Trust no 1

Nije sve SF

Vladimir Vučinić, Net++ technology

Endpoint Security

Data and Threat Security Everywhere

Endpoint Security is Mission Critical for Businesses

Endpoints are **the primary target** of attackers

If a single threat (e.g. targeted ransomware) gets through, it can **bring down the business**

Endpoint security **stops more threats** vs other control points, and provides **deep visibility** on attacks

Effective Endpoint security **reduces the customer's operational burden** or business disruption

Symantec™ by Broadcom Software

Symantec
Endpoint Security Complete

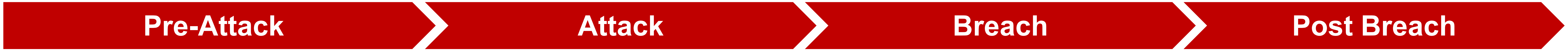
Industry-best protection across all devices and OSes

Windows, Mac, Linux, iOS, Android, Windows 10S

- Endpoint Protection (evolution of SEP)
- Endpoint Detection & Response
- Threat Hunter & Threat Intelligence
- Adaptive Protection
- Application Control
- Threat Defense for Active Directory

Customers Need Symantec Endpoint Security Complete

Technology Consolidation & Innovation Across the Entire MITRE ATT&CK Chain



ATTACK SURFACE REDUCTION

- Breach Assessment
- Device Control
- Application Control

ATTACK PREVENTION

- Machine Learning-driven Exploit and Malware Prevention
- Behavior-based Prevention
- Network Integrity, Wi-Fi Reputation, and Smart VPN

BREACH PREVENTION

- Deception
- Active Directory Defense
- Auto-managed Policies
- Network Firewall & Intrusion Prevention

DETECTION & RESPONSE

- Flight Data Recorder
- Behavioral Forensics
- Threat Hunter with Machine Learning and Expert Analysis
- Rapid Response

Adaptive Protection – Threat landscape insights, custom behavioral insights, and recommendations

Single Agent – all operating systems: Windows, Mac, Linux, Windows S Mode, Android, and iOS – including servers

Global Intelligence Network – World’s largest civilian cyber intelligence network

Integrated Cyber Defense – Enabling Symantec and third-party integrations

Investing in Symantec Endpoint Security Complete (SESC)

Leading-edge Security

- Custom attack surface reduction via Adaptive Protection
- Protect against lateral movement attacks via Threat Defense for AD
- Mitigate targeted attacks with accuracy and confidence via Threat Hunter

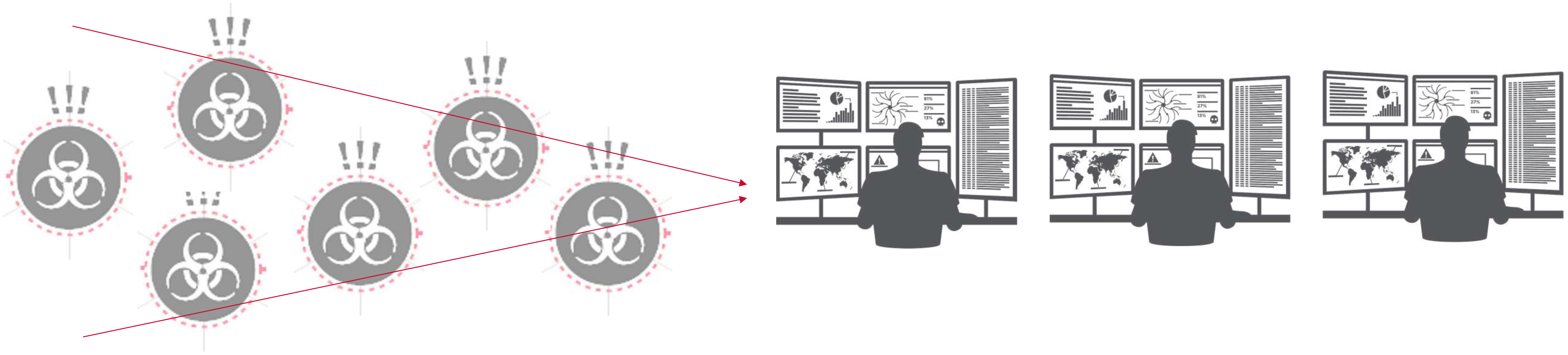
Ease of Deployment

- Single agent for Endpoint Protection and Web traffic redirection
- Available on-premises, in-cloud or hybrid
- Investment in operational continuity

High Value Integrations

- Zero Trust Network Access (ZTNA) to private applications
- Cross-control-point data correlation
- Device health for network security

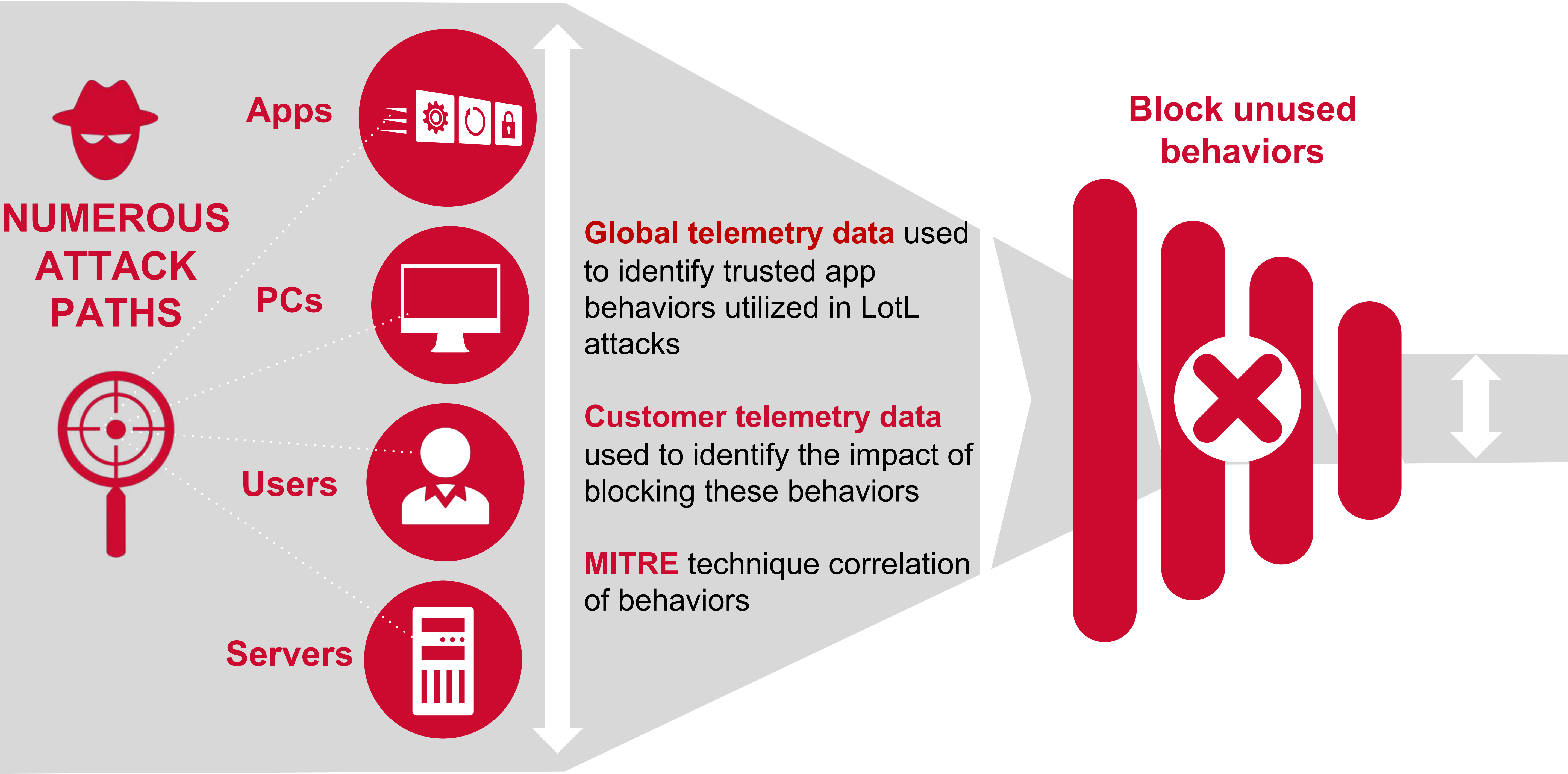
An Ounce of Prevention is Worth a Pound of Detection & Response



