

Cortex Secures The Future

REINVENTING SECURITY OPERATIONS

Name

Title



How to use this deck

This deck is meant to be a modular master deck for customer meetings.

Please note that most meetings will be focused on either Cortex XDR or Demisto (and not both) so please make a copy and reduce the slides down to meet the needs of the specific meeting.

If you would like create your own personal personal copy to customize, use File -> “Make a copy”

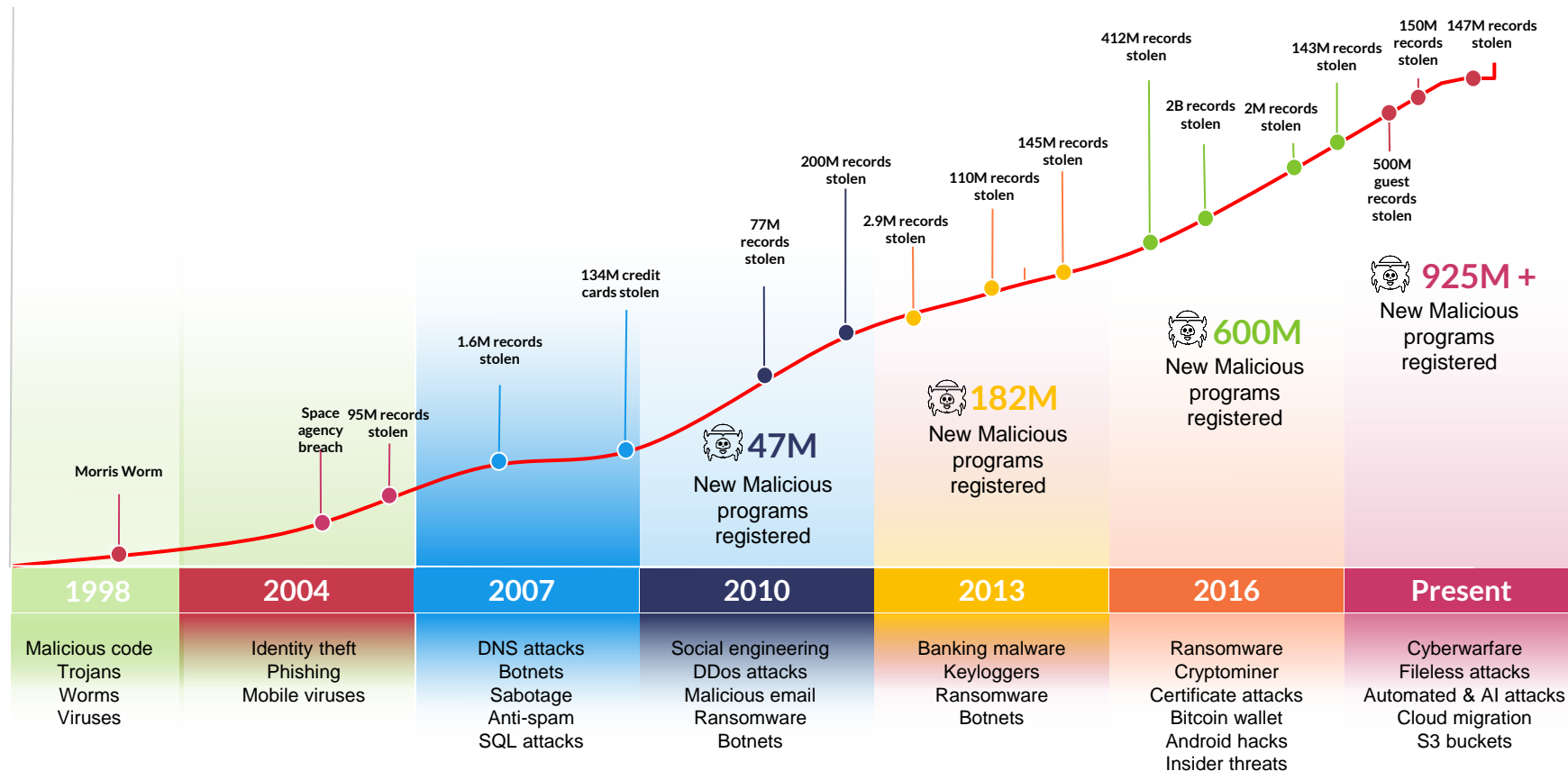
Standalone decks with additional product slides:

- [Cortex XDR](#)
- [Demisto](#)

