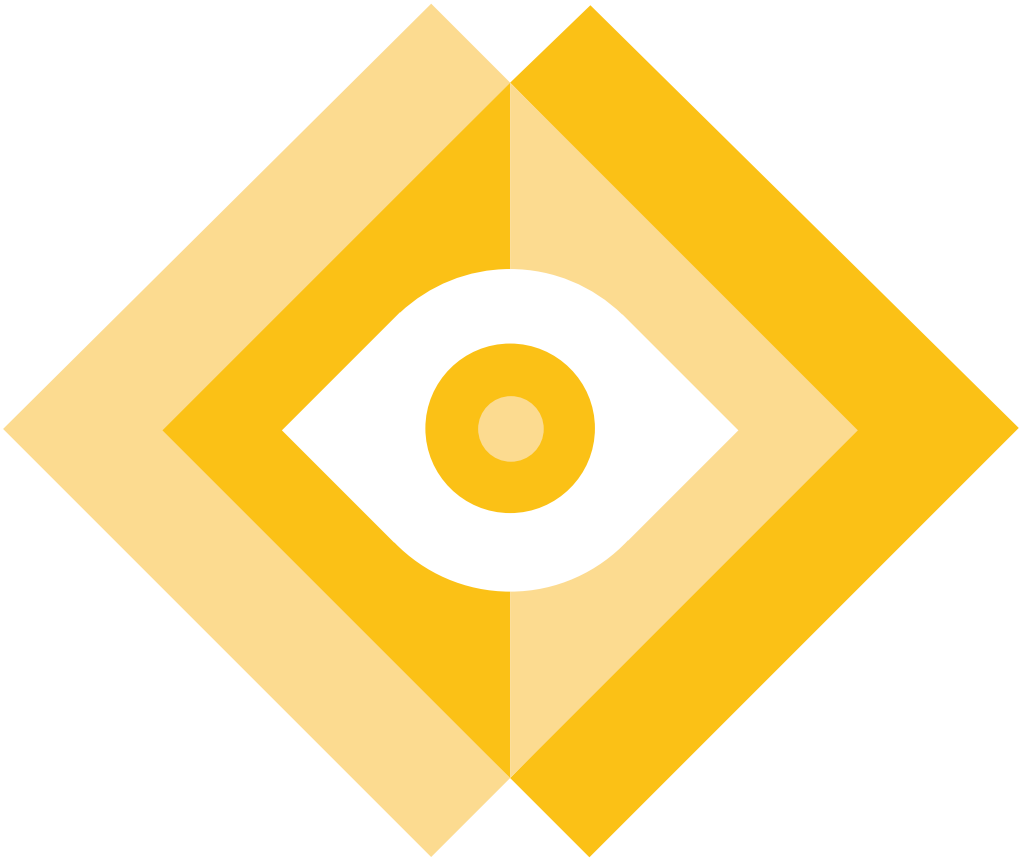


Targeted Attack Analytics

Using Cloud-based Artificial Intelligence for Enterprise-Focused Advanced Threat Protection

A Key Part of an Integrated Cyber Defense Platform

WHITE PAPER

Symantec™

Contents

Executive Summary

As enterprise security teams shore up defenses against malware, ransomware, and other external threats, and use existing tools to patch vulnerabilities, attackers are shifting their attack strategy from zero-day exploits (which have become too costly and complex) to 'living off the land' techniques. In fact, the Symantec 2018 Internet Security Threat Report, Volume 23 (ISTR 23) notes that only 27 percent of the 140 Symantec-tracked attack groups used zero-day vulnerabilities.

Existing security prevention tools cannot block sophisticated, previously unknown living off the land attacks that use tools already on the targeted system. By utilizing clean system tools and dropping in as few files as possible, attackers avoid being blocked or caught by traditional scanners and security measures. Also, memory-only attacks are even more difficult to detect as they leave very little evidence in their wake.

The only defense is a more holistic approach, one that uses both global and local context informed by attack analytics, continuously enhanced and bolstered with new analytics. The solution should address both inside and external actors.

Symantec big data analytics and targeted attack research, and Endpoint Detect and Response (EDR) supplement existing security tools, enabling enterprises to expose previously unknown attacks. Only Symantec brings together rich telemetry, artificial intelligence, advanced machine learning, and research expertise to identify hard-to-detect attacks with high confidence (both at the machine and enterprise levels).

Our massive, high-quality dataset, machine learning technologies, and collective research expertise gives Symantec customers unparalleled, tailored, and prioritized incident notification with clear recommendations for response and remediation. Delivered as a cloud service, TAA enables new and enhanced analytics to be continually delivered to our EDR customers (using Advanced Threat Protection: Endpoint) without the need for on-going updates.

Symantec Holistic Analytics Approach

Cloud architecture

Cloud-based artificial intelligence deliver evolving analytics without the need for intrusive product updates.

Endpoint telemetry across termination points

Global telemetry data enhances the local enterprise view with Symantec Endpoint Protection device visibility as well as all Symantec endpoint, mobile, email, network, and web intelligence.