- Without good prevention, more attacks get through
- When attacks get through, there’s a greater burden on the SOC
- Incident response is expensive; Symantec’s prevention helps reduce costs

Adaptive Protection | Prevent Living off the Land Attacks

POTENTIAL ATTACK PATHWAYS



Global telemetry data used to identify trusted app behaviors utilized in LotL attacks

Customer telemetry data used to identify the impact of blocking these behaviors

MITRE technique correlation of behaviors

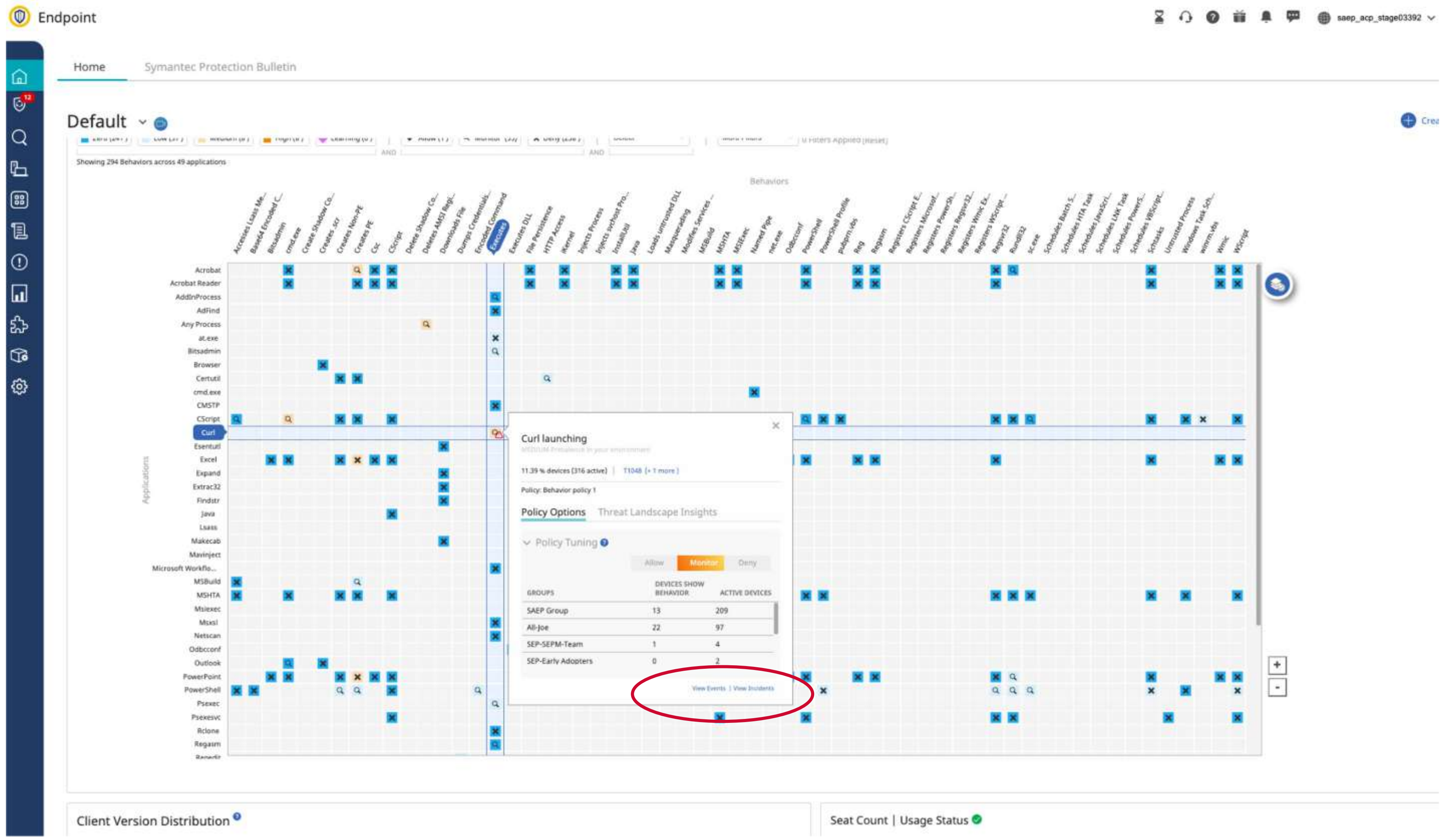
With Adaptive Enabled:

- Prevention that is **unique** to your organization
- Prevention that **adapts** to your organization needs
- **Increasingly difficult** for attackers to perform **lateral movement**

Mapping Detection to Prevention Controls

MITRE ATT&CK Framework for Endpoints

Most detections can be prevented



Curl launching

MEDIUM Prevalence in your environment

11.39 % devices (316 active) | T1048 (+ 1 more)

