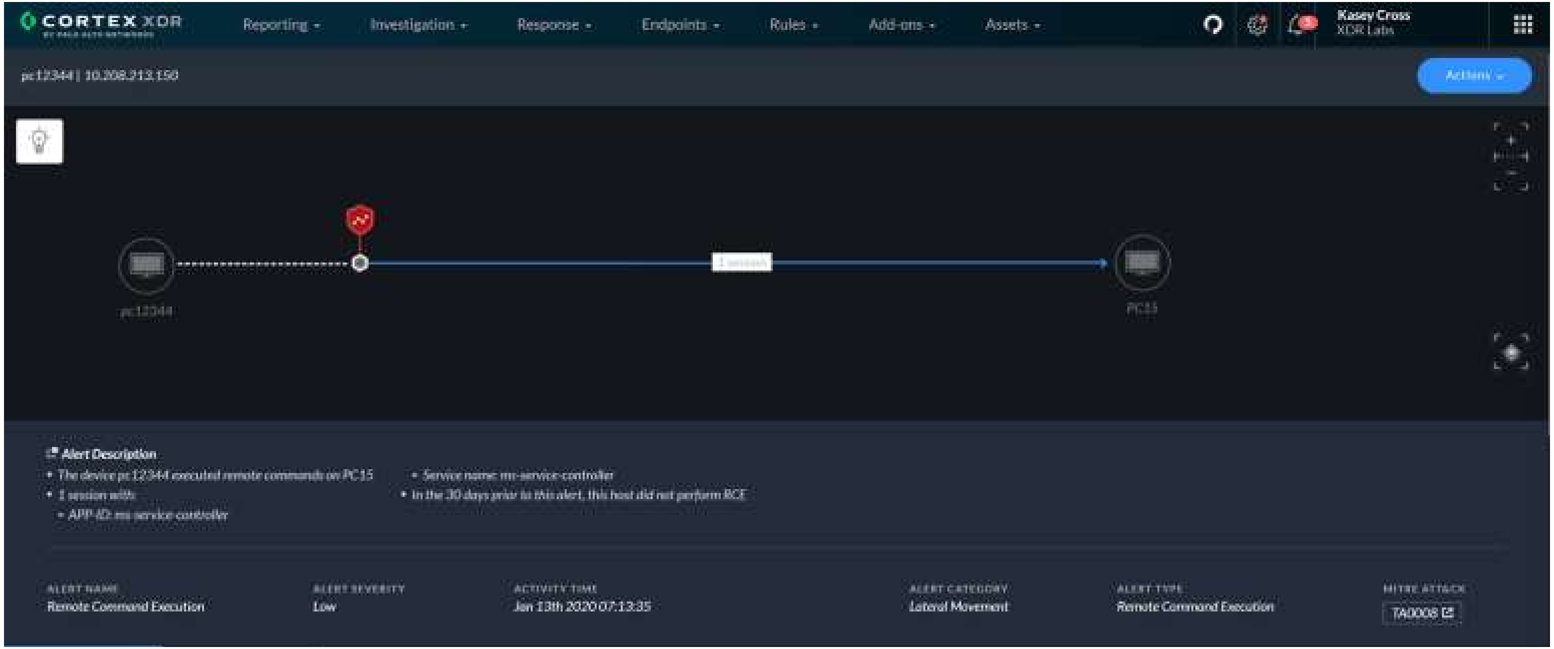


Behavioral analytics per customer for NTA, UBA

AI-based analysis with WildFire & Cortex XDR agent

Crowdsourced analytics to improve accuracy

Behavioral Analytics Enhancements



Alert Description

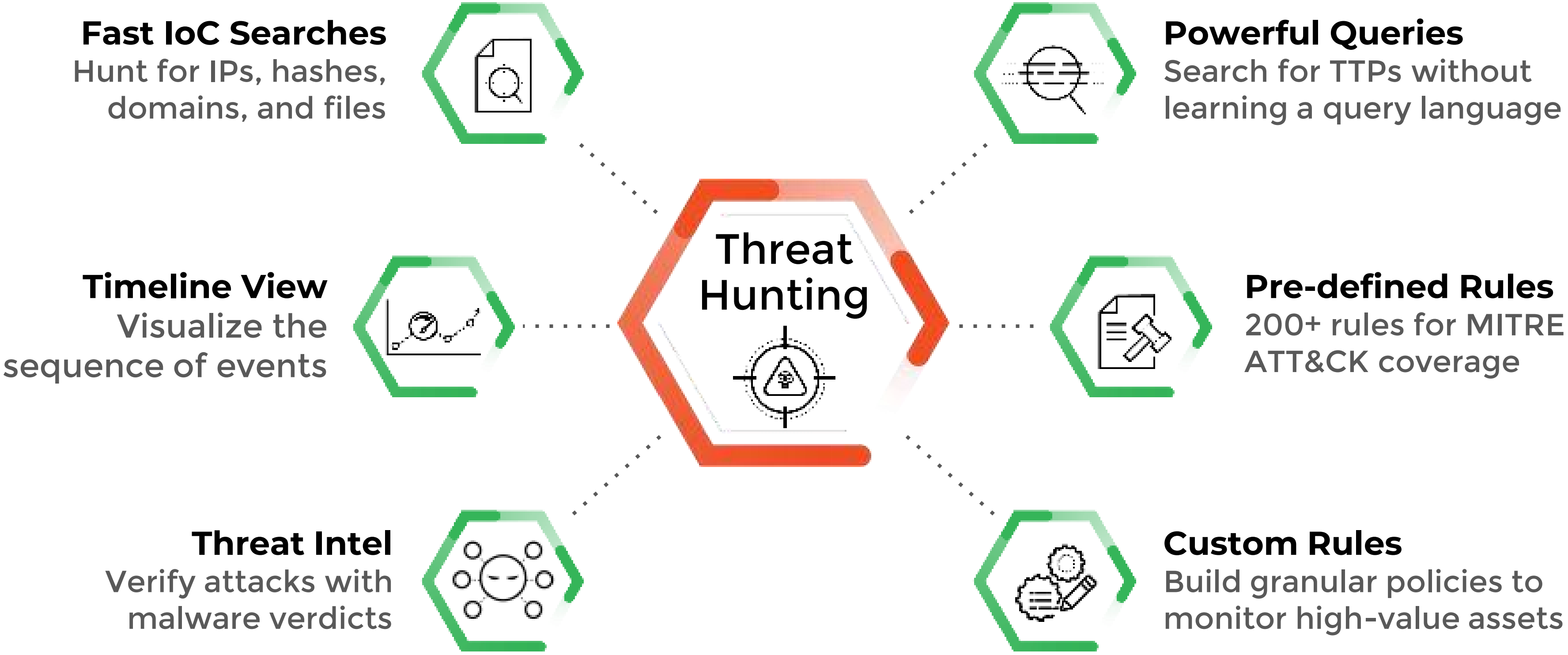
- The device pc12344 executed remote commands on PC15
- 1 session with:
  - APP-ID: ms-service-controller
  - Service name: ms-service-controller
- In the 30 days prior to this alert, this host did not perform RCE

ALERT NAME	ALERT SEVERITY	ACTIVITY TIME	ALERT CATEGORY	ALERT TYPE	MITRE ATTACK
Remote Command Execution	Low	Jan 13th 2020 07:13:35	Lateral Movement	Remote Command Execution	TA0008

Reduce the mean-time-to-detect with shorter behavioral profiling times, more granular alert exceptions, and increased alert accuracy.