Emerging Challenges in Security Operations



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

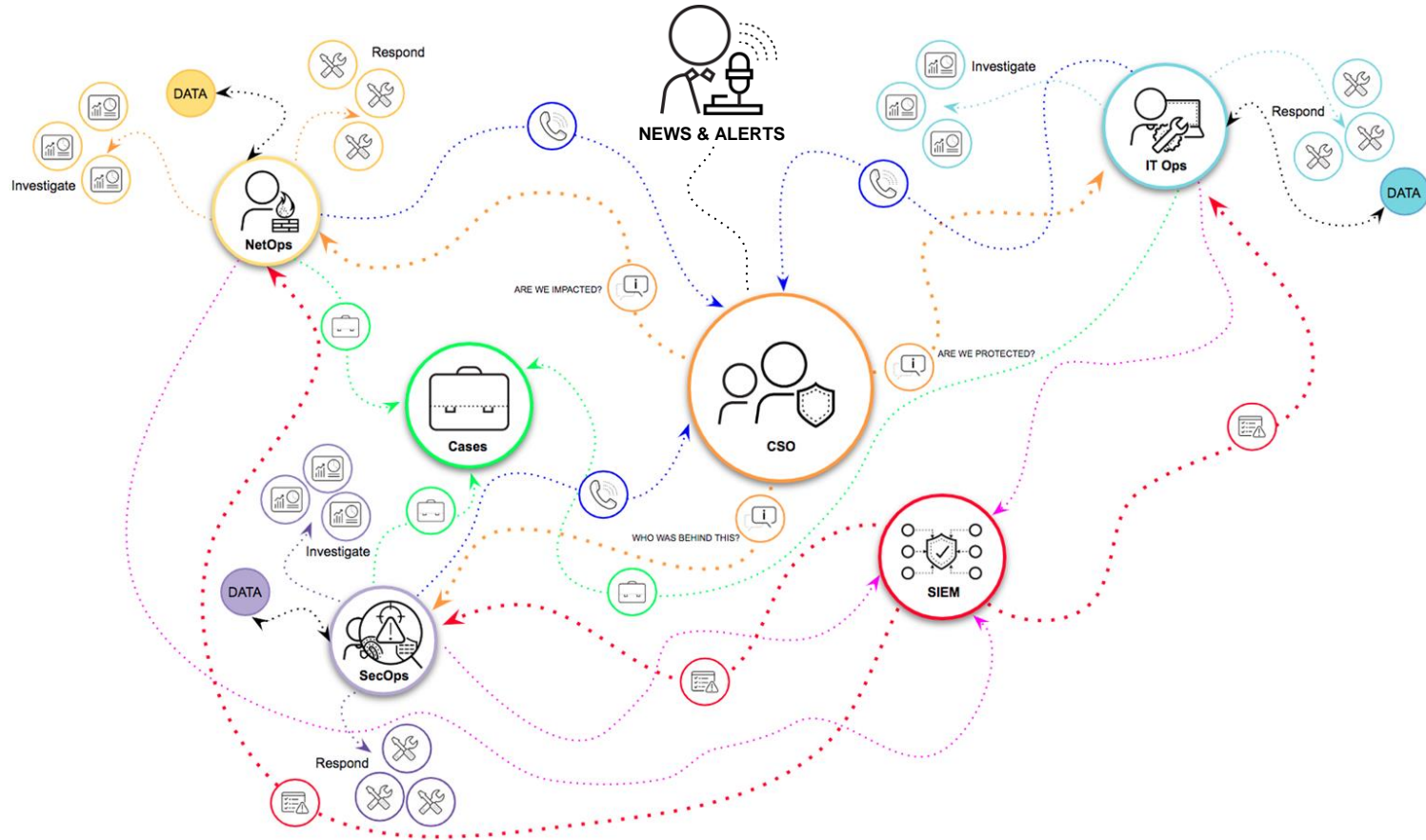


Limited Context

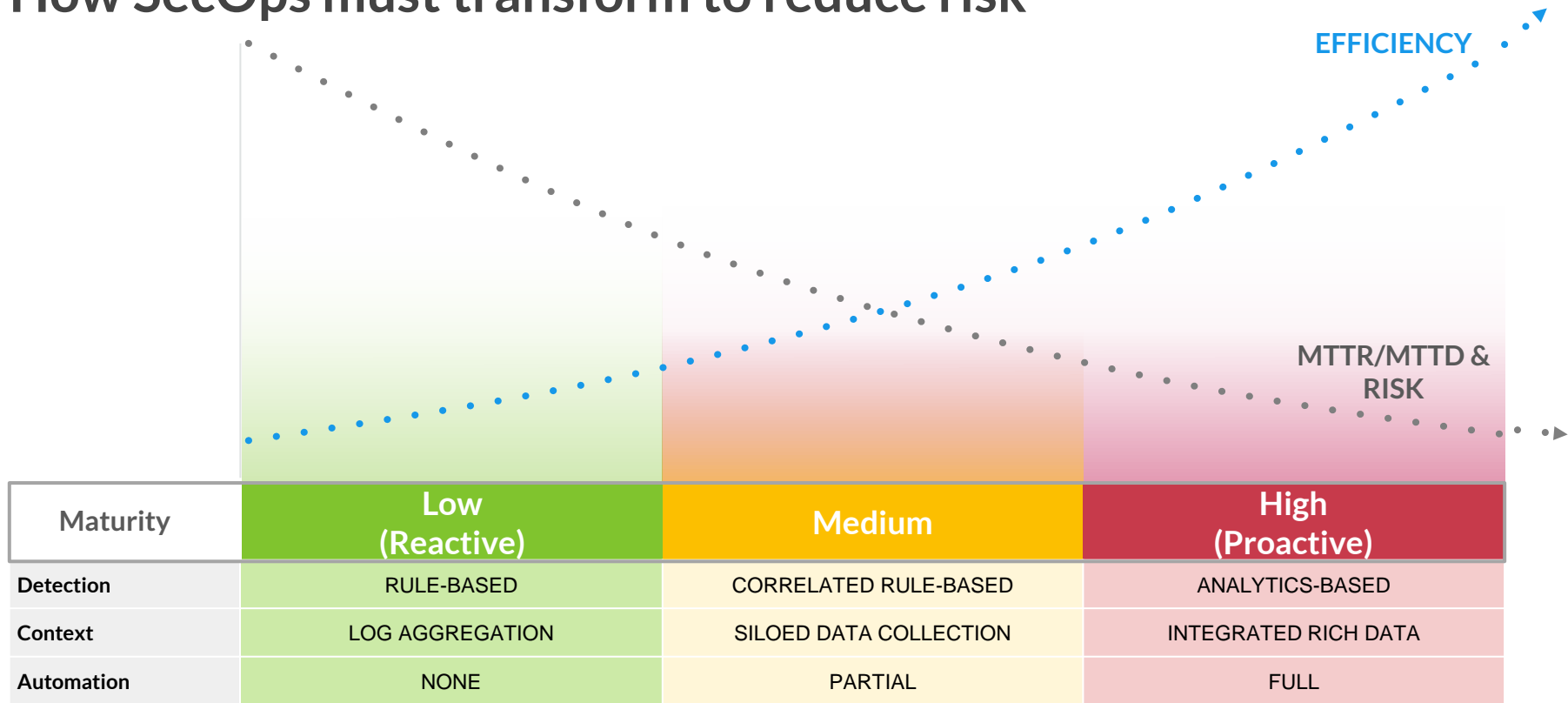
It takes days to investigate threats

4+ days
to complete an investigation

The reality (and complexity) of security operations



How SecOps must transform to reduce risk



Our Unique Approach



Reinventing SecOps with Cortex



Prevent everything
you can

**Traps & Next-Generation
Firewall**



Everything you can't
prevent, detect
and investigate fast

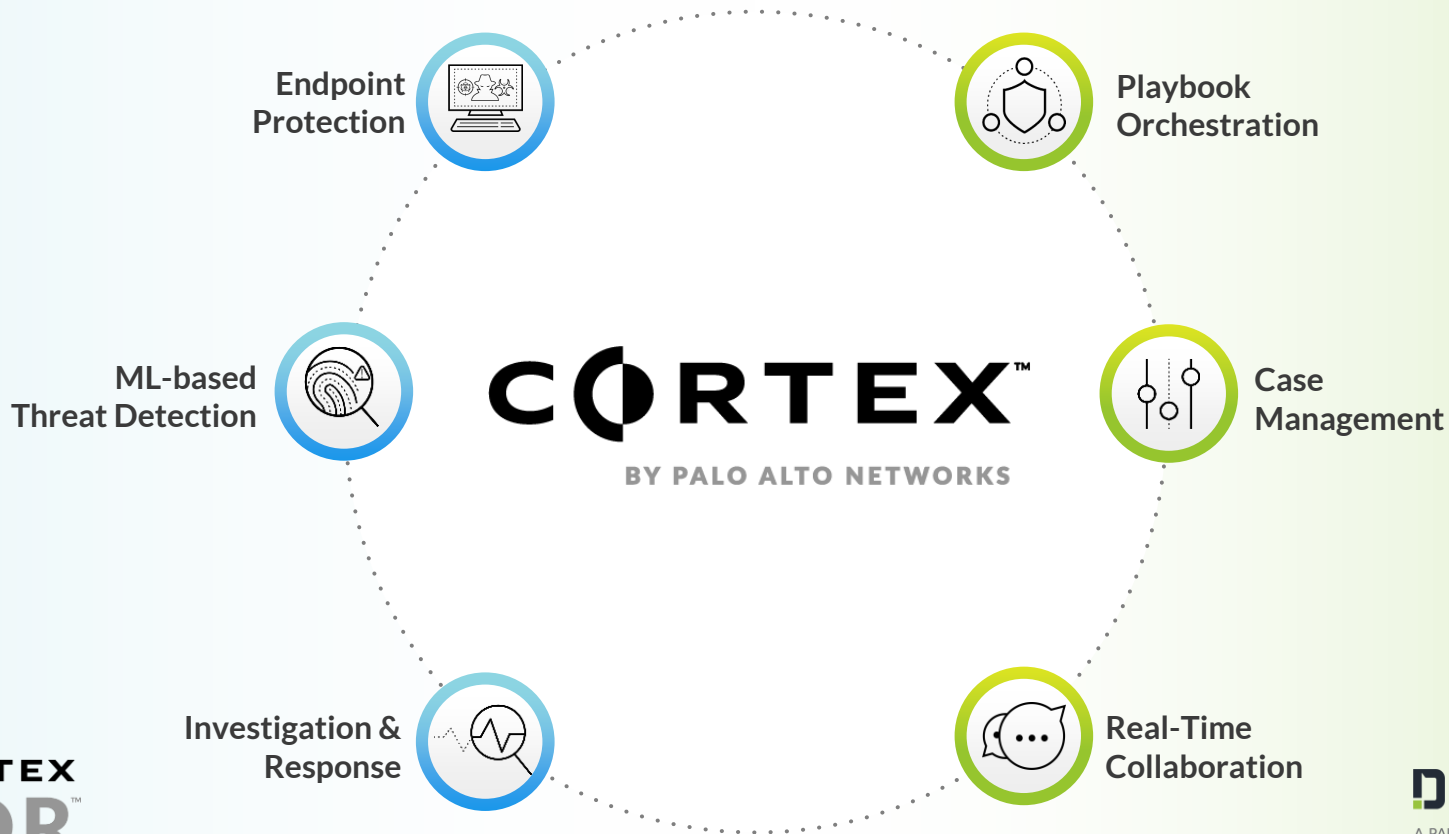
**Cortex XDR
& AutoFocus**