Policy: Behavior policy 1

Policy Options | Threat Landscape Insights

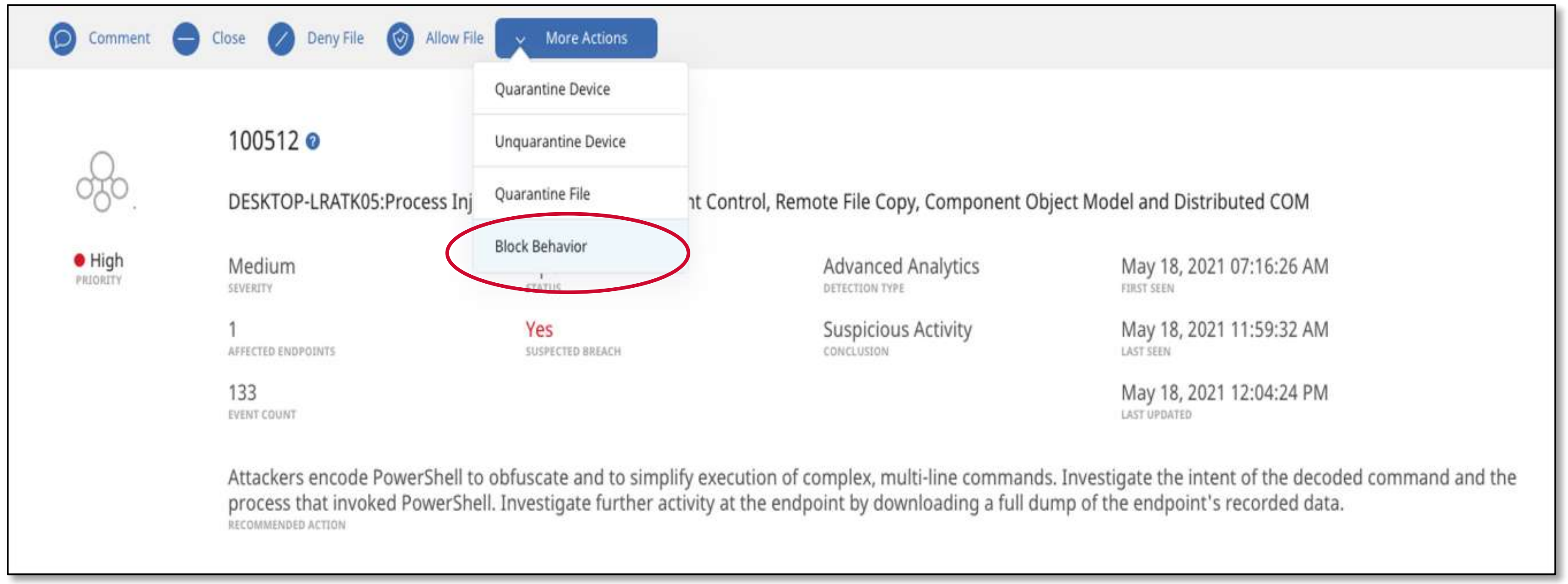
Policy Tuning

Allow [✓ Monitor] Deny

GROUPS	DEVICES SHOW BEHAVIOR	ACTIVE DEVICES
SAEP Group	13	209
All-Joe	22	97
SEP-SEPM-Team	1	4
SEP-Early Adopters	0	2

View Events | View Incidents

Granular policy-based controls to detect and block



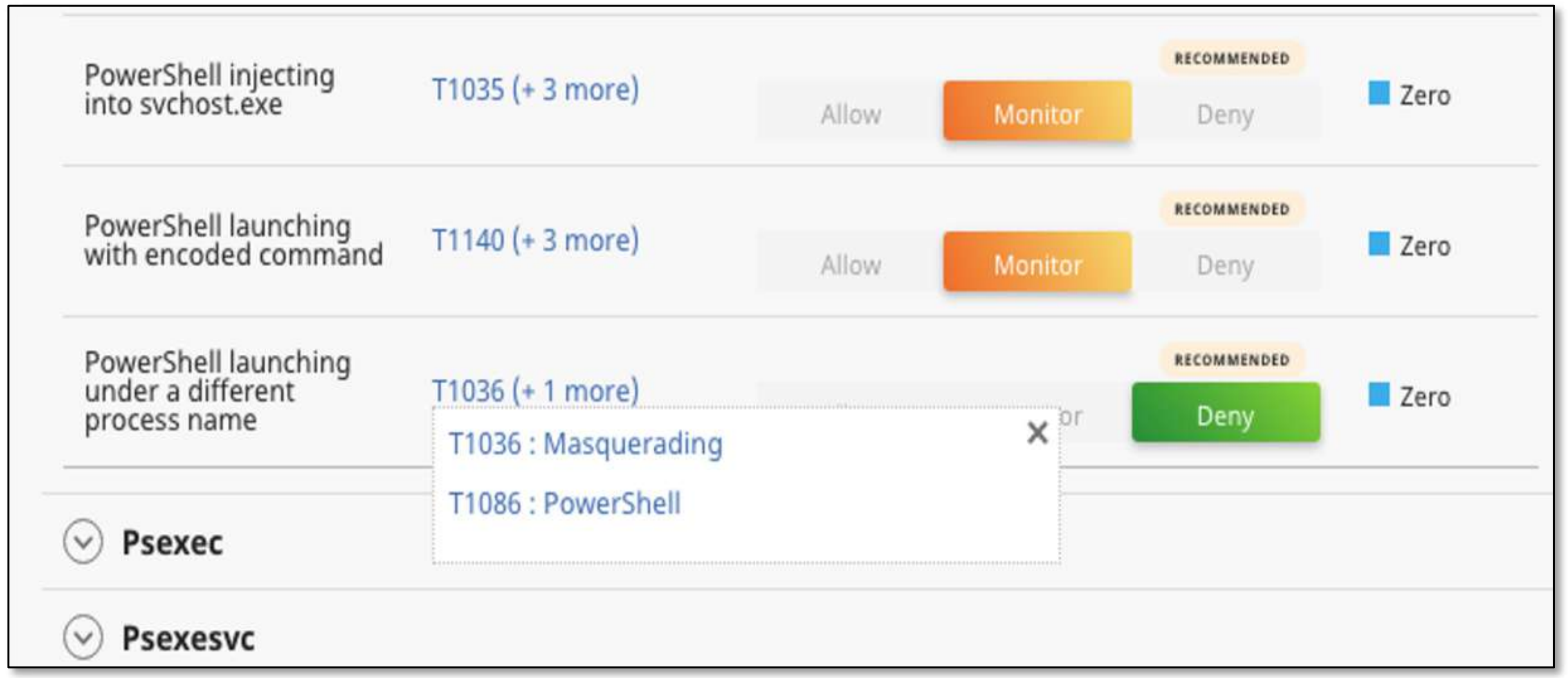
100512

DESKTOP-LRATK05:Process Inj ... nt Control, Remote File Copy, Component Object Model and Distributed COM

High PRIORITY	Medium SEVERITY	STATUS	Advanced Analytics DETECTION TYPE	May 18, 2021 07:16:26 AM FIRST SEEN
	1 AFFECTED ENDPOINTS	Yes SUSPECTED BREACH	Suspicious Activity CONCLUSION	May 18, 2021 11:59:32 AM LAST SEEN
	133 EVENT COUNT			May 18, 2021 12:04:24 PM LAST UPDATED

Attackers encode PowerShell to obfuscate and to simplify execution of complex, multi-line commands. Investigate the intent of the decoded command and the process that invoked PowerShell. Investigate further activity at the endpoint by downloading a full dump of the endpoint's recorded data.