Investigation and Response

Empower analysts to hunt for threats



Threat Hunting

Fast IoC Searches
Hunt for IPs, hashes, domains, and files

Powerful Queries
Search for TTPs without learning a query language

Timeline View
Visualize the sequence of events

Pre-defined Rules
200+ rules for MITRE ATT&CK coverage

Threat Intel
Verify attacks with malware verdicts

Custom Rules
Build granular policies to monitor high-value assets

Powerful Network Visibility for NGFW Customers

Custom network-based detection rules

Build BIOCs to alert on network firewall traffic logs

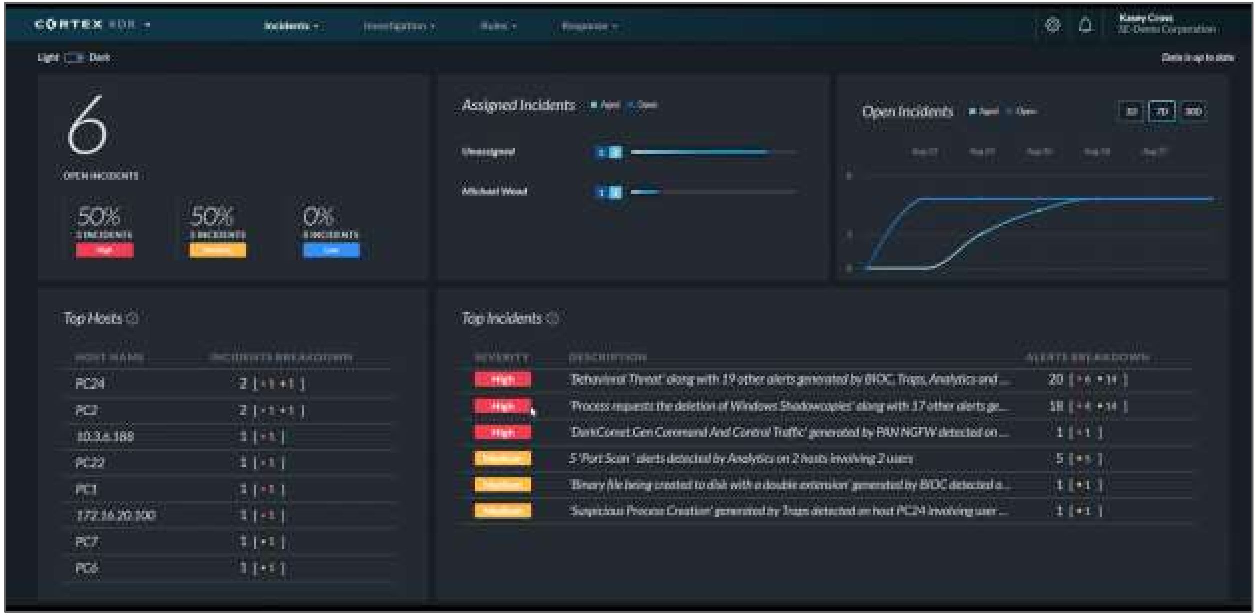
Flexible Exploration on Network Logs

Use the query builder on network logs to help with investigations

Network & Endpoint Data in Causality View

Get a complete picture by seeing the endpoint activity of multiple devices linked by network data

Speed up alert triage with the unified incident engine



Top Hosts

HOST NAME	INCIDENTS BREAKDOWN
PC24	2 [•1 •1]
PC2	2 [•1 •1]
10.3.6.188	1 [•1]
PC22	1 [•1]
PC1	1 [•1]
172.16.20.100	1 [•1]
PC7	1 [•1]
PC6	1 [•1]

Top Incidents

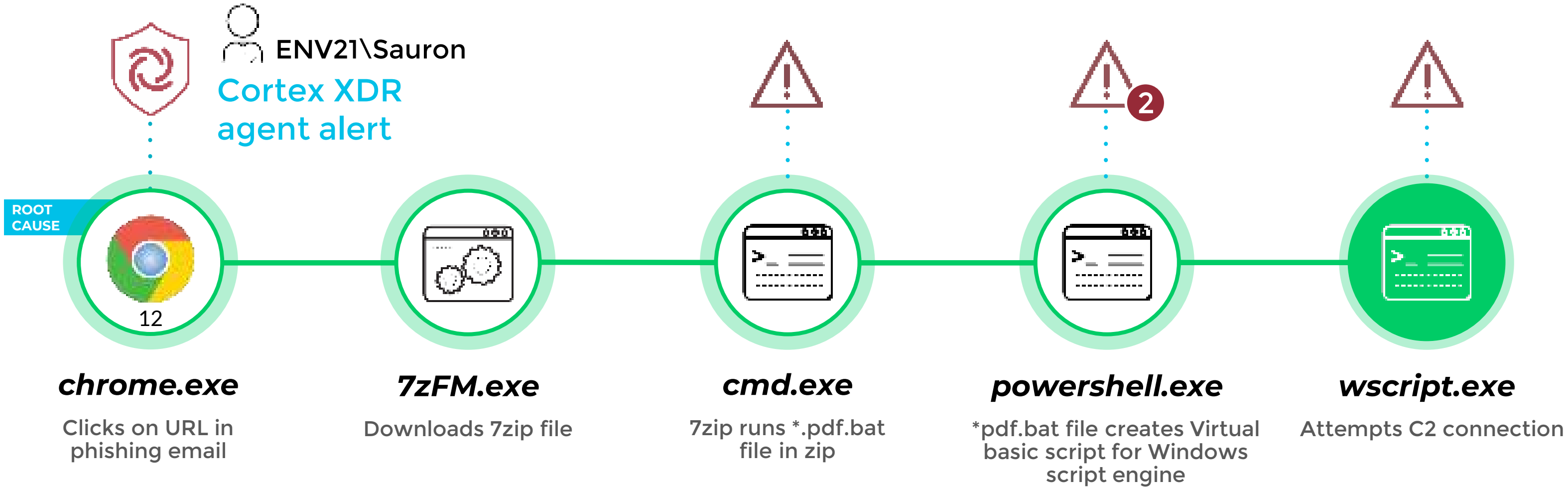
SEVERITY	DESCRIPTION	ALERTS BREAKDOWN
High	'Behavioral Threat' along with 19 other alerts generated by BIOC, Traps, Analytics and ...	20 [•6 •14]
High	'Process requests the deletion of Windows Shadowcopies' along with 17 other alerts ge...	18 [•4 •14]
High	'DarkComet.Gen Command And Control Traffic' generated by PAN NGFW detected on ...	1 [•1]
Medium	5 'Port Scan ' alerts detected by Analytics on 2 hosts involving 2 users	5 [•5]
Medium	'Binary file being created to disk with a double extension' generated by BIOC detected o...	1 [•1]
Medium	'Suspicious Process Creation' generated by Traps detected on host PC24 involving user ...	1 [•1]