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

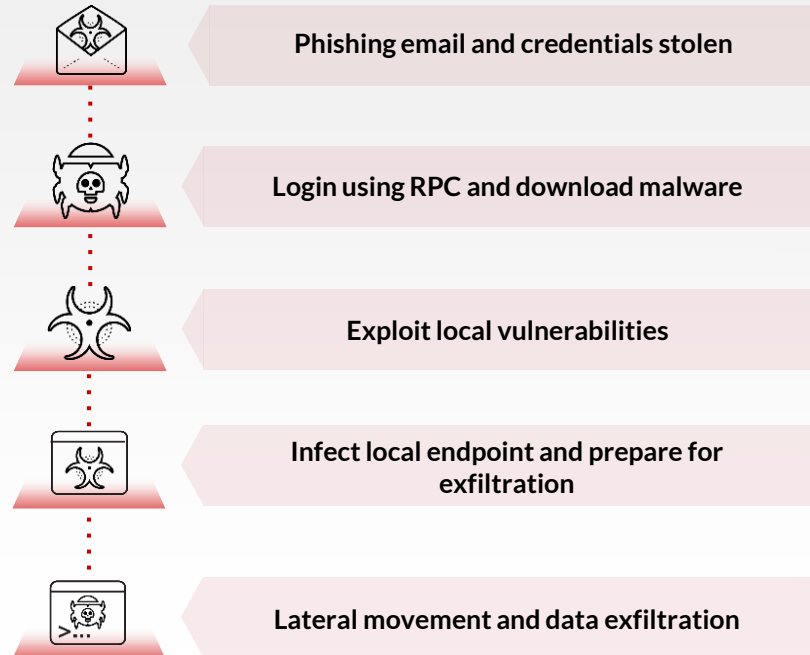


Endpoint Detection & Response is Limited

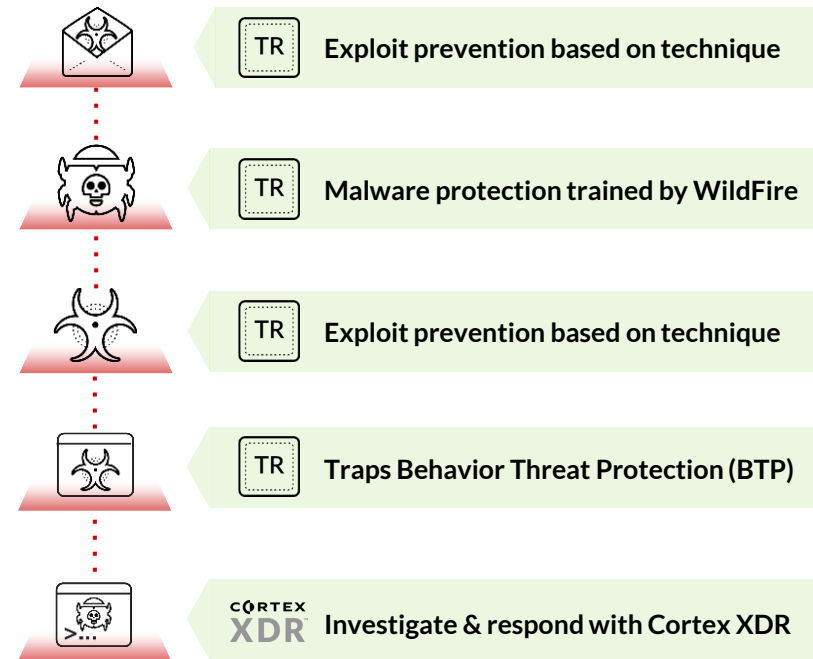
EDR is locked to the endpoint and lacks a solution for unmanaged devices

Our Approach: Endpoint protection

Before



After



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



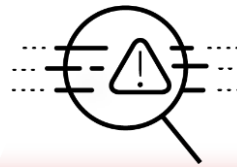
You Can't Prevent All Attacks

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

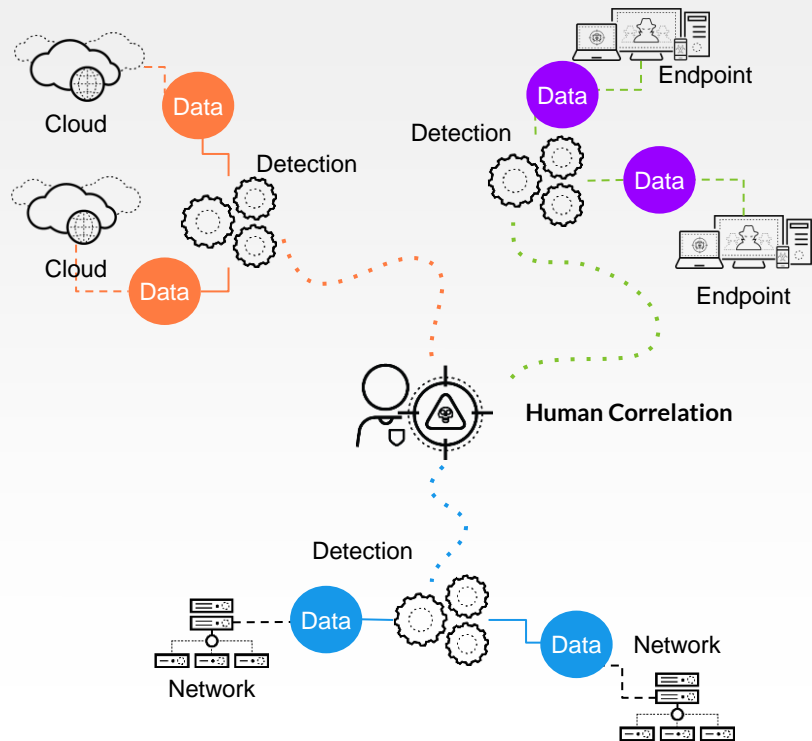


Anomaly Detection is not a "Human" Job

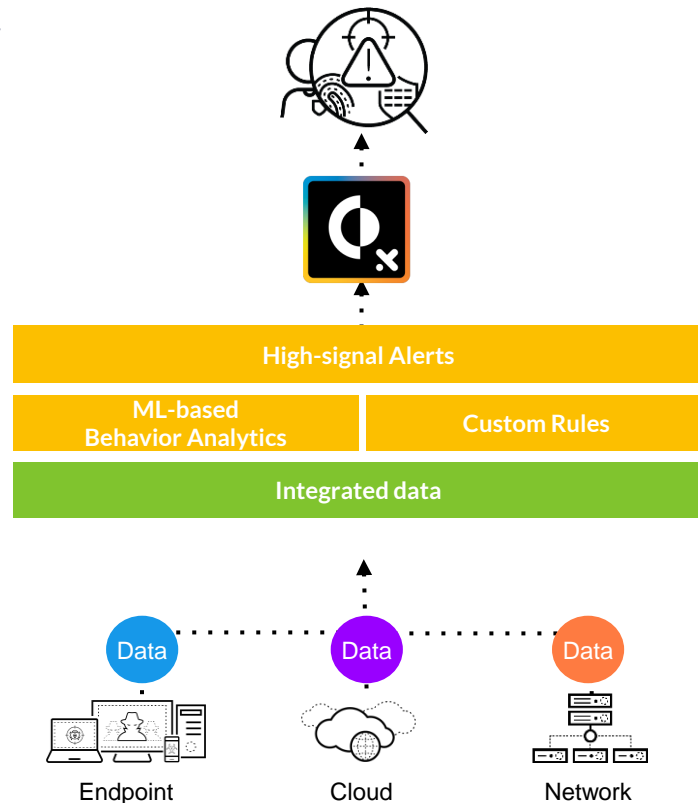
Detecting anomalies
requires analyzing a
comprehensive data set