RECOMMENDED ACTION



PowerShell injecting into svchost.exe	T1035 (+ 3 more)	Allow [✓ Monitor] Deny (RECOMMENDED)	Zero
PowerShell launching with encoded command	T1140 (+ 3 more)	Allow [✓ Monitor] Deny (RECOMMENDED)	Zero
PowerShell launching under a different process name	T1036 (+ 1 more)	[✓ Deny] (RECOMMENDED)	Zero

T1036 : Masquerading

T1086 : PowerShell

Psexec

Psexesvc

Threat Hunter Augments the SOC

Bring the combined power of Machine Learning & Expert Analysts to help identify potential breaches

FIND TARGETED ATTACK ACTIVITY

Discover high-fidelity incidents using rich telemetry, machine learning & cloud analytics

RECEIVE INDICATORS FROM EXPERT ANALYSTS

Gain detailed findings from Symantec Threat Expert Analysts including tactics, techniques, and procedures (TTPs) used by adversaries.

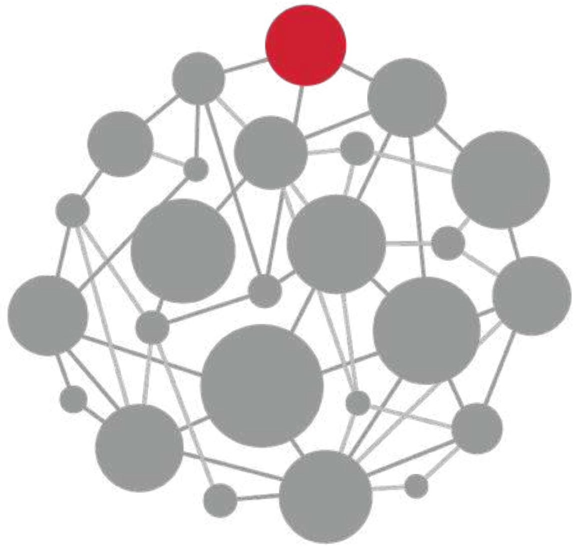
ACCESS FULL GLOBAL INTELLIGENCE

Identify attacks through intuitive access (+ via API) to Symantec’s global security data

Get alerted to overt threats and threats that ‘hide in plain sight’

Threat Intelligence Data Feed

Directly Access Symantec Global Intelligence Network through API



Real-time Threat Enrichment

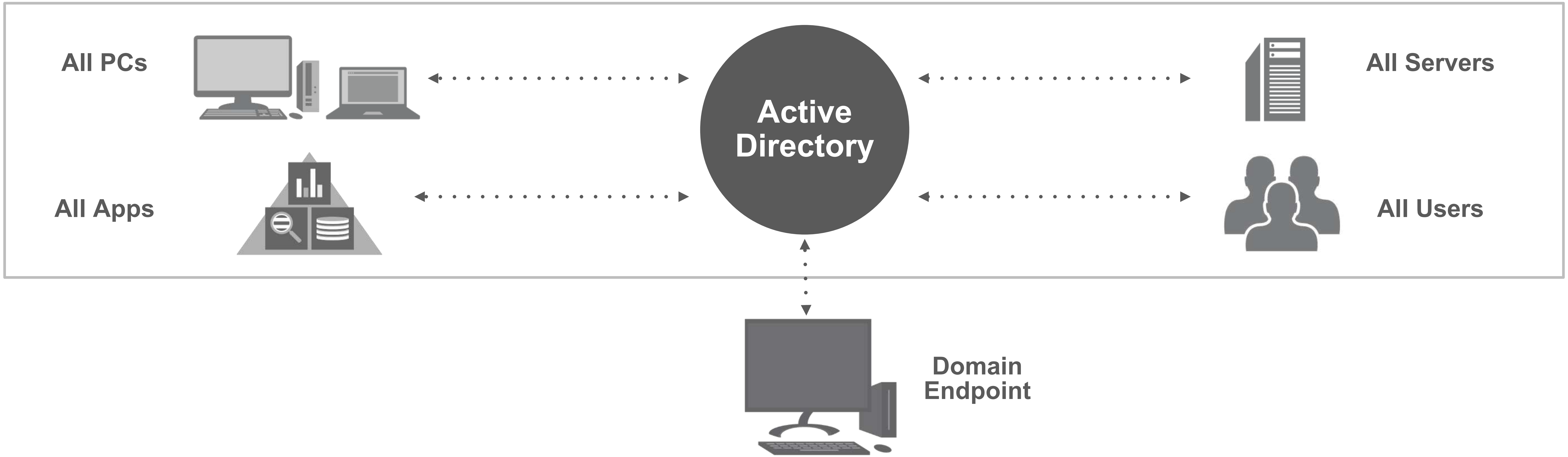
- Accelerate investigations by quickly finding **context on IOCs**
- Identify scope of attack by finding **related IOCs**
- **Integrates** with Threat Intelligence Platforms

Strategic Intelligence to prepare for emerging threats and campaigns

- Learn about threats and campaigns targeting **specific industries and geographies**
- Gain perspective on ongoing **global threats**
- Receive critical threat information, updated daily, monthly, and quarterly

Active Directory is Part of Nearly Every Targeted Attack

With a few queries to active directory at the breached endpoint, an attacker can obtain all information about the corporation and move laterally