Speed investigation by turning multiple related alerts into one incident

View high-level status of all incidents from the unified dashboard

Get a full picture of an attack, including attacker tools and affected hosts

Accelerate investigations by seeing every step in the attack



ENV21\Sauron

Cortex XDR agent alert

chrome.exe

Clicks on URL in phishing email

7zFM.exe

Downloads 7zip file

cmd.exe

7zip runs *.pdf.bat file in zip

powershell.exe

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

wscript.exe

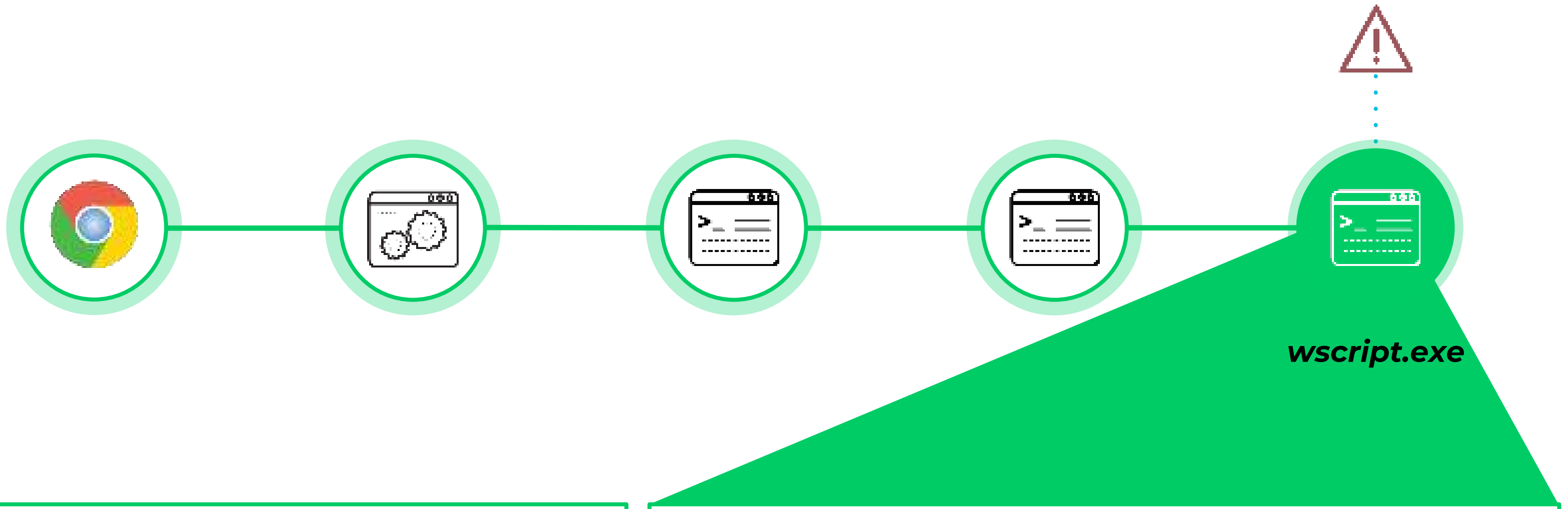
Attempts C2 connection

1 See the entire chain of events with one click

2 Instantly understand the root cause

3 Get full context including threat intel in one view

Make better decisions with AutoFocus threat intel



AF

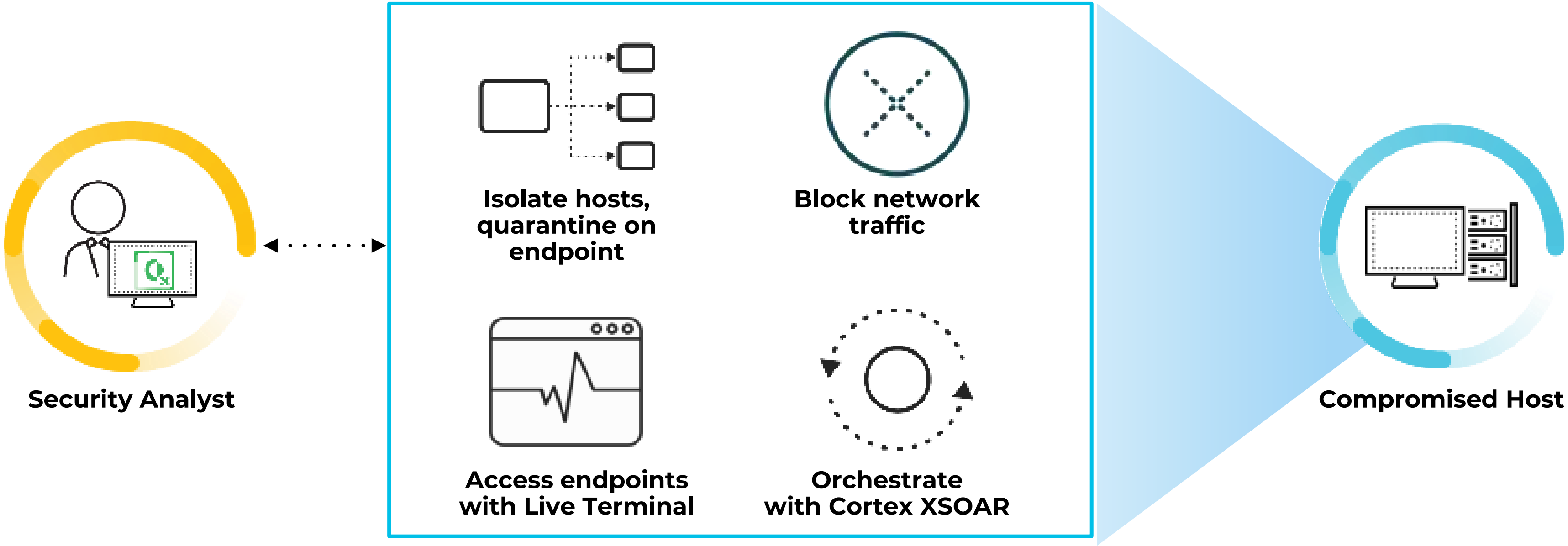
Industry's largest collection of high-fidelity threat intelligence

Add attribution with Unit 42

Improve speed & accuracy

Create custom reports & dashboards

Quickly contain threats with instant actions



Isolate hosts, quarantine on endpoint
Block network traffic
Access endpoints with Live Terminal
Orchestrate with Cortex XSOAR
Security Analyst
Compromised Host

Isolate hosts, block traffic and kill processes

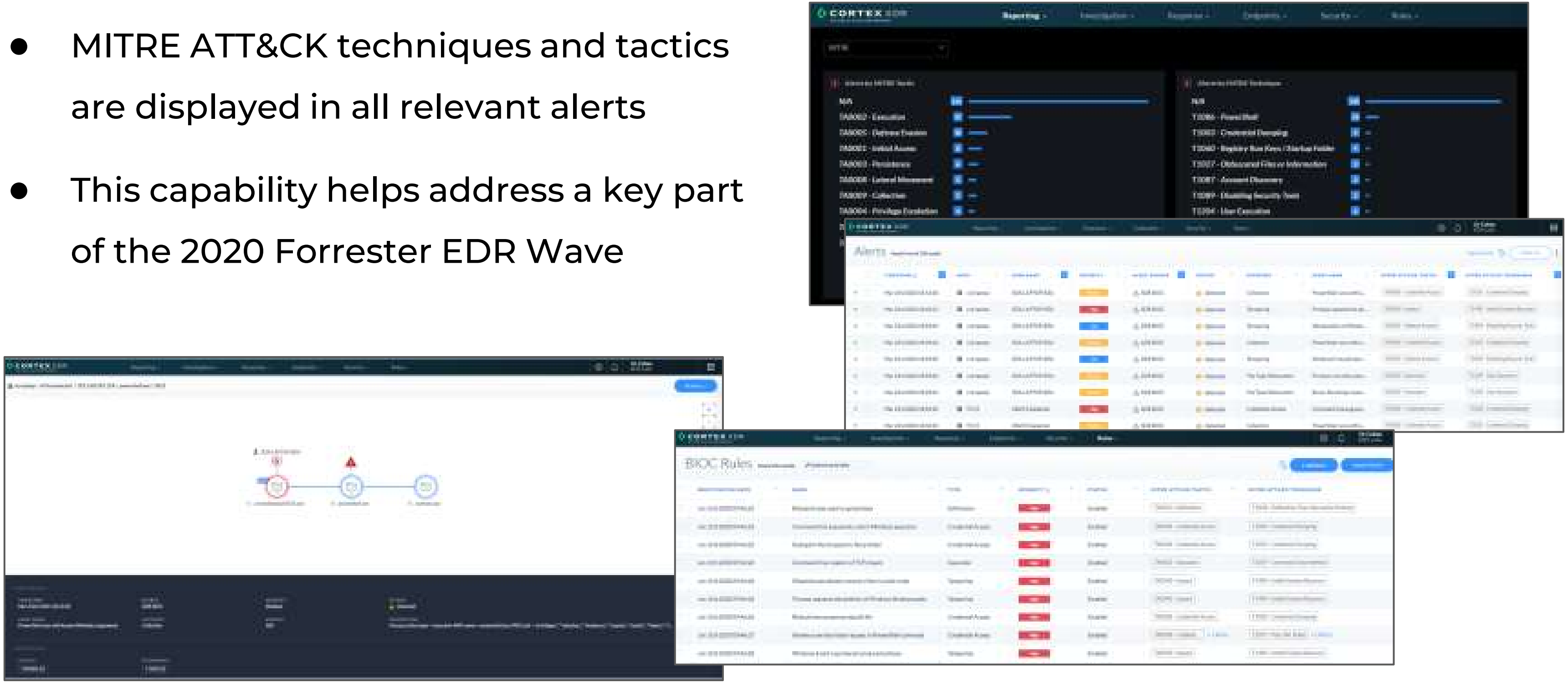
Directly connect to endpoints for granular custom actions & forensics

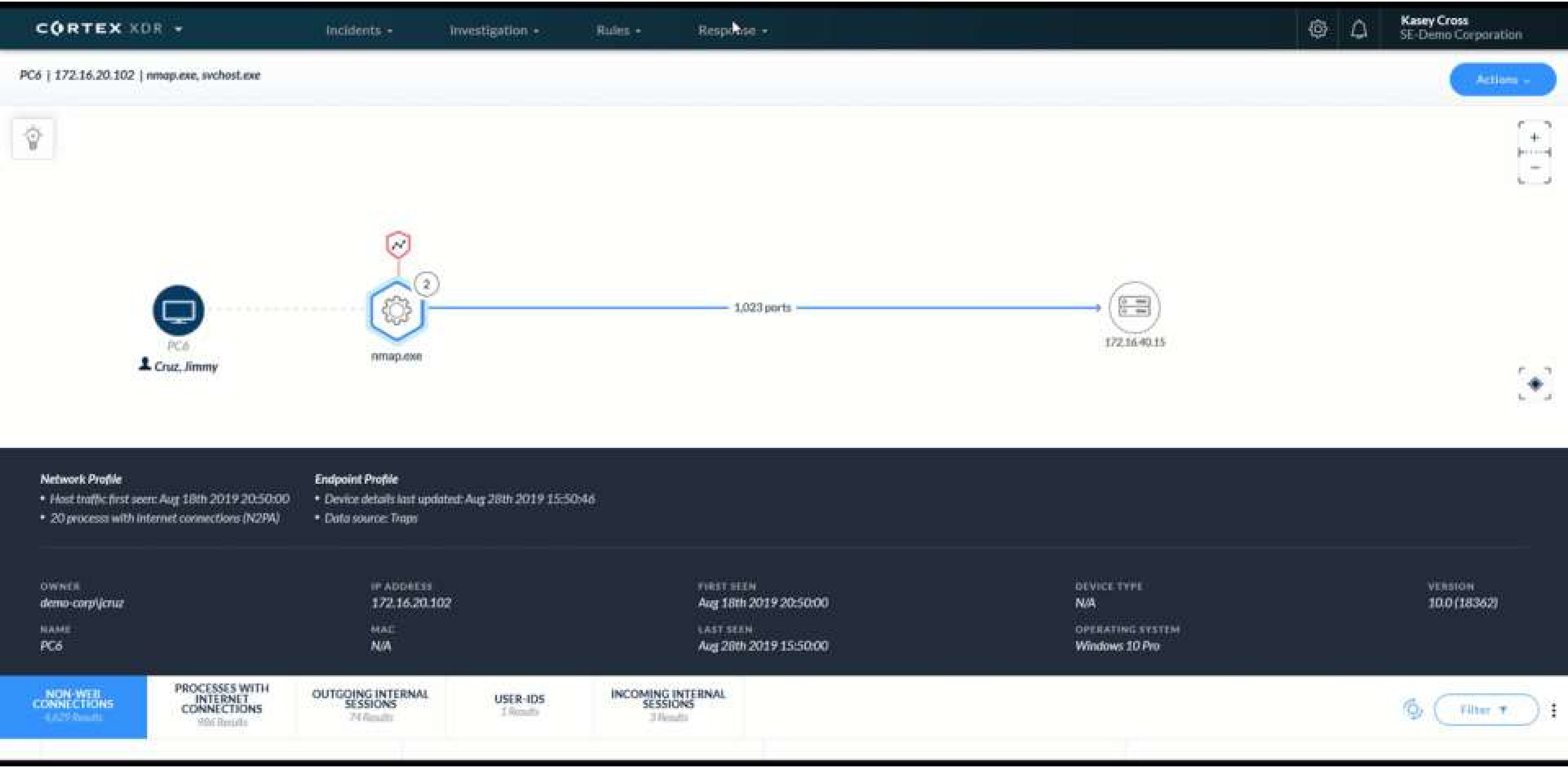
Orchestrate response across any security tool with Cortex XSOAR