Our Approach: Threat detection

Before



After



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

Use Case: Investigation & Response



The Problem: Threat containment takes too long



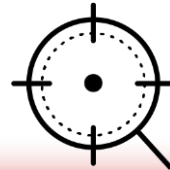
Limited Context Across Multiple Alerts

Analysts have to review each alert individually



Investigations Are Highly Manual

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

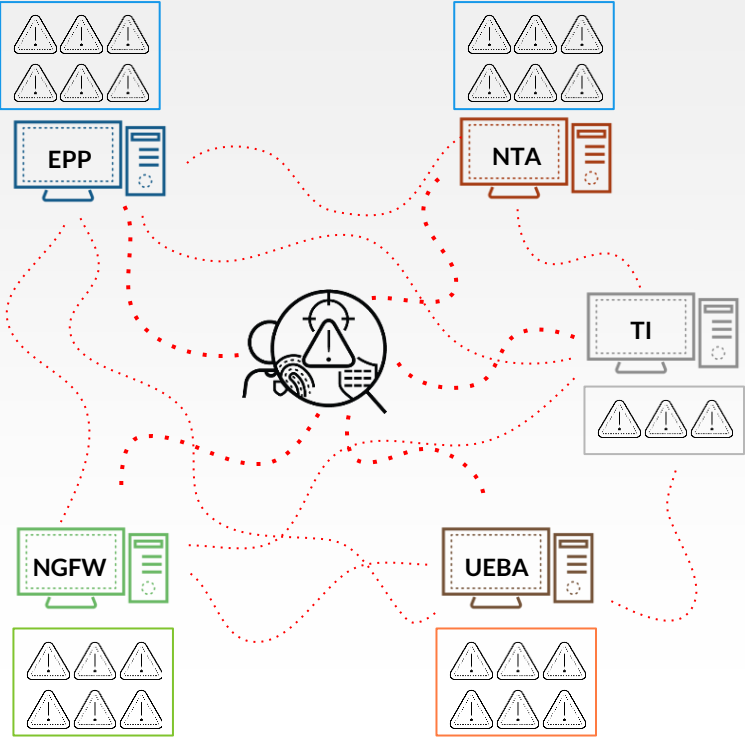


Finding Root Cause Takes Too Long

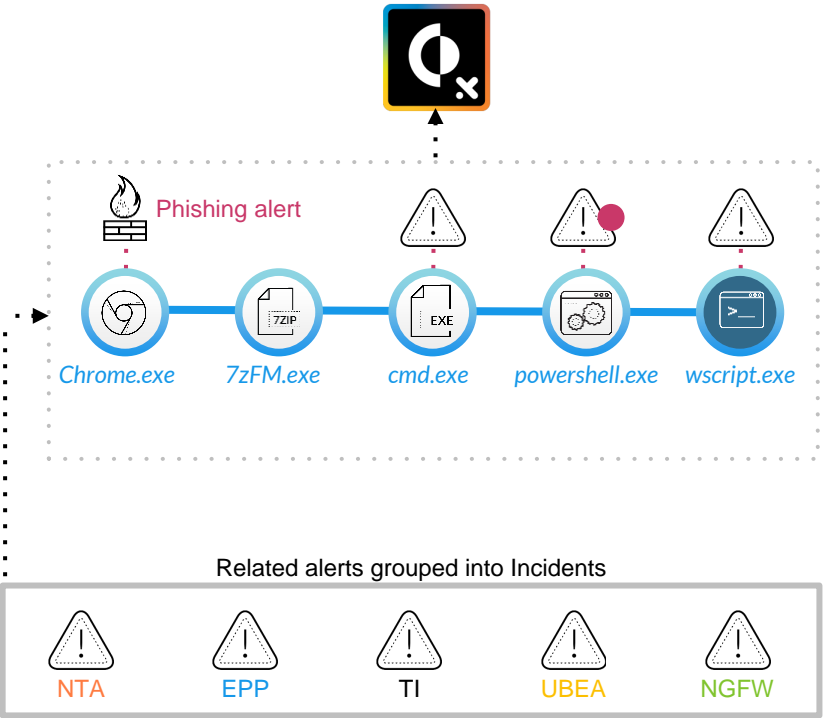
By the time you find root cause, the attack has progressed

Our Approach: Investigation & response

Before



After

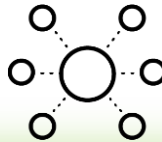


Key Differentiators: Cut investigation & response time



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: Phishing Response (Demisto)



The Problem: Phishing response is hard



High Alert Volumes

Phishing attacks are frequent, easy to execute, and act as the entry vector for most security attacks



Disjointed Processes

Security teams must coordinate across email inboxes, threat intel, NGFW, ticketing, and other tools for phishing response



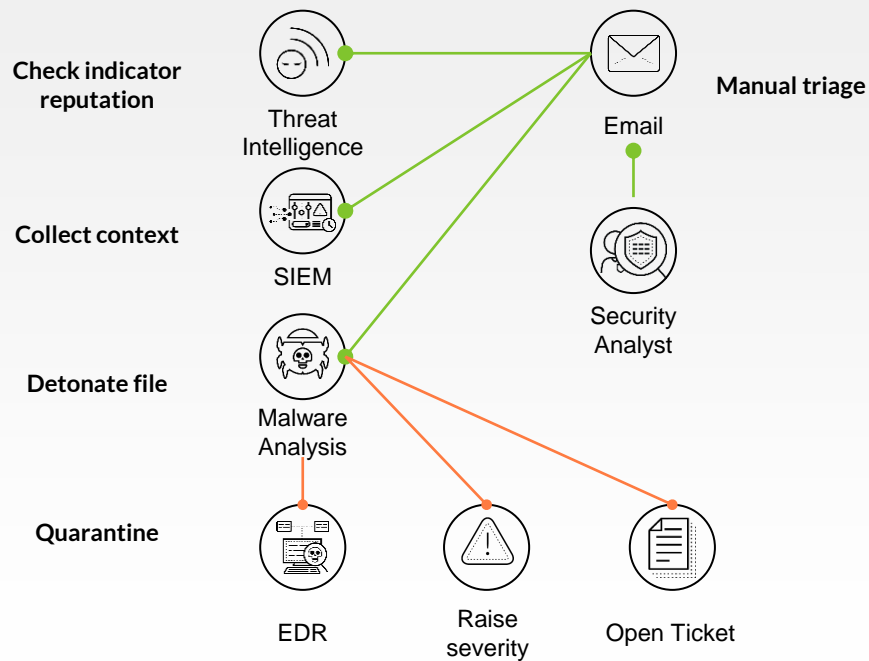
Ever-Present and Growing

95% of all attacks on enterprise networks are a result of spear phishing¹

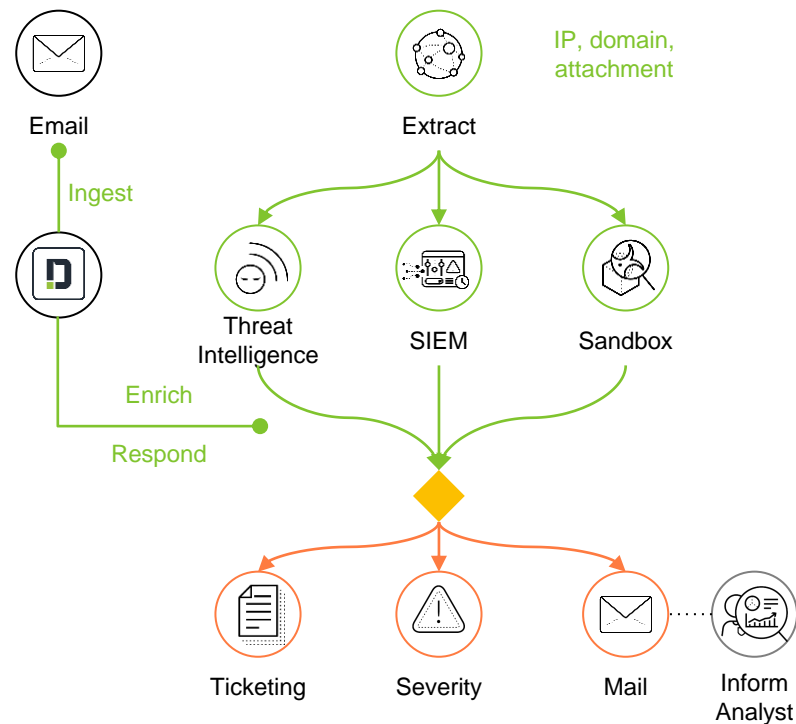
¹Source: <https://www.networkworld.com/article/2164139/network-security/how-to-blunt-spear-phishing-attacks.html>

Our Approach: Phishing response

Before



After

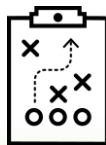


Key Differentiators: Automate and standardize phishing response



Product Integrations

Demisto integrates with all security tools commonly used for phishing enrichment and response



Intuitive Response Playbooks

OOTB and custom task-based workflows enable security teams to coordinate across teams, products, and infrastructures



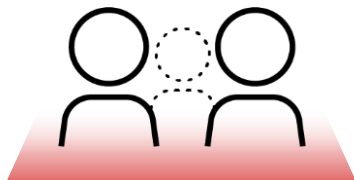
Automated Actions

1000s of automated actions across security tools make scalable phishing response a reality

Use Case: IT And Security Processes Automation (Demisto)

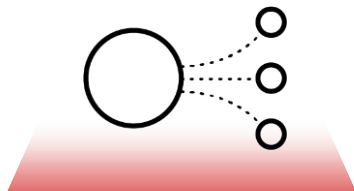


The Problem: Processes are disjointed



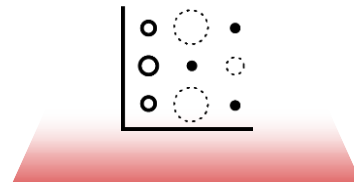
Team Silos

Managing and responding to security incidents involves end users, IT team, NOC team, and other stakeholders



Shifting Context

Coordinating across security tools involves shifting context, leading to rework and fragmented documentation