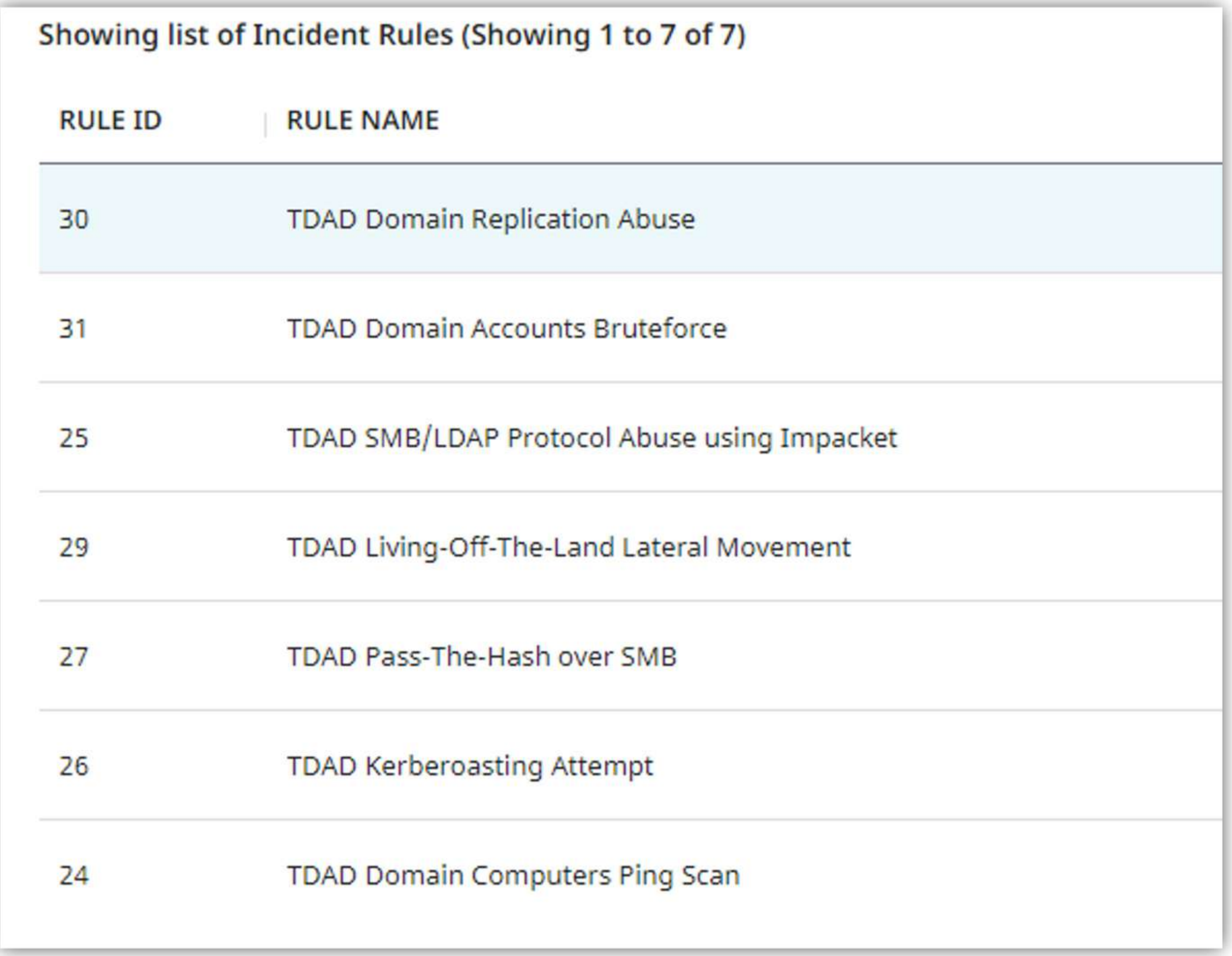


It takes attackers ~7 minutes to compromise and own the domain controller

Protecting Against Active Directory based Attacks

AI-Driven Intrusion Detection, Investigation, and Containment

- Deploy a dissolvable in-memory code on every endpoint connect to the AD domain to obfuscate the AD reconnaissance that stops the first lateral movement attempt right at the endpoint.
  - Obfuscation is AI-driven
  - Built into SES agent
  - No running process, no resources consumed
  - No changes to Active Directory
- Early into the attack cycle, have low false positive and stop the attempt right at the point of breach.



Showing list of Incident Rules (Showing 1 to 7 of 7)

RULE ID	RULE NAME
30	TDAD Domain Replication Abuse
31	TDAD Domain Accounts Bruteforce
25	TDAD SMB/LDAP Protocol Abuse using Impacket
29	TDAD Living-Off-The-Land Lateral Movement
27	TDAD Pass-The-Hash over SMB
26	TDAD Kerberoasting Attempt
24	TDAD Domain Computers Ping Scan

>99% success rate of stopping attackers on their first move

Symantec Endpoint Protection By the Numbers

Game-Changing Security that Scales with the Threat Landscape

Intrusion Prevention

890M+	Threats blocked per month
1.4M+	Ransomware attacks detected per month
576M+	Vulnerability attacks stopped per month
4.6M+	IOT attacks blocked per month

File Inspection Technologies

54.6M+	Detections per month across 50+ distinct engine types
3.7M+	Unknown and 0 day threats blocked per month using advanced Machine Learning
2M+	Attacks in command lines such as living-off-the-land attacks blocked per month