MITRE ATT&CK Tagging for Alerts and BIOC Rules

MITRE | ATT&CK™

- MITRE ATT&CK techniques and tactics are displayed in all relevant alerts
- This capability helps address a key part of the 2020 Forrester EDR Wave


CORTEX EDR
N/A
TA0002 - Execution
TA0005 - Defense Evasion
TA0001 - Initial Access
TA0003 - Persistence
TA0008 - Lateral Movement
TA0009 - Collection
TA0004 - Privilege Escalation
T1086 - PowerShell
T1003 - Credential Dumping
T1060 - Registry Run Keys / Startup Folder
T1027 - Obfuscated Files or Information
T1087 - Account Discovery
T1089 - Disabling Security Tools
T1204 - User Execution
Alerts
BIOC Rules



PC6 | 172.16.20.102 | nmap.exe, svchost.exe

Network Profile

- *Host traffic first seen: Aug 18th 2019 20:50:00*
- *20 process with internet connections (N2PA)*

Endpoint Profile

- *Device details last updated: Aug 28th 2019 15:50:46*
- *Data source: Traps*

OWNER
demo-corp\jcruz

NAME
PC6

IP ADDRESS
172.16.20.102

MAC
N/A

FIRST SEEN
Aug 18th 2019 20:50:00

LAST SEEN
Aug 28th 2019 15:50:00

DEVICE TYPE
N/A

OPERATING SYSTEM
Windows 10 Pro

VERSION
10.0 (18362)

Host Insights Module

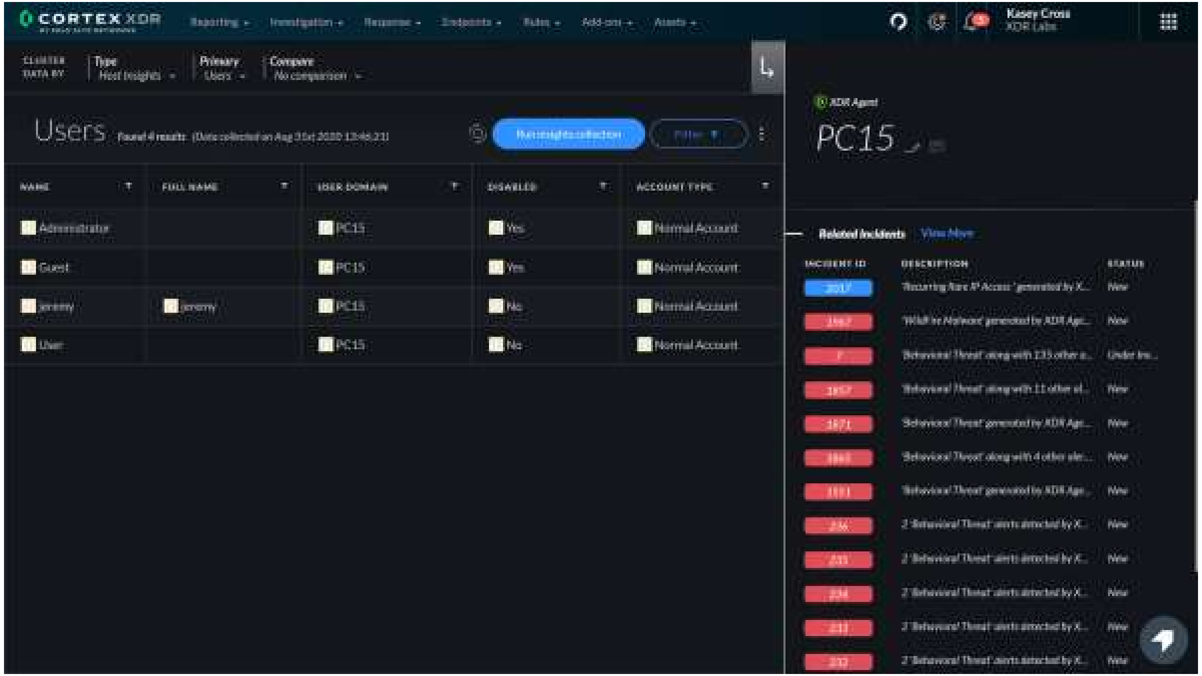
Search and Destroy

Application & System Visibility

Vulnerability Management

Get unprecedented endpoint visibility and flexible, fast response

New Asset View



CLUSTER DATA BY | Type: Host Insights | Primary: Users | Compare: No comparison

Users Found 4 results (Data collected on Aug 31st 2020 13:46:21)

NAME	FULL NAME	USER DOMAIN	DISABLED	ACCOUNT TYPE
Administrator		PC15	Yes	Normal Account
Guest		PC15	Yes	Normal Account
jeremy	jeremy	PC15	No	Normal Account
User		PC15	No	Normal Account

XDR Agent

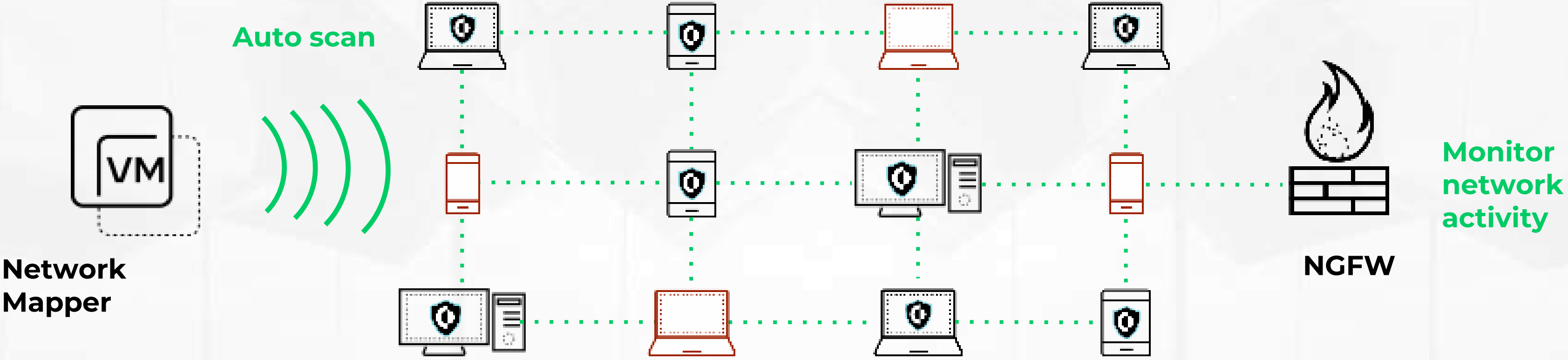
PC15

Related Incidents View More

INCIDENT ID	DESCRIPTION	STATUS
2017	'Recurring Rare IP Access ' generated by X...	New
1967	'WildFire Malware' generated by XDR Age...	New
7	'Behavioral Threat' along with 135 other a...	Under In...
1957	'Behavioral Threat' along with 11 other al...	New
1871	'Behavioral Threat' generated by XDR Age...	New
[illegible]	'Behavioral Threat' along with 4 other ale...	New
[illegible]	'Behavioral Threat' generated by XDR Age...	New
236	2 'Behavioral Threat' alerts detected by X...	New
235	2 'Behavioral Threat' alerts detected by X...	New
234	2 'Behavioral Threat' alerts detected by X...	New
233	2 'Behavioral Threat' alerts detected by X...	New
232	2 'Behavioral Threat' alerts detected by X...	New