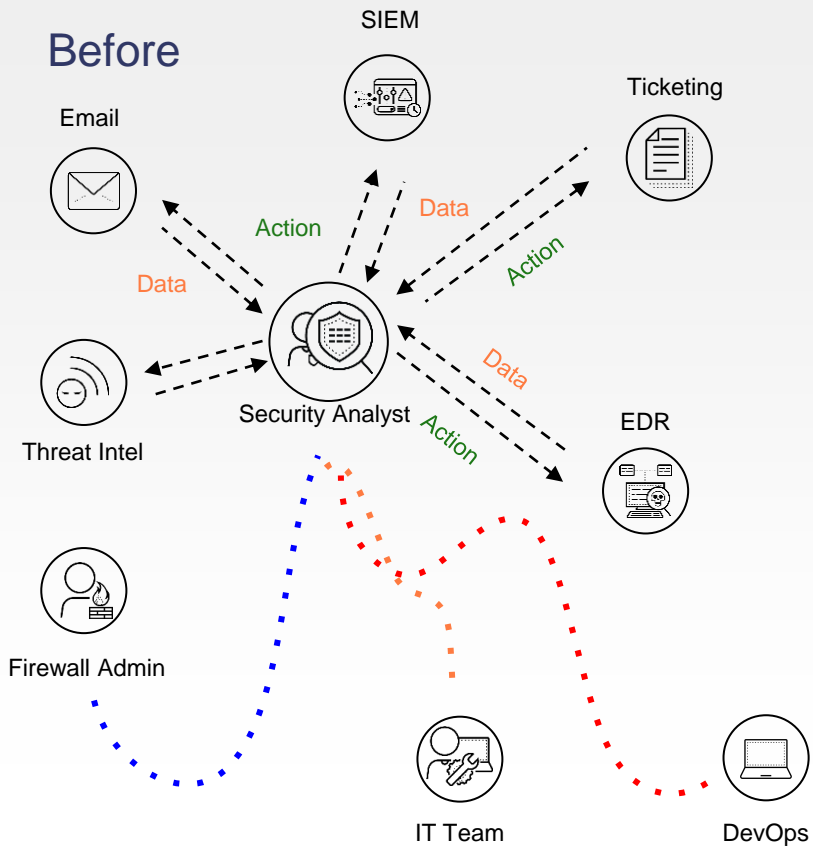


Lack of Metrics

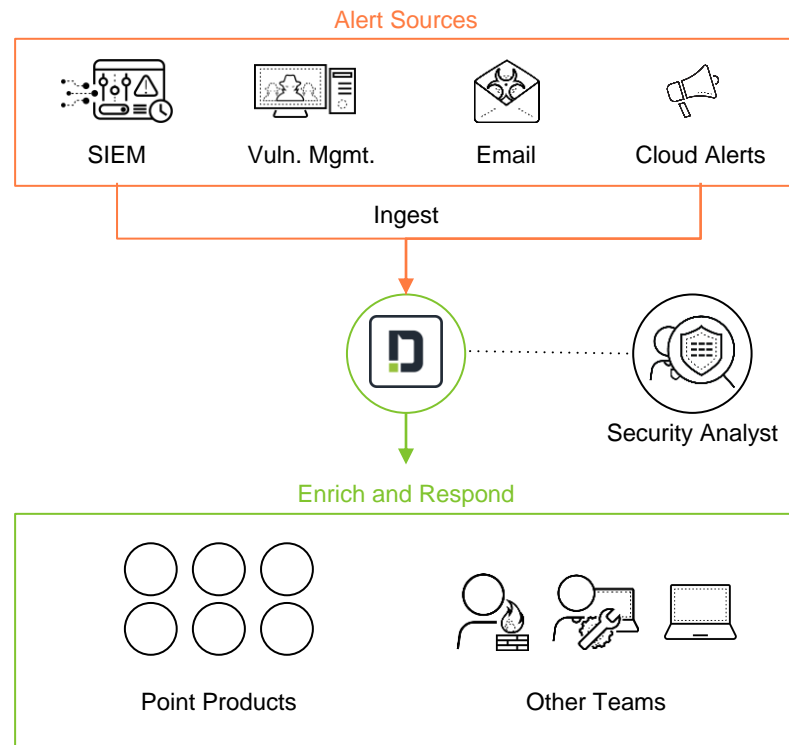
Security teams lack the time, flexibility, and centralized data to visualize relevant metrics and track performance

Our Approach: Security processes

Before



After



Key Differentiators: Centralized incident management with security context



Cross-team Communication

Communicate with end users, security teammates, and other teams, both in real-time and through automated tasks



Security Focused Context

Ingest all security alerts for centralized view and context across the incident response lifecycle



Granular Dashboards

View cross-sections of incident, indicator, and analyst data with custom, widget-driven dashboards and reports