Behavioral Security

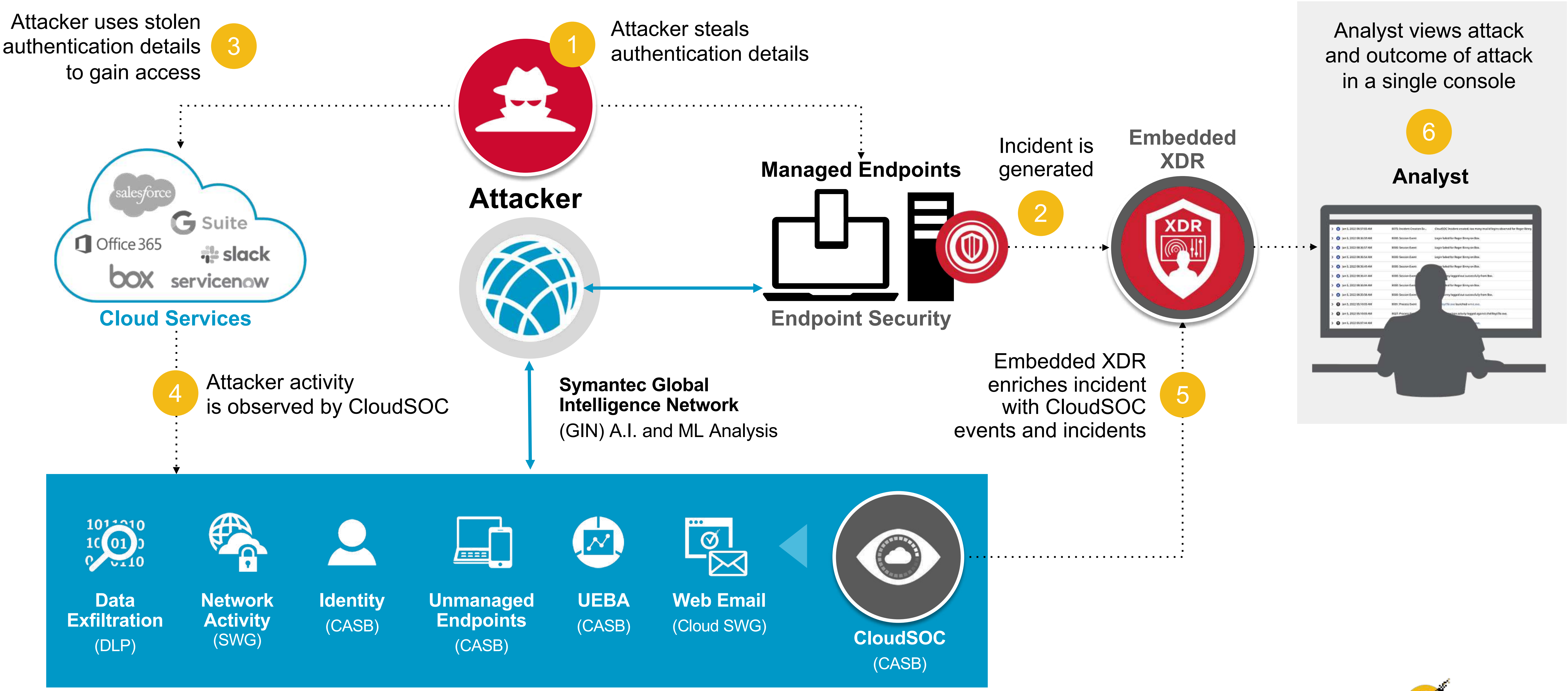
1.4M+	Threats blocked per month
650K+	Powershell related attacks blocked per month
1.7K+	Coinminer attacks stopped
138K+	AMSI events blocked per month

Above data is for May 2022

Symantec by Broadcom Software

Symantec XDR in Action

Correlates suspicious user behavior on endpoints and cloud services



Attacker

1 Attacker steals authentication details

Managed Endpoints

Endpoint Security

Incident is generated 2

Embedded XDR

Analyst views attack and outcome of attack in a single console

6 Analyst

Attacker uses stolen authentication details to gain access 3

Cloud Services

4 Attacker activity is observed by CloudSOC

Symantec Global Intelligence Network
(GIN) A.I. and ML Analysis

Embedded XDR enriches incident with CloudSOC events and incidents 5

Data Exfiltration (DLP)

Network Activity (SWG)

Identity (CASB)

Unmanaged Endpoints (CASB)

UEBA (CASB)

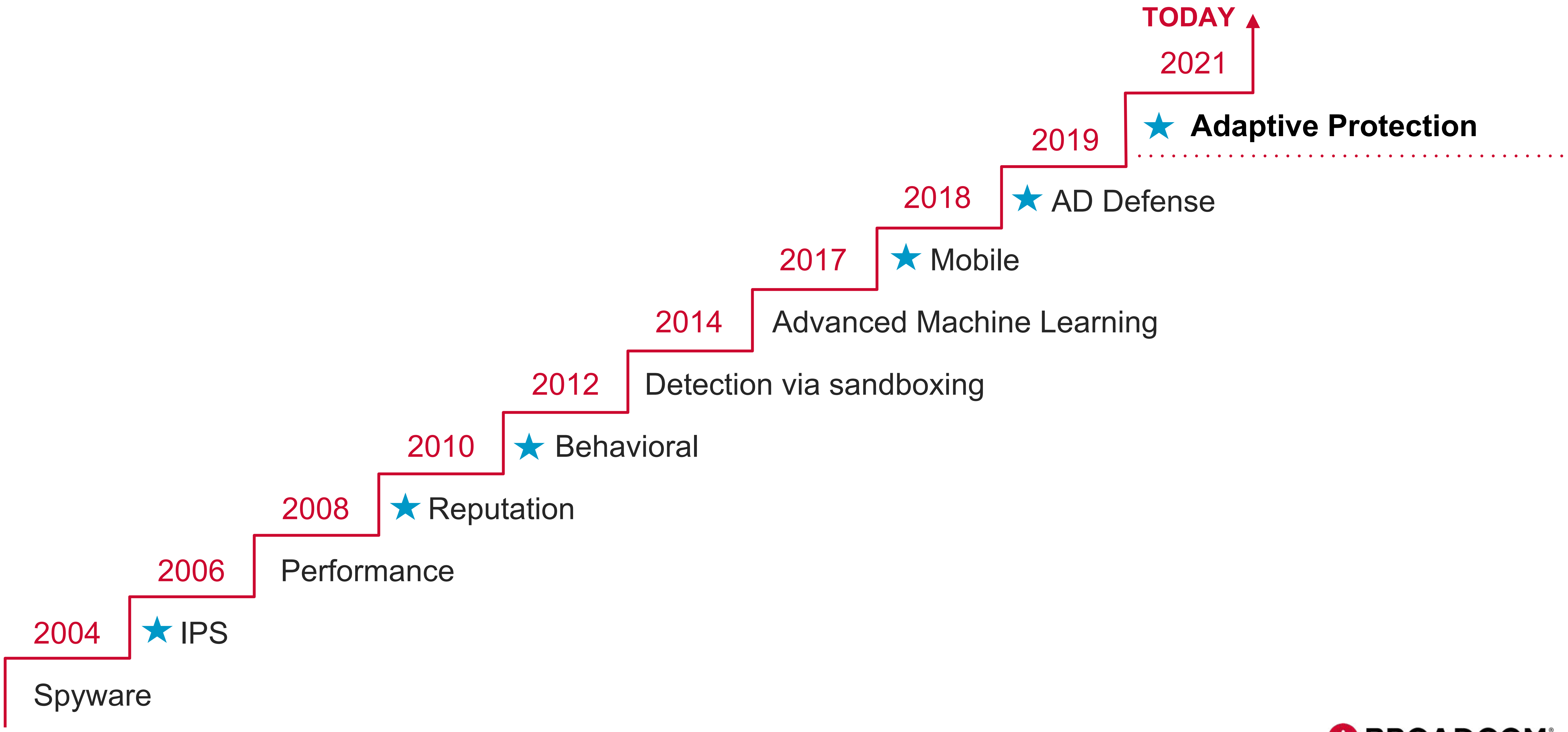
Web Email (Cloud SWG)

CloudSOC (CASB)