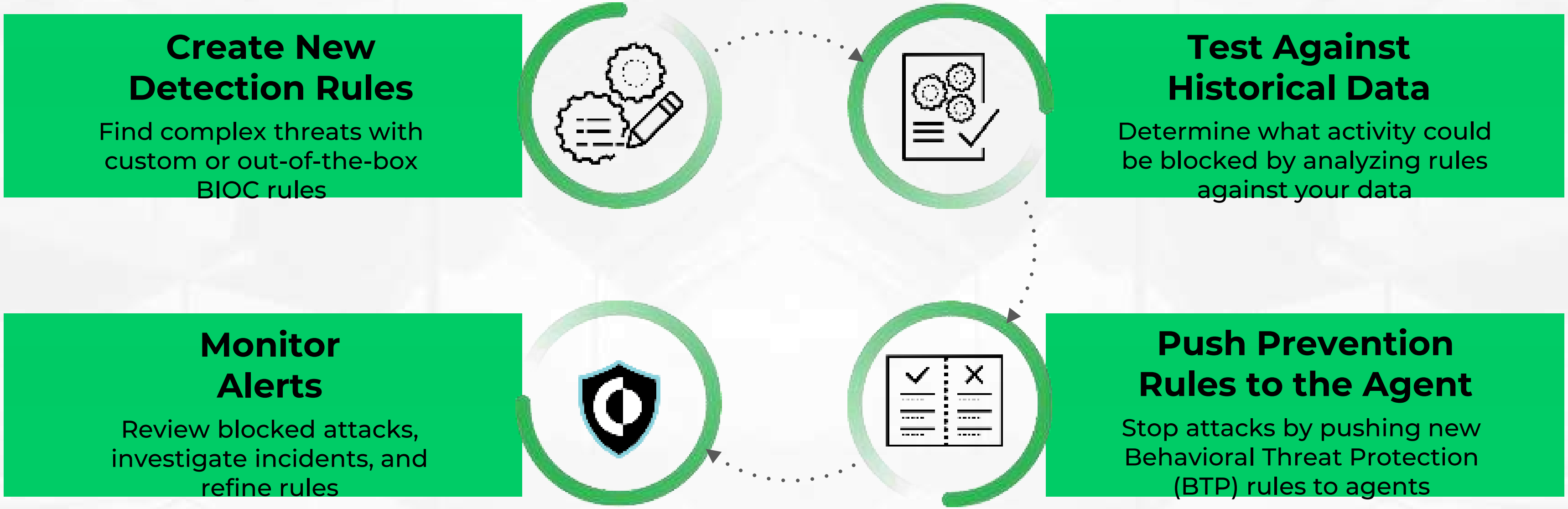
Get a full picture of an asset to assess host and user risk levels and to speed investigations

Rogue Device Discovery



The industry's most complete rogue device detection combining network scans and passive monitoring from traffic logs

Closed-Loop Prevention



Create New Detection Rules

Find complex threats with custom or out-of-the-box BIOC rules

Test Against Historical Data

Determine what activity could be blocked by analyzing rules against your data

Push Prevention Rules to the Agent

Stop attacks by pushing new Behavioral Threat Protection (BTP) rules to agents

Monitor Alerts

Review blocked attacks, investigate incidents, and refine rules

Rapidly transform new detection rules into automated protections

Remediation: Host Restore

Delete malicious files

Remove registry key changes

Restore modified files using Windows Shadow Copy

Remediate all events in an incident holistically

Easily revert to a clean state without re-imaging endpoints

Managed Threat Hunting

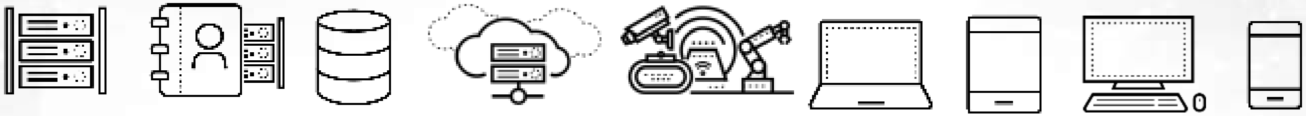
Key differentiator: **Get 24x7 managed threat hunting**

Managed Threat Hunting

- World-class hunters monitor your environment for complex attacks
- Deep knowledge of XDR data sources and Palo Alto Networks threat intelligence
- Early access to emerging Cortex XDR research

Cortex XDR

- Full visibility across endpoint, network & cloud
- Analytics and threat detection across all data sources generate leads for hunting
- Powerful data exploration & integrated threat intel



Get Peace of Mind with Managed Threat Hunting

Built on Cortex XDR Data

Analytics on integrated endpoint, network, and cloud data for unrivaled threat hunting

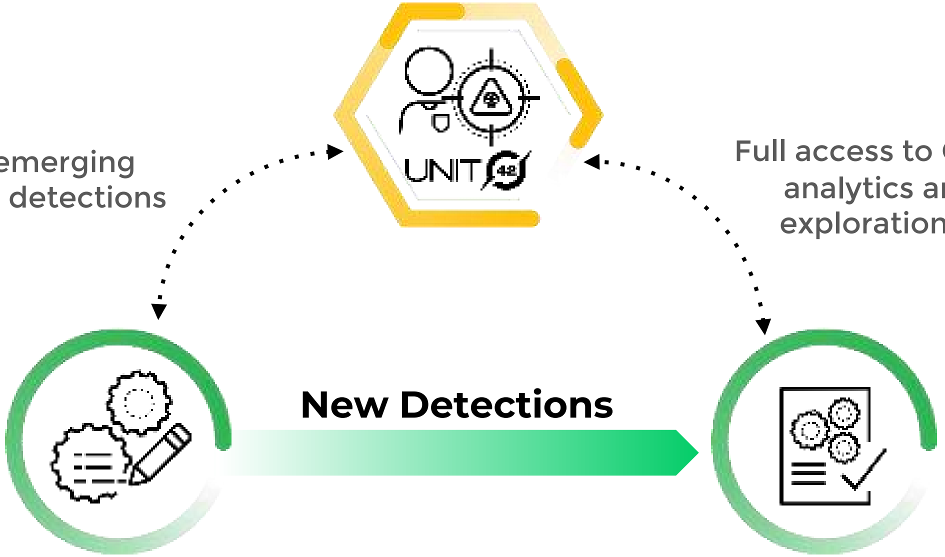
Backed by Unit 42

World-renowned threat hunters continuously monitor your environment for attacks

Enriched with Context

High-fidelity threat intel informs Threat and Impact Reports

How Hunters Find New Threats



Managed Threat Hunting Team

Hunters leverage the Cortex XDR platform and ongoing research to uncover hidden threats