Cortex XDR Detection & Response



Cortex XDR breaks down silos to stop all attacks

CORTEX
XDR™



The new category for
detection & response

Best-in-class prevention

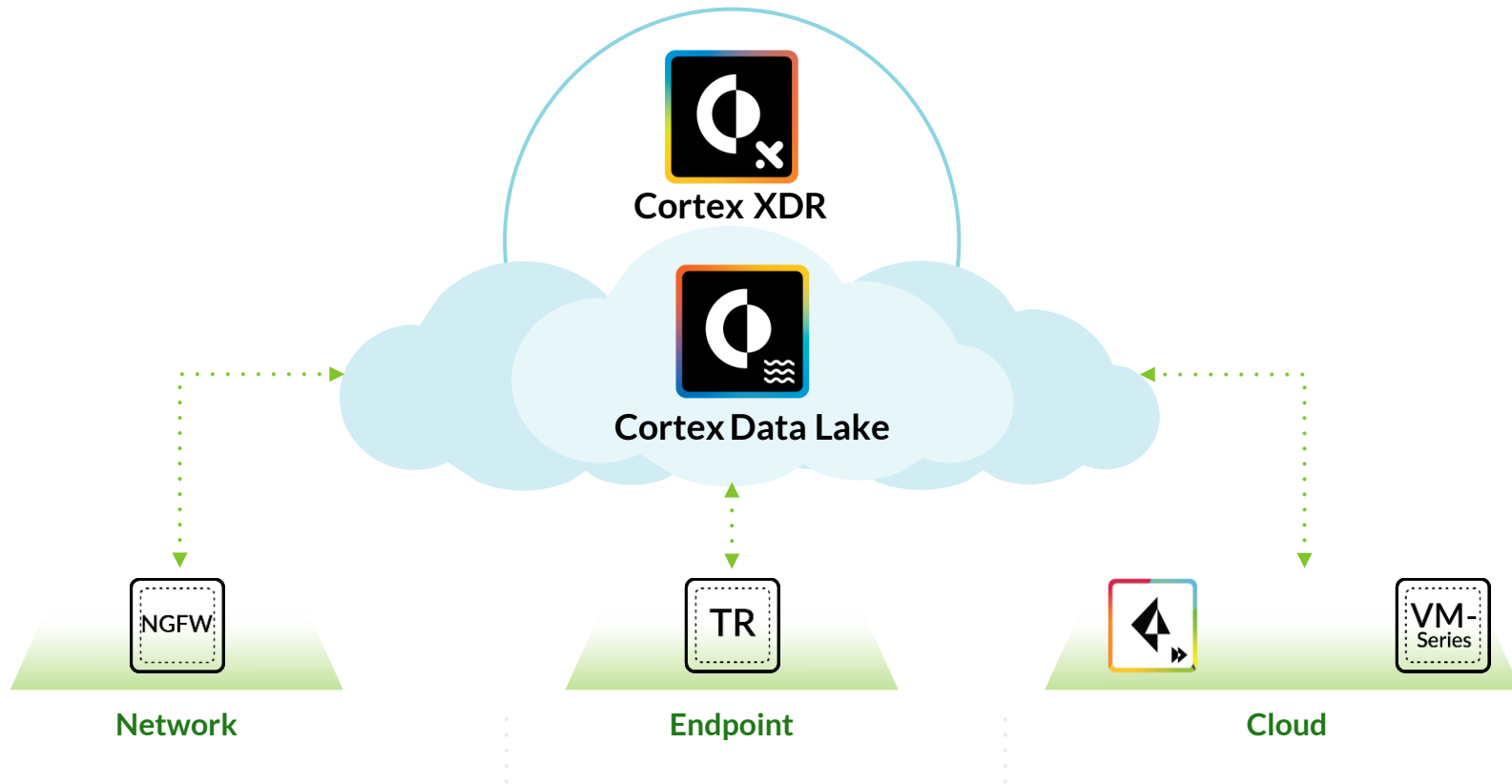
Most comprehensive security data asset

Continuous ML-based detection

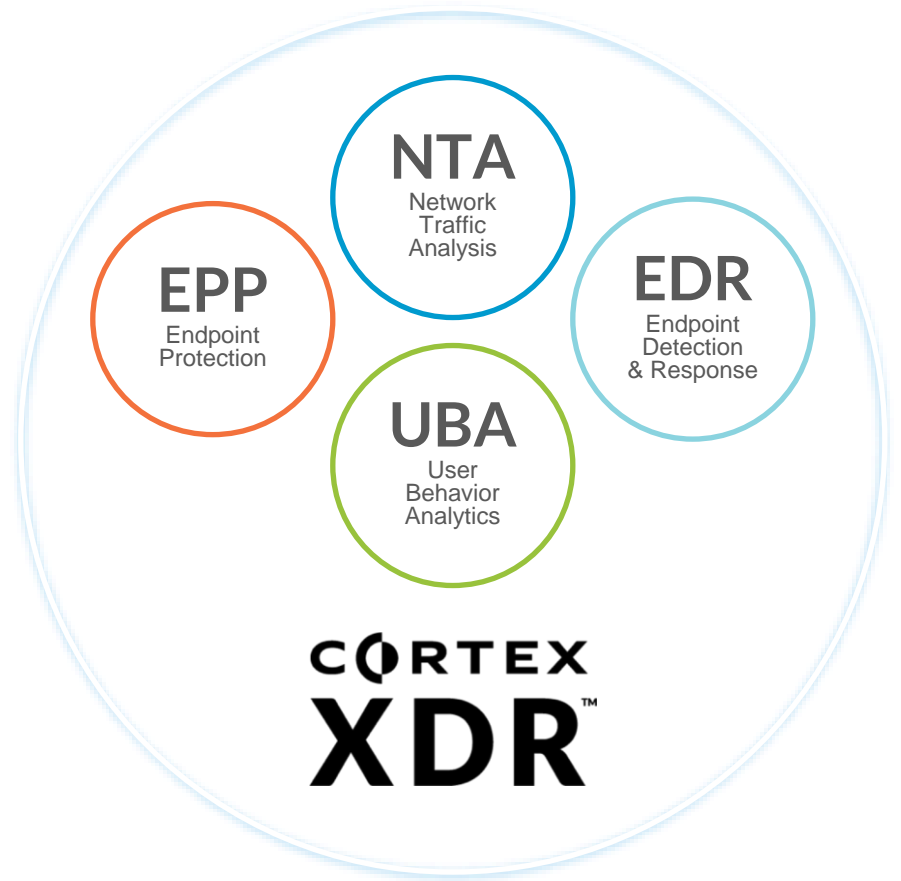
Automated root-cause analysis

Integrated response for network and endpoint

The industry's best security data asset



Breaking down point products operating in silos



Best-in-class prevention with Traps



Prevent all malware

High fidelity local detection
powered by WildFire



Block exploits

Stop based on
exploit techniques



Analyze suspicious patterns

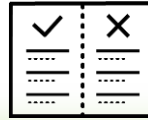
Behavioral Threat Protection
analyzes behaviors together to
flag complex attacks

Continuous ML-based detection



High-signal alerts

Find stealthy threats
with ML & behavioral
analytics



Custom rules

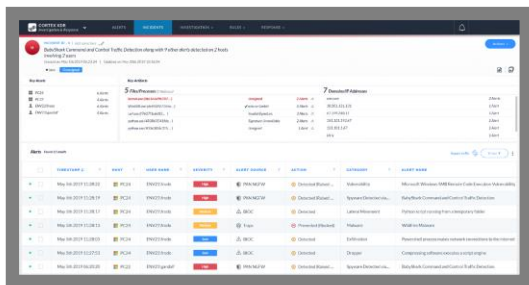
Constantly improve
detection with custom
behavioral rules



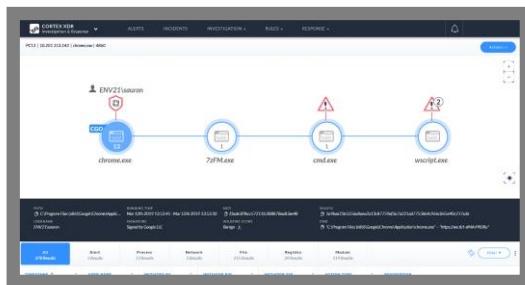
Simplified hunting

Quickly find new threats
with complete evidence
and powerful searches

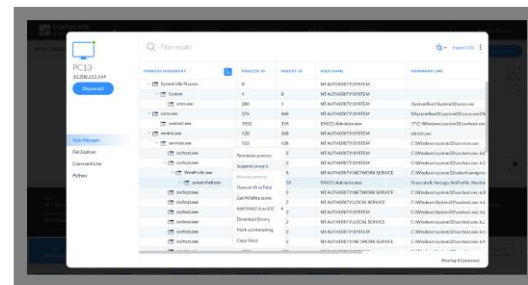
Automate root-cause analysis for investigation & response



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

Augment your team with Cortex MDR partners



Achieve the full potential of Cortex XDR at any maturity level with trusted partners



“

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

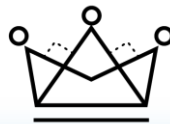
Cortex XDR value



**Reduce risk of data
breach**



**Cut detection &
response times**



**Increase security
operations efficiency**



**Reduce alert
fatigue & turnover**



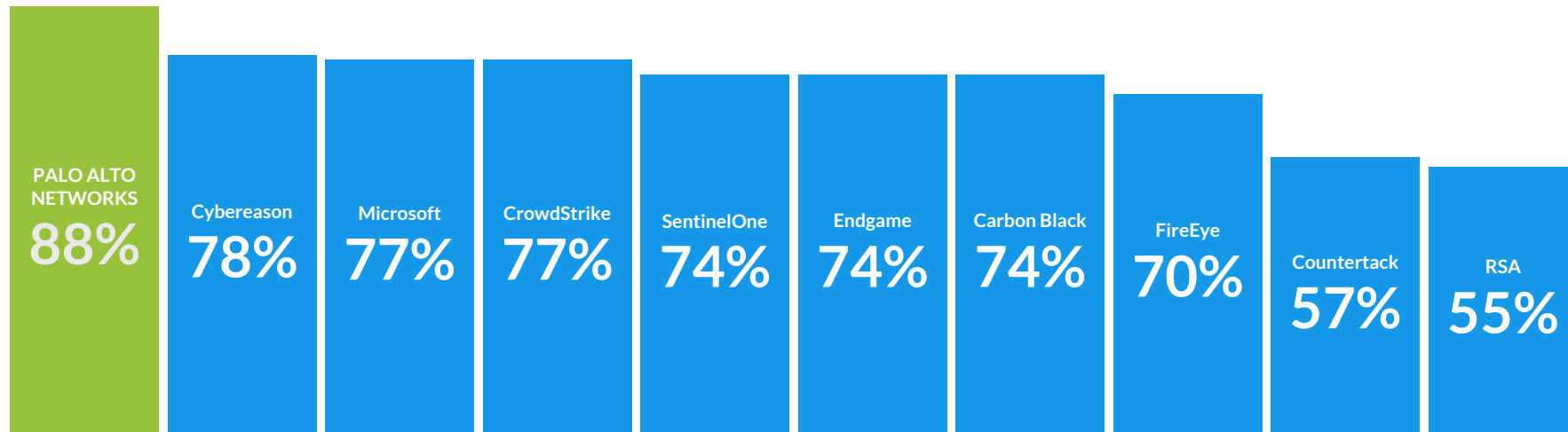
**Maximize detection
& response investments**



**Lower TCO by
44%**

Cortex XDR achieves best MITRE ATT&CK coverage

Scored higher than all other vendors with 93% fewer misses



Attack technique coverage

Demisto: Security Orchestration, Automation, And Response



What is Demisto?

Accelerate Response

Respond to incidents with speed and scale



Hundreds of integrations



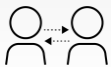
Thousands of security actions



Cross correlations

Collaborate & Learn

Improve investigation quality by working together



Virtual War Room



Investigation Canvas

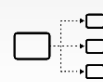


Machine Learning



Standardize Process

Respond to incidents the same way every time



Task-based workflows



Visual playbook editor



SLA & metric tracking

Reduce Risk

Reduce business and security risk



Dashboards & reports



Auto documentation



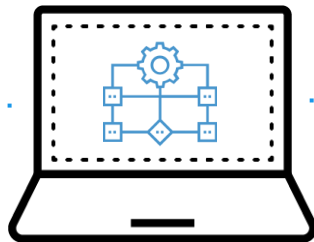
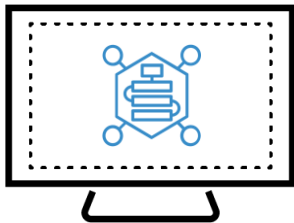
Improved ROI

What is SOAR?