Innovation Does Not Stop Here

Symantec’s Protection Innovation Journey

Continually responding to the threat landscape with innovation and new solutions



Spyware

2004 ★ IPS

2006 Performance

2008 ★ Reputation

2010 ★ Behavioral

2012 Detection via sandboxing

2014 Advanced Machine Learning

2017 ★ Mobile

2018 ★ AD Defense

2019 ★ **Adaptive Protection**

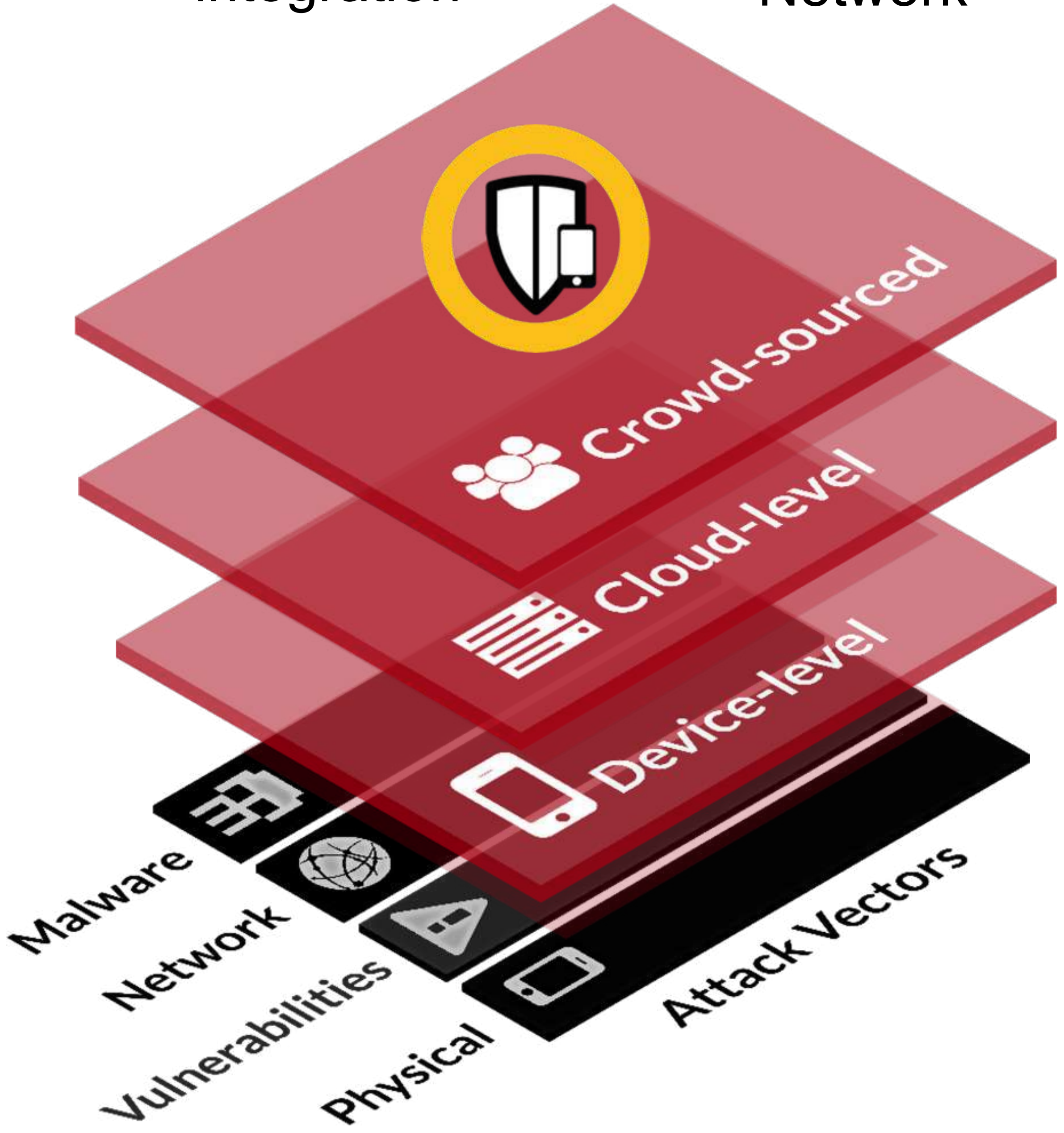
2021

TODAY

Mobile Threat Defense is Included in Symantec Endpoint Security

MOBILE PROTECTION

- Malware
- Web Security integration
- Vulnerabilities
- Network

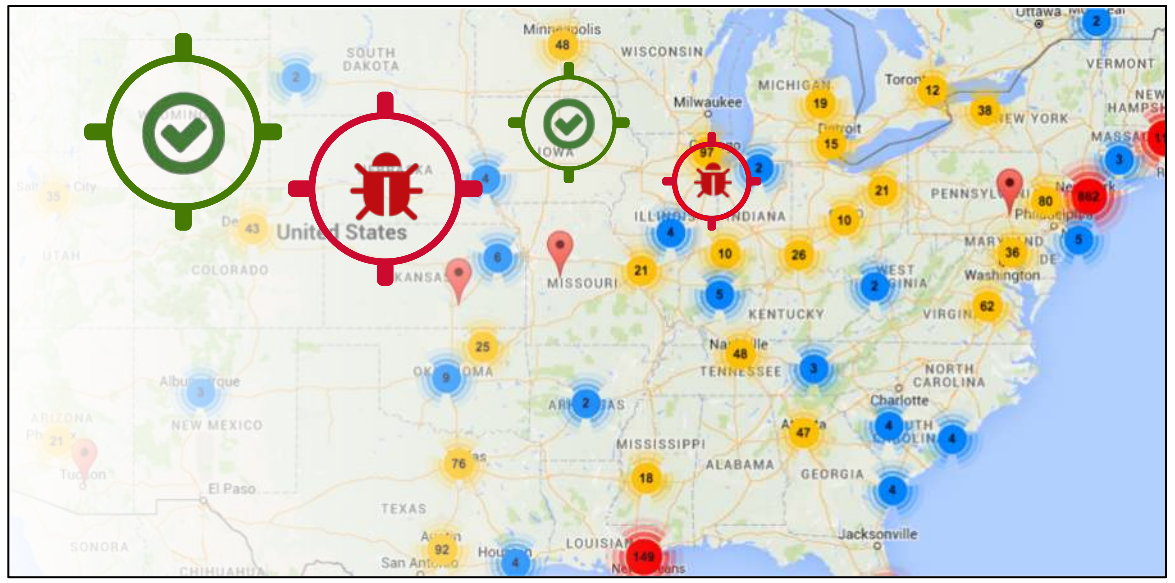


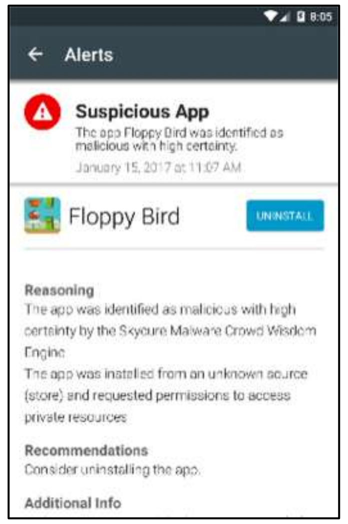
THREAT INTELLIGENCE

- Crowd-sourced
- Integrated Global Intelligence Network
- SEP Mobile research

PUBLIC APP

- Simple deployment & maintenance
- Ensured privacy
- Minimal footprint




8:05

Alerts

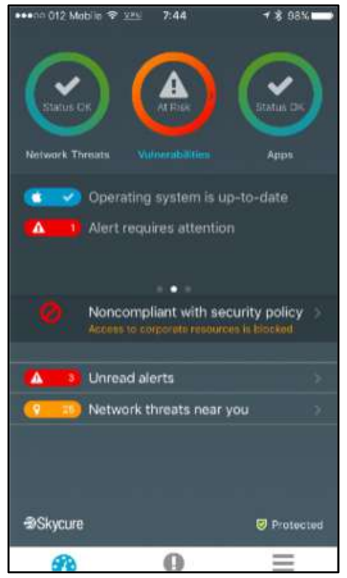
Suspicious App
The app Floppy Bird was identified as malicious with high certainty.
January 15, 2017 at 11:07 AM

Floppy Bird UNINSTALL

Reasoning
The app was identified as malicious with high certainty by the Skycure Malware Crowd Wisdom Engine
The app was installed from an unknown source (store) and requested permissions to access private resources