Access to emerging research and detections

Full access to Cortex XDR analytics and data exploration engine

New Detections

Cortex XDR Research

Researchers analyze emerging threats and develop and test new detections

Cortex XDR Platform

New detections are released to Cortex XDR customers on a regular basis

UNIT 42

A Global Threat Intelligence Team

With years of defense, cyberwarfare, intelligence & industry experience

Threat Hunting Specialists

With deep knowledge of attacker tools, techniques and procedures

Malware Analysis Authorities

That are adept at forensics analysis and reverse engineering malware

World-Recognized Researchers

that partners with the security community and law enforcement

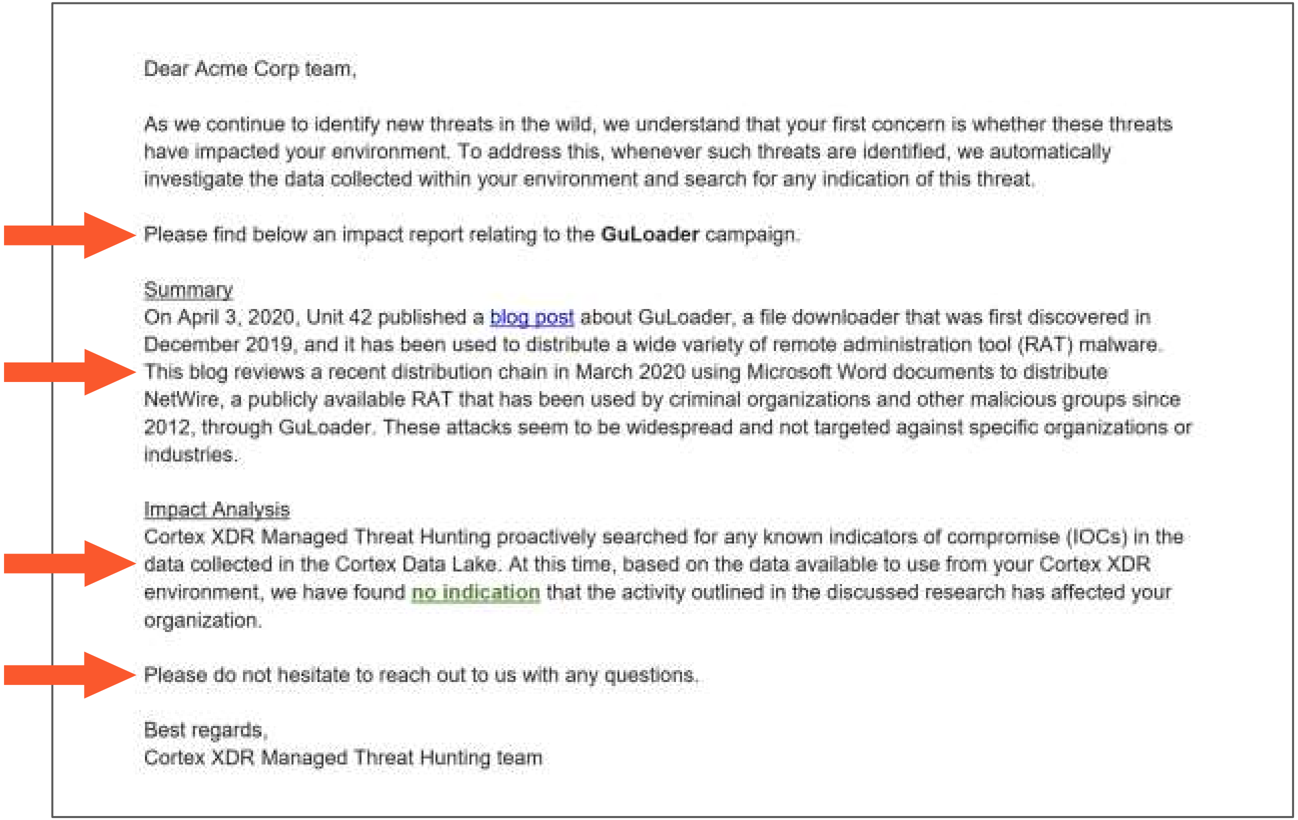
Stay Ahead of Emerging Threats with Impact Reports

Threat: GuLoader Campaign

Summary: Campaign description with links to more resources

Impact: The attack did not affect the customer

Assistance: Direct access to Unit 42 experts



Dear Acme Corp team,

As we continue to identify new threats in the wild, we understand that your first concern is whether these threats have impacted your environment. To address this, whenever such threats are identified, we automatically investigate the data collected within your environment and search for any indication of this threat.

Please find below an impact report relating to the **GuLoader** campaign.

Summary
On April 3, 2020, Unit 42 published a blog post about GuLoader, a file downloader that was first discovered in December 2019, and it has been used to distribute a wide variety of remote administration tool (RAT) malware. This blog reviews a recent distribution chain in March 2020 using Microsoft Word documents to distribute NetWire, a publicly available RAT that has been used by criminal organizations and other malicious groups since 2012, through GuLoader. These attacks seem to be widespread and not targeted against specific organizations or industries.

Impact Analysis
Cortex XDR Managed Threat Hunting proactively searched for any known indicators of compromise (IOCs) in the data collected in the Cortex Data Lake. At this time, based on the data available to use from your Cortex XDR environment, we have found **no indication** that the activity outlined in the discussed research has affected your organization.

Please do not hesitate to reach out to us with any questions.

Best regards,
Cortex XDR Managed Threat Hunting team

HUNTING AT SCALE

MANUAL HUNTING

Testing Hypothesis

New Attack Techniques

Manual investigations

SEMI-AUTOMATED HUNTING

Automation and Playbooks

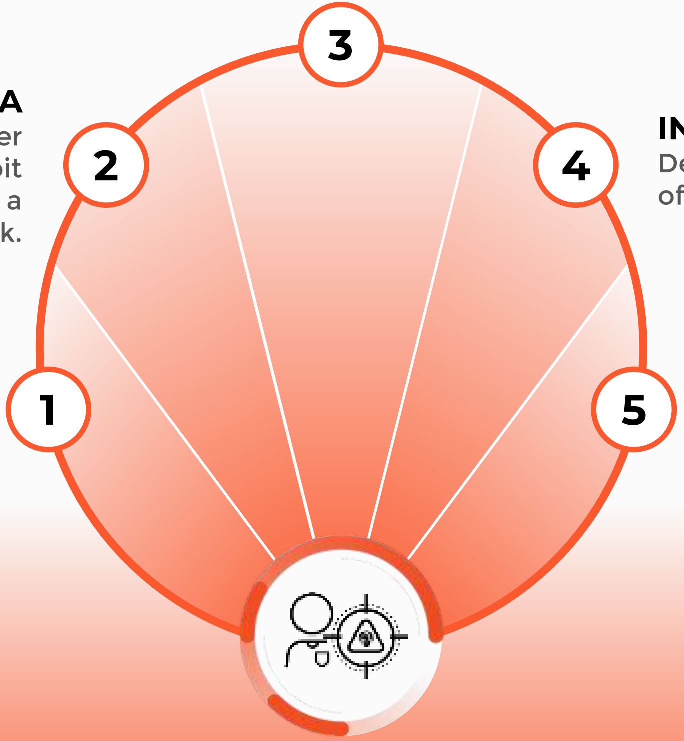
Signals and Detectors

Threat Intelligence

Extended Data Sources

AI and Machine Learning

MANUAL HUNTING



1

DATA SOURCES

Network, endpoint, cloud and third-party data sources provided by customers.

2

IDEA

Based on findings from other cases or a newly published exploit or attack, the hunter will design a query to look for the attack.

3

HYPOTHESIS

The hunter will validate the hypothesis, check results, and refine the hypothesis until the hunter has discovered threats or is confident that no threat exists.

4

INVESTIGATION

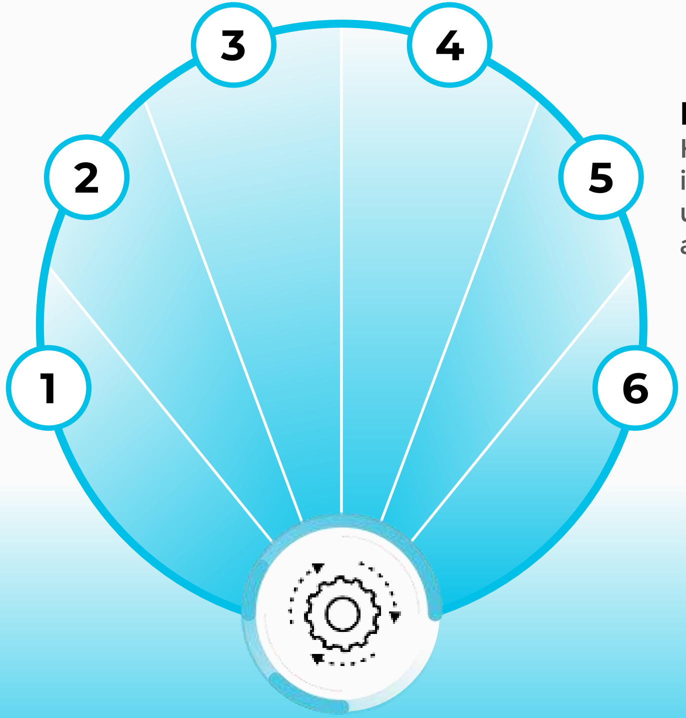
Deeper investigation of the findings and evidence.

5

REPORT

The hunter sends a report with findings to the customer.

SEMI-AUTOMATED HUNTING



DATA SOURCES

Network, endpoint, cloud and third-party data sources provided by customers.

SIGNALS

Smart signals analyzing all collected data in order to every discover threat. Signals are based on one or all customers.

ENRICHMENT & PRIORITIZATION

Enriching incidents found by the signals and prioritization.

INITIAL INVESTIGATION

The first step for the hunter is to validate the signal before investigating it in the Cortex XDR management console.

DEEP INVESTIGATION

Hunter performs a manual investigation to confirm the threat and understand the full scope of the attack.

REPORT

The hunter sends a report with findings to the customer.