Security **O**rchestration, **A**utomation, and **R**esponse

Orchestration

- Playbooks, runbooks, workflows
- Logically organized plan of action
- Controlling, activating security product stack from central location



Automation

- Automated scripts
- Extensible product integrations
- Machine execution of playbook tasks

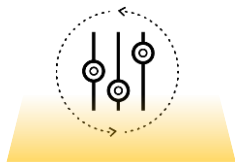
Response

- Case management
- Analysis and reporting
- Communication and collaboration



Respond, automate, and manage with Demisto

Alert
sources



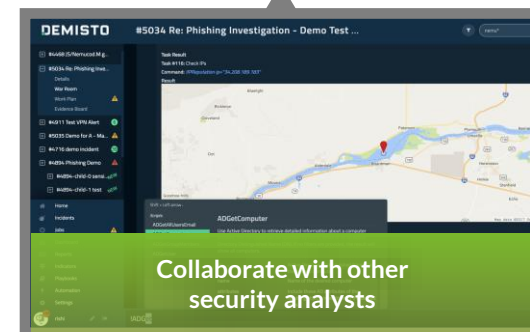
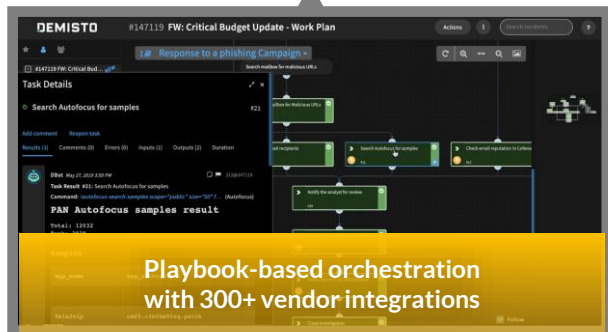
Respond and automate



Manage incidents

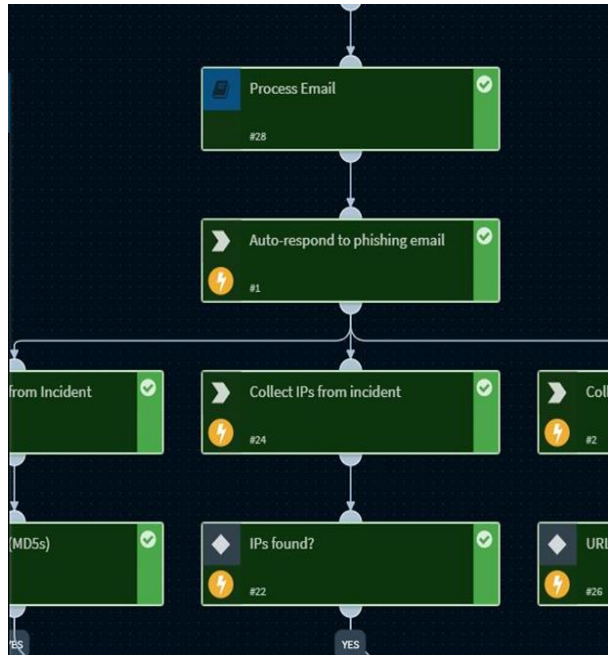


Collaborate and learn



Why Demisto?

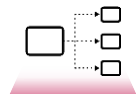
Demisto is a workflow automation engine



Respond to incidents with **speed** and **scale**



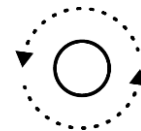
100s of product integrations



1000s of security actions



Visual playbook editor



Workflow Automation Engine



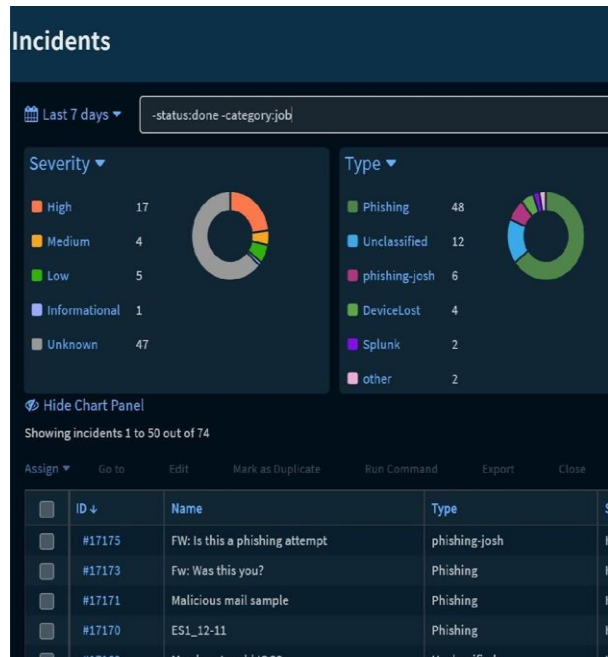
Security Ticketing System



Collaboration Platform

Why Demisto?

Demisto is a security ticketing system



Standardize process across
products, teams and use cases



Ingest, search, and query
ALL security alerts



SLA/Metric tracking



Dashboards and Reporting



Workflow
Automation Engine



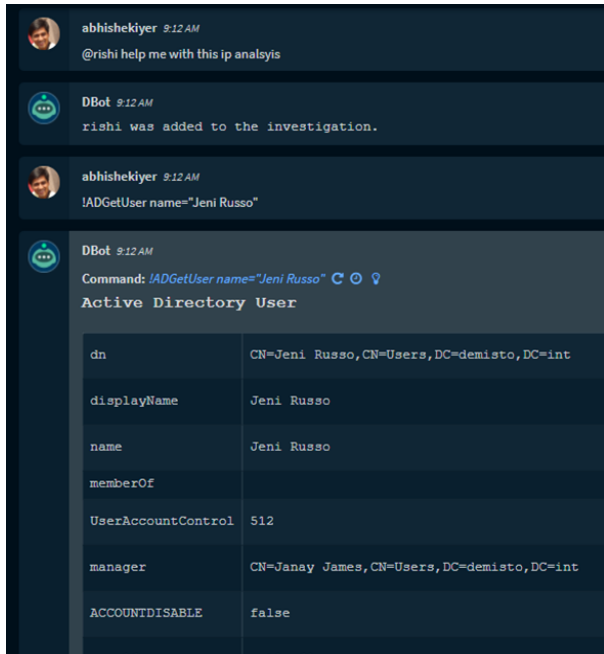
Security Ticketing
System



Collaboration
Platform

Why Demisto?




Demisto is a collaboration platform



abhishekiyer 9:12 AM
@rishi help me with this ip analysis

DBot 9:12 AM
rishi was added to the investigation.

abhishekiyer 9:12 AM
!ADGetUser name="Jeni Russo"

DBot 9:12 AM
Command: !ADGetUser name="Jeni Russo"   
Active Directory User

dn	CN=Jeni Russo,CN=Users,DC=demisto,DC=int
displayName	Jeni Russo
name	Jeni Russo
memberOf	
UserAccountControl	512
manager	CN=Janay James,CN=Users,DC=demisto,DC=int
ACCOUNTDISABLE	false