Recommendations
Consider uninstalling the app.

Additional Info


012 Mobile VPN 7:44 98%

Status OK — Network Threats
At Risk — Vulnerabilities
Status OK — Apps

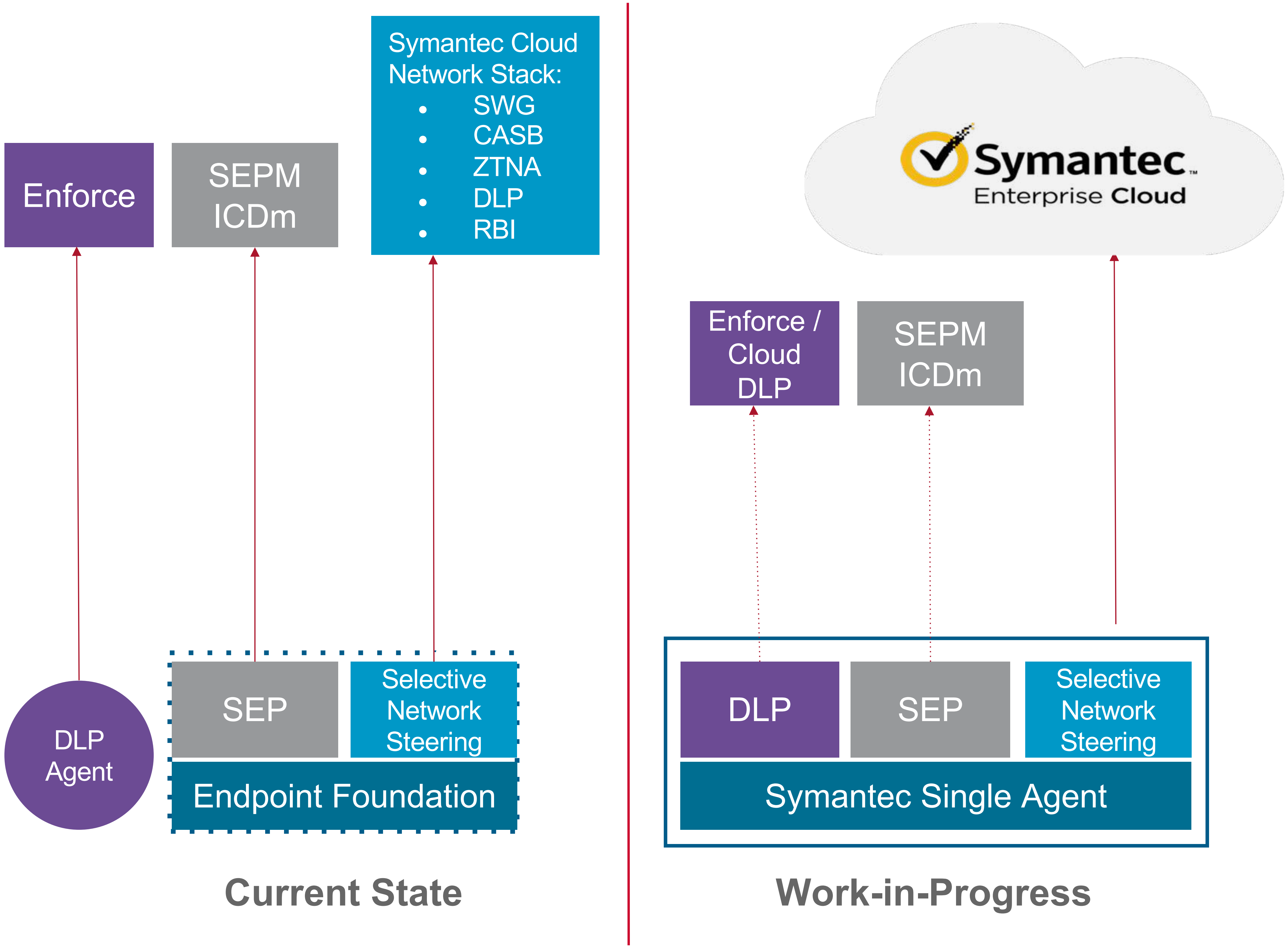
Operating system is up-to-date
1 Alert requires attention

Noncompliant with security policy
Access to corporate resources is blocked

3 Unread alerts
25 Network threats near you

Skycure Protected

Single Agent: Future Proof SASE, Reduced Operational Overhead



Benefits

- Futureproof
- Single management plan for all Symantec technologies
- Reduced endpoint resource consumption
- Rapid adoption both on & off network
- One platform for install, updates, & troubleshooting

Symantec’s Unique Endpoint Protection Capabilities

- Host-based IPS: Block attacks on the wire before they reach your endpoint
- Prevention of LotL -enabled threats
- Prevention of AD based lateral movement and credential misuse
- Enriched IOC’s and alerts powered by the Cloud Analytics
- Device Compliance & Location based protection policy targeting and enforcement
- Single Agent that protects mobile & older version of OS and also handles SASE use cases

Net++
TECHNOLOGY

HVALA NA PAŽNJI

011 36999 967
www.netpp.rs
office@netpp.rs