THREAT HUNTING TOOLS

HUNTERS KNOWLEDGE

Unit 42 experts

CORTEX XDR MANAGED THREAT HUNTING

Special version of Cortex XDR allows us to get eyes across all Managed Threat Hunting customers, ask questions and perform investigations

AUTOFOCUS

A high-fidelity threat intelligence feed powered by WildFire findings

WILDFIRE

A cloud-delivered malware analysis service

CORTEX XSOAR

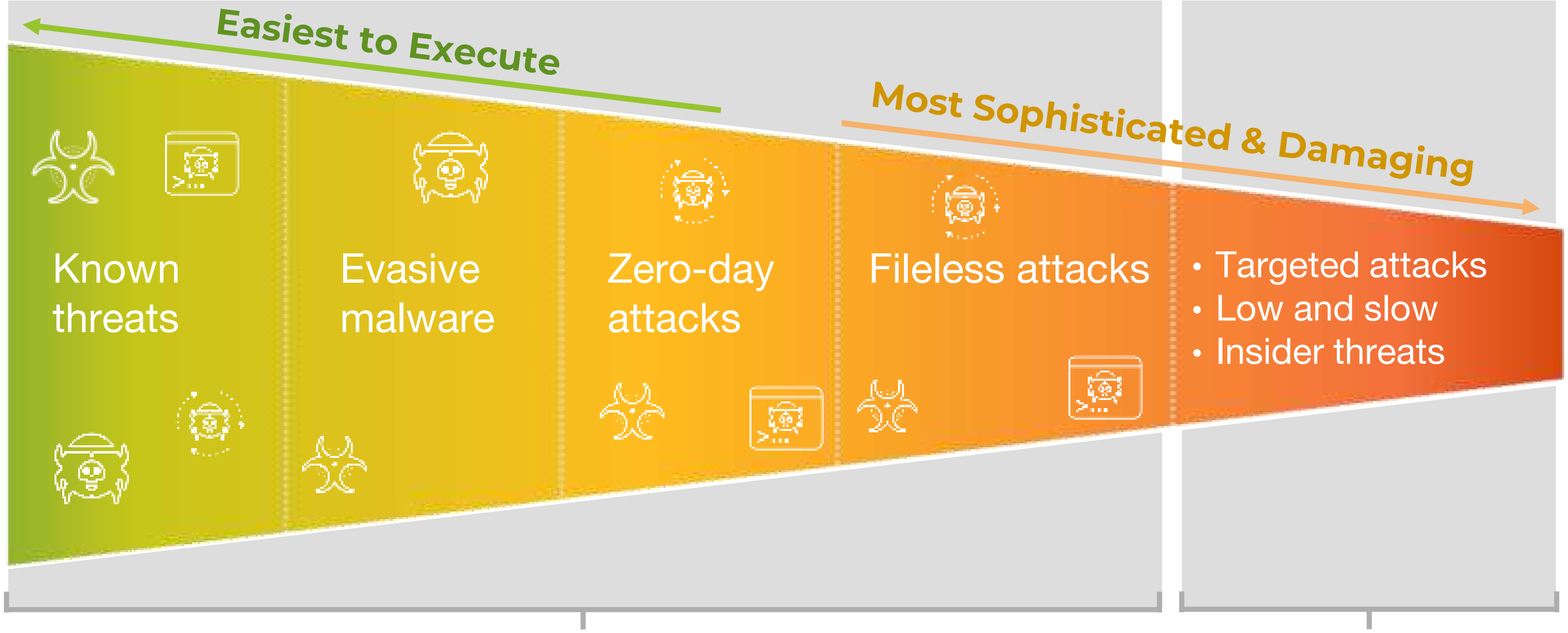
Playbooks to aggregate and normalize threat intel, enrich incidents, reduce false positives, de-duplicate activities & produce experimental signals

EXTERNAL RESOURCES

VT, Cuckoo, URL Analyzer, GCP

Why XDR?

Advanced Attacks Require Detection & Response

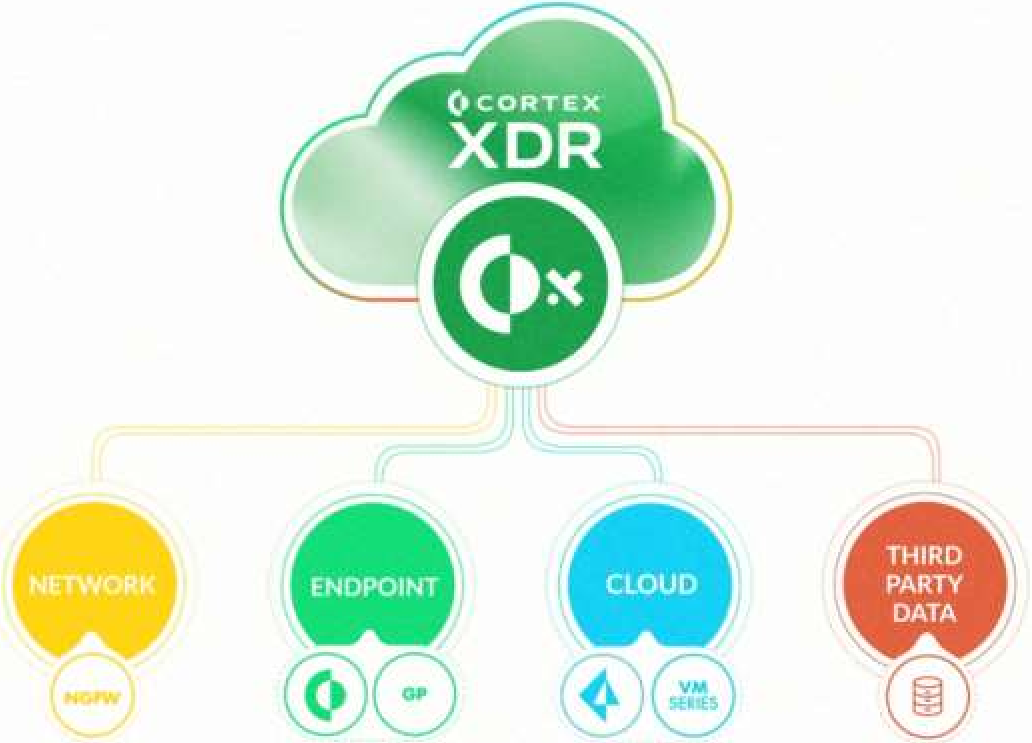


99%+ of attacks can be prevented with the right tools

<1% require analysis over time & across layers with machine learning

EPP
UEBA
AV
SIEM
EDR
NTA

XDR



Cortex XDR detects stealthy attacks by analyzing integrated data with machine learning and behavioral analytics

Gartner

> “
>
> **In response to the security skills gap and attacker trends, XDR tools, ML and automation capability are emerging to improve security productivity and detection accuracy**
>
> ”

Top Security and Risk Management Trends, Gartner, February 27, 2020

Cortex XDR Accelerates Investigations 8x Compared to Siloed Tools

Capability	Average Time Reduction
Grouping alerts into incidents (50x average alert reduction)	40%
Data stitching for root cause analysis of network, endpoint and cloud alerts	50%
Reduction in false positives driven by machine learning across network, endpoint and cloud data	20%
Rich contextual alerts to reduce investigation times	20%
Threat hunting, pivoting, Quick Launcher, Hash/IP View, native search	20%
Live Terminal, script execution for faster investigation and response	20%
Total Combined Time Savings	**88% Savings**
Investigation and Response Time per Incident	**5 Minutes Instead of 40 Minutes**

Total Time Savings Calculation = 1 – (60% x 50% x 80% x 80% x 80% x 80%) = 87.7%

Cortex XDR Lowers TCO 44% Compared to Siloed Tools

Capability	Palo Alto Networks Platform (List Price)	Siloed Security Tools (List Price)
Endpoint detection and response (EDR) and endpoint protection (EPP)	**$285,000/year** for Cortex XDR Pro per Endpoint with 30-day endpoint data collection, excluding Cortex Data Lake	**$430,000/year** for separate EPP and EDR agents with 30 days of storage
Network traffic analysis[1]	**$274,500/year** for Cortex XDR Pro per TB with 30-day network data collection, excluding Cortex Data Lake	**$430,000/year** for NTA appliances and network taps or flow generators
User and entity behavior analytics	**$0**; included with Cortex XDR	**$280,000/year** for add-on UEBA or subscription for SIEM
Alert triage and investigation overhead	**$215,200/year** for 2 cybersecurity analysts	**$376,660/year** for 3.5 analysts[2]
SOC alert policy creation and tuning	**$53,800/year** for 0.5 cybersecurity analyst	**$107,600/year** for 1 cybersecurity analyst[3]
Operating costs for software, hardware, and log servers	**$122,799/year** for 1.5 IT and desktop admins	**$245,598/year** for 3 IT and desktop admins[9]
Network Log Collection	With Cortex	Without Cortex
Log storage for network security management	**$172,000/year** for Cortex Data Lake, including support	**$133,100** for redundant Panorama M-600 log collector appliances and premium support[4]
Total Cost of Ownership	**$1,123,299/year**	**$2,002,958/year**

[1] Cortex XDR includes network traffic analysis, but customers must collect network traffic logs, which increases storage requirements and thus subscription costs.

[2] Siloed tools reduce productivity, require more staff, and increase alert triage and investigation expenses.

[3] Cortex XDR includes nearly 200 predefined BIOC rules as well as analytics detection algorithms out of the box. Analysis of anonymized cloud-based metrics informs development of predefined rules as part of product updates, lowering policy tuning costs.