Improve investigation quality by
working together



Virtual War Room



Real-time security actions



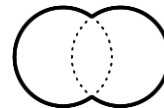
Auto-documentation



**Workflow
Automation Engine**

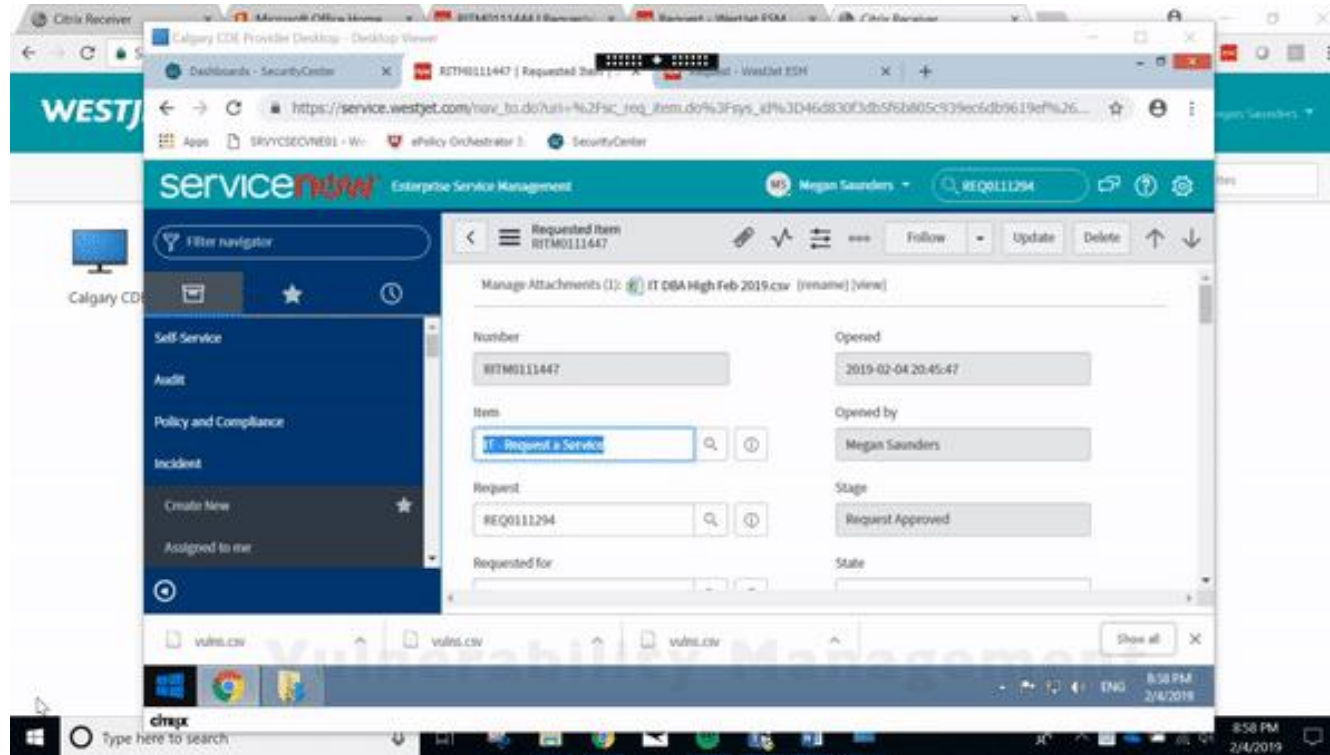


**Security Ticketing
System**



**Collaboration
Platform**

Before Demisto



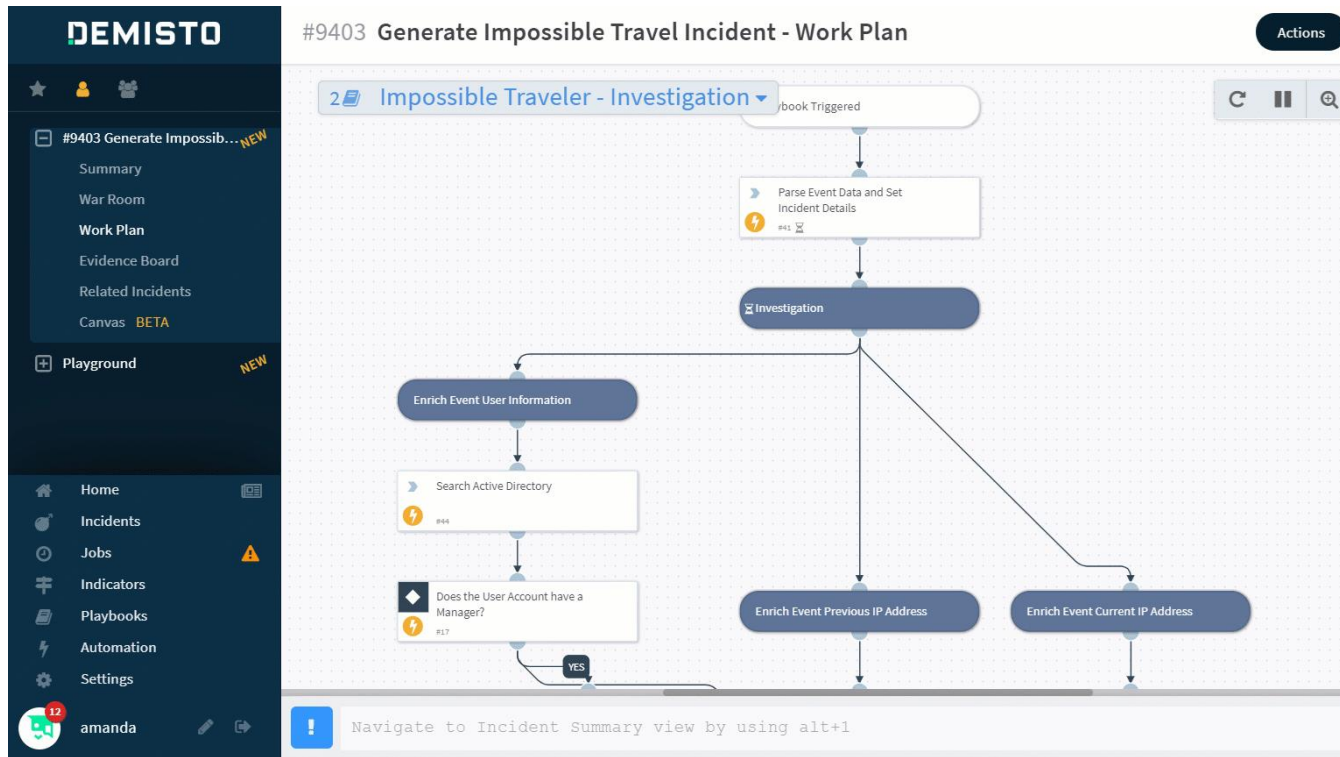
Disparate
alert sources

Lack of
defined process

Repetitive and manual
actions

Lack of product
interconnectivity

After Demisto



All alerts flowing
into one console

Standardized
and enforceable
processes

Automated high-
quantity
actions

Cross-product
coordination

Breadth of Demisto use-cases



Breadth of Demisto integrations

Analytics and SIEM



Threat Intelligence



Malware Analysis



Endpoint



Network Security



Authentication



Email Gateway



Ticketing



Messaging



Cloud



...and more!



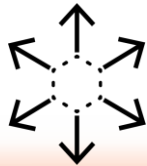
“

Demisto's process modularity and automation has helped us stay agile as we onboard new technologies. Demisto is really the constant 'sheet music' that keeps our security orchestra going.

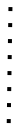
”

Sean Hastings, Senior Information Security Analyst

Demisto value



**Standardize and scale
processes**



**Reduced weekly
alerts from
10,000 to 500**



**Lower response times
with automation**



**Reduced response
times from
3 days to 25 minutes**



**Coordinate actions
across security products**



**Automated 30% of
incidents for
1 FTE time saved**

*Real stats from Demisto customers

“

Launched in 2015, Demisto rapidly became one of the most visible security orchestration, automation and response (SOAR) vendors, outshining vendors launched years earlier. An early focus on user interface (and not just the APIs), its inclusion of machine learning, usable Slack integration, and sizable stable of out-of-the box integration with tools and online services makes it a popular SOAR tool.

”

Anton Chuvakin, Ex-Research VP, Gartner

Demisto successfully maps with all of Gartner's recommended capabilities for SOAR vendors.

[View Full PDF](#) 



"Cool Vendor" in Security Operations and Vulnerability Management, 2018

Palo Alto Networks: Better Together



SECURE THE ENTERPRISE



SECURE THE CLOUD



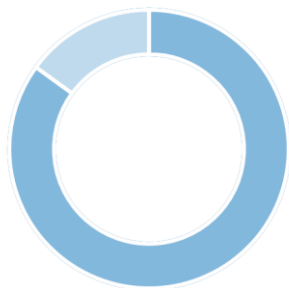
SECURE THE FUTURE



The world's leading cybersecurity company

85

of Fortune 100
rely on Palo Alto Networks

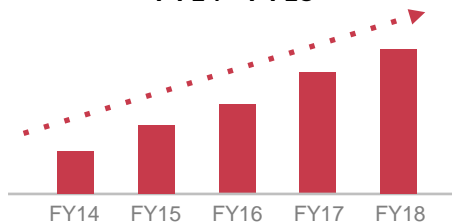


63% of the Global 2K
are Palo Alto Networks customers

#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

Next steps

**Get a Hassle-Free
Cortex XDR Demo**



**Take Demisto
For a Spin**



Thank You

paloaltonetworks.com

Email: name@paloaltonetworks.com

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



CORTEX™
BY PALO ALTO NETWORKS