[4] Siloed tools require extra overhead to manage and maintain separate EPP and EDR agents; NTA sensors; and on-premises log storage, analysis, and management servers

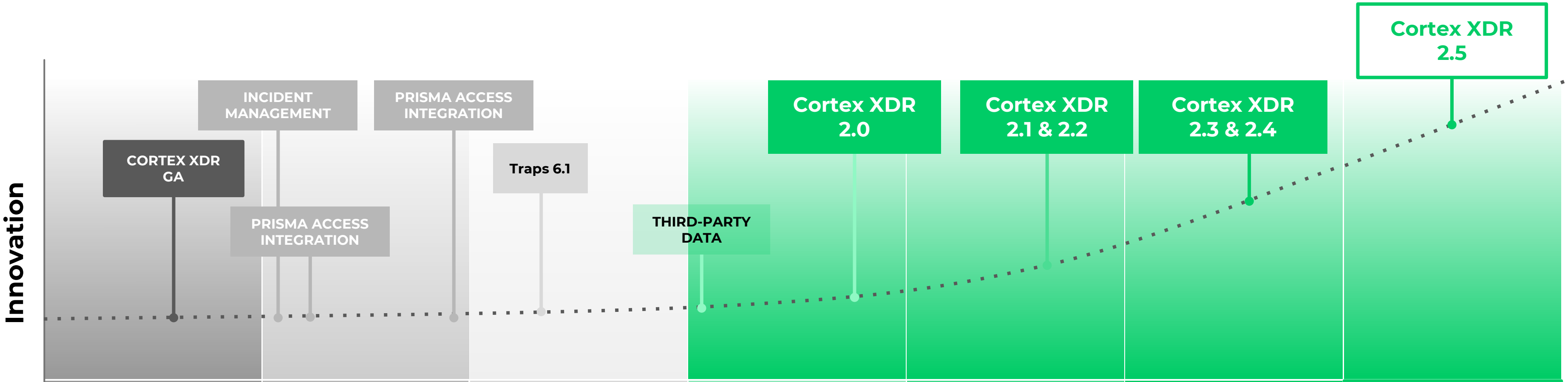
Sample Organization for TCO Calculation

Sample Organization	
Total number of users	10,000
Total number of managed and unmanaged devices	25,000
Current firewalls	Palo Alto Networks Next-Generation Firewalls
Current firewall management	Panorama appliances
Current antivirus	Legacy antivirus agent
Project objectives	• Replace antivirus • Reduce mean time to respond (MTTR) by 50% • Improve visibility to managed and unmanaged devices • Store logs for Panorama for 30 days
Cost of a cybersecurity analyst	$107,600/year[1]
Cost of an IT administrator	$81,866/year[2]

[1] Based on $79,738 average salary with 135% overhead for taxes, benefits, bonuses, and office costs. Salary information from Glassdoor.com as of June 20, 2019.

[2] Based on $60,642/year average salary with 135% overhead for taxes, benefits, bonuses, and office costs. Salary information from Glassdoor.com as of June 20, 2019.

Rapid Pace of Innovation for Cortex XDR



Q1 2019

- Traps endpoint protection with EDR data
- Cortex XDR app
- Live Terminal
- Incident Management

Q2 2019

- Incident management dashboard
- Role-based access control
- IOC and alert exclusions
- Prisma Access & SOAR integration

Q3 2019

- BTP for Linux and macOS
- EDR data for Linux and macOS
- Enhanced Traps response options
- App-ID & URL filtering category integration

Q4 2019

- Third-party log & alert support
- Rebuilt Traps within Cortex XDR
- Reporting
- Device Control
- AI-driven local analysis engine

Q1 2020

- Enhanced network visibility
- Granular RBAC
- Log & alert forwarding
- Windows event logs
- Dashboard customization

Q2 2020

- Disk encryption
- Host firewall
- Script execution
- Vulnerability management
- Threat Intelligence Platform integration

Q3 2020

- Host Insights
- Rogue Device Discovery
- Remediation Enhancements
- Customizable Prevention (BIOC to BTP)

Industry-Leading MDR Services from Our Partners

Vendor-based MDR falls short

Vendor-based MDR services	MDR built on Cortex XDR
Miss critical data sources beyond endpoint for investigations	Stitched network, endpoint, cloud & 3rd-party data for investigation
Lack flexibility in technology and locked into the vendor's stack	Provides the best service with flexibility to evolve as needs change
No SLA guarantee of MTTD and MTTR reduction	Guaranteed reduction of MTTD & MTTR to <60 minutes

DON'T GET ROPED INTO MANAGED ENDPOINT DETECTION AND RESPONSE

All the benefits of Cortex XDR, and more...

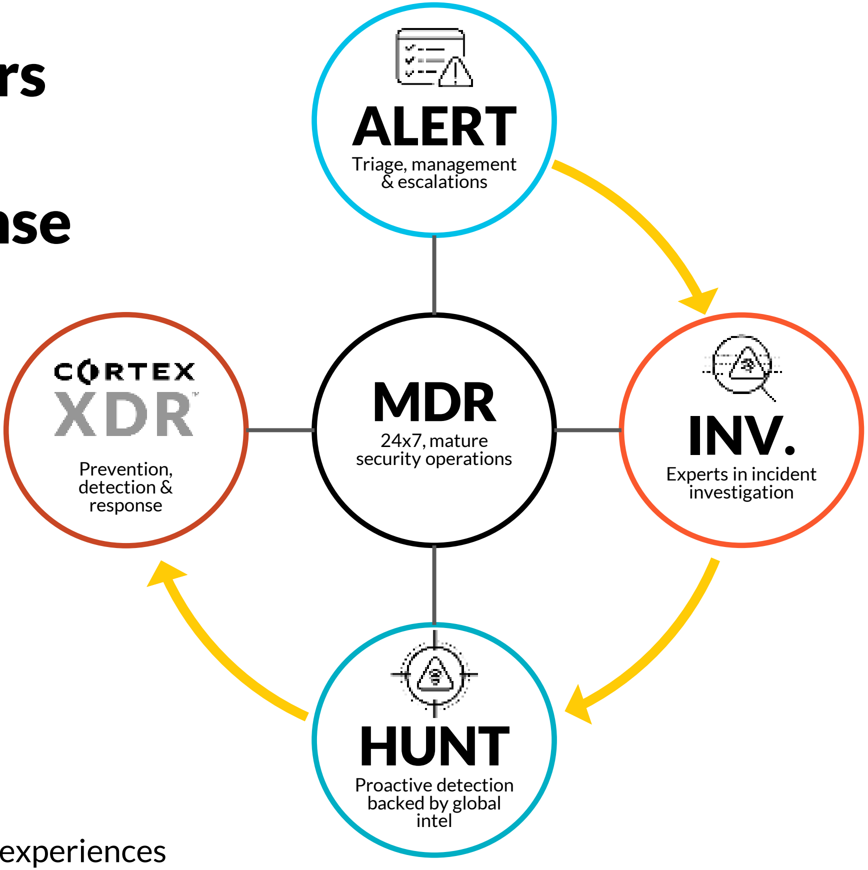
Value	Cortex XDR	With MDR
Automated ML-based detections	✓	✓
Custom rules	✓	✓
Root cause analysis	✓	✓
Endpoint, network & cloud prevention	✓	✓
Live response	✓	✓
Incident grouping	✓	✓
Proactive threat hunters	✓	✓
24x7x365 Experienced Security Analysts		✓
Investigation of every alert		✓
Expert forensic analysis		✓
Guided remediation actions		✓
Direct access to analysts		✓
Mobile application		✓
Dedicated SLAs for MTTD & MTTR		✓

MANAGED SERVICE PARTNER

Our expert MDR partners can instantly pivot from threat hunting to response

MDR provider requirements:

- History of deep forensic and incident response expertise
- Fast, accurate alert triage, prioritization and investigation
- Concrete detection, investigation and response SLAs
- Smart, closed-loop operations to bolster intelligence from past experiences



ALERT
Triage, management & escalations

INV.
Experts in incident investigation

HUNT
Proactive detection backed by global intel

CORTEX XDR
Prevention, detection & response

MDR
24x7, mature security operations

ALERT

Triage,
management
& escalations

24x7 monitoring and management of alerts generated by Cortex XDR

Experts in alert triage ensure every alert is analyzed and no threat is missed

Custom escalation workflows show only the most pertinent attacks to the customer

INV.

Experts in incident investigation

Quickly identify root cause to pinpoint attack vectors and stop advancement

Instantly pivot to incident response armed with our partners battle-tested best practices

Gain 50+ years of combined experience of threat investigations and incident handling from our partners

HUNT

Proactive detection backed by global intel

Find stealthy attacks with continuous hunting and benefit from applied knowledge across all customers

Get customized BIOCs that optimize visibility and reduce detection time for your unique environment

Integrated threat intelligence from our partners to broaden detection parameters and find the latest threats

CORTEX XDR™

Prevention, detection & response

One integrated platform enable best-in-class MDR services across network, endpoint, cloud & 3rd-party data

Detect and respond to more threats with leading alert context and accuracy, proven by MITRE ATT&CK

Empowers our partners' analysts to meet and exceed time-based SLAs by investigating up to 8x faster