Cloud 'data lake'

Symantec amasses a staggering amount of telemetry; our authoritative data lake comprises nine trillion rows, and logs 120,000 security events per second.

Analytic apps

Analytics apps sift through the cloud data lake to identify targeted attacks; these apps include Breach Analytics, PowerShell, Lateral Movement, and Command and Control Beaconing.

Incident store

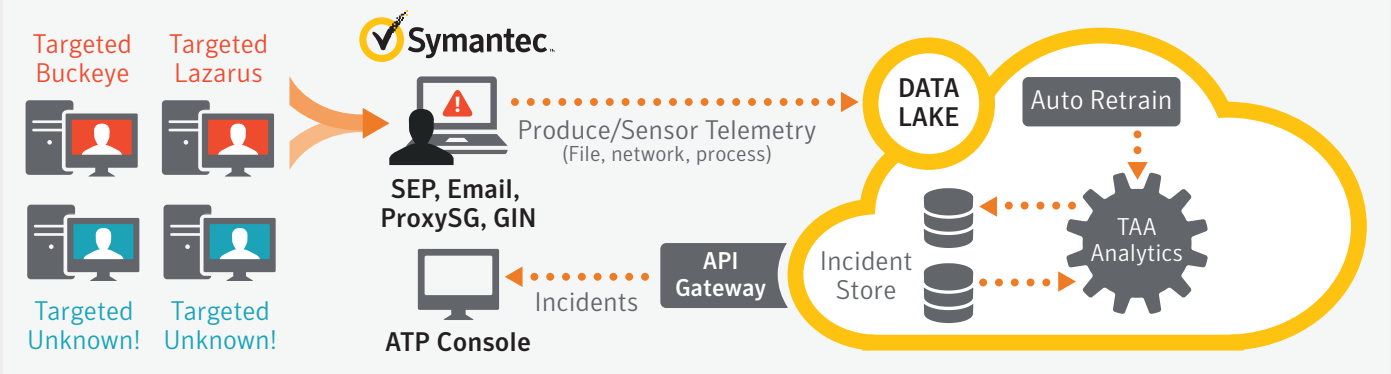
TAA provides descriptive, prioritized incidents including recommended actions to drive incident resolution. TAA provides the EDR console with more than an alert; the incident contains descriptive evidence along with recommended actions. Incidents are generated in the cloud enabling updates and refinement over time.

Continuous feed to EDR and feedback for retraining

The system includes a feedback loop.

- TAA identifies incidents with AI and advanced machine learning
- SOC analysts evaluate the insights
- Analysts feed back into the system, retraining to limit false positives and reinforcing correct alerts

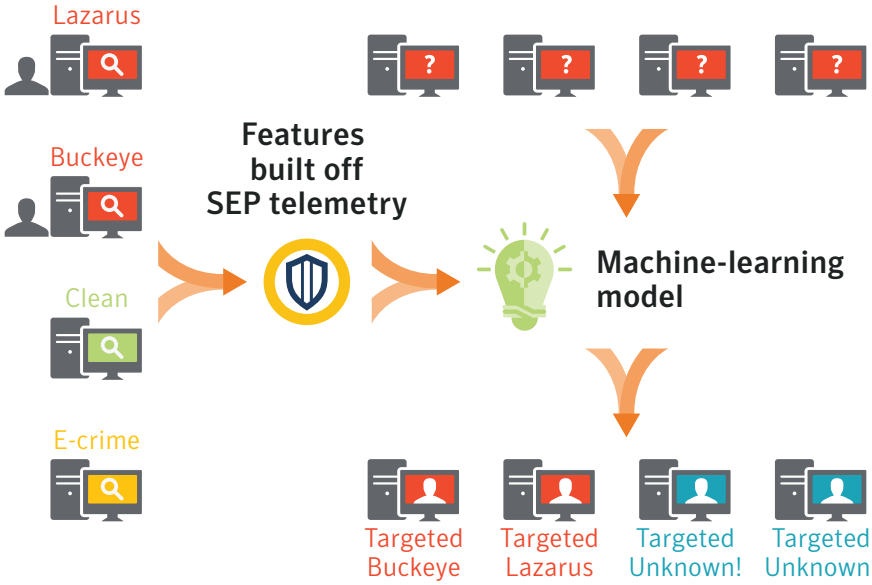
This human retraining of algorithms further refines the analytics engine.



Highlighted analytic: Breach detection

Symantec combines targeted attack analytics with research from our Attack Investigator Team (AIT) to find advanced attacks; our analytics evolve to match new attack patterns. Breach detection is one example of how our analytics help stop deliberate incursions.

We analyze data from known compromised machines at the process and file level, and assess the standard tools used at the time of compromise as well as network activity. We feed this telemetry to our learning model to train it on how a targeted incursion behaves. When we see similar suspicious behavior, we can send incidents in real time to our EDR customers (via ATP: Endpoint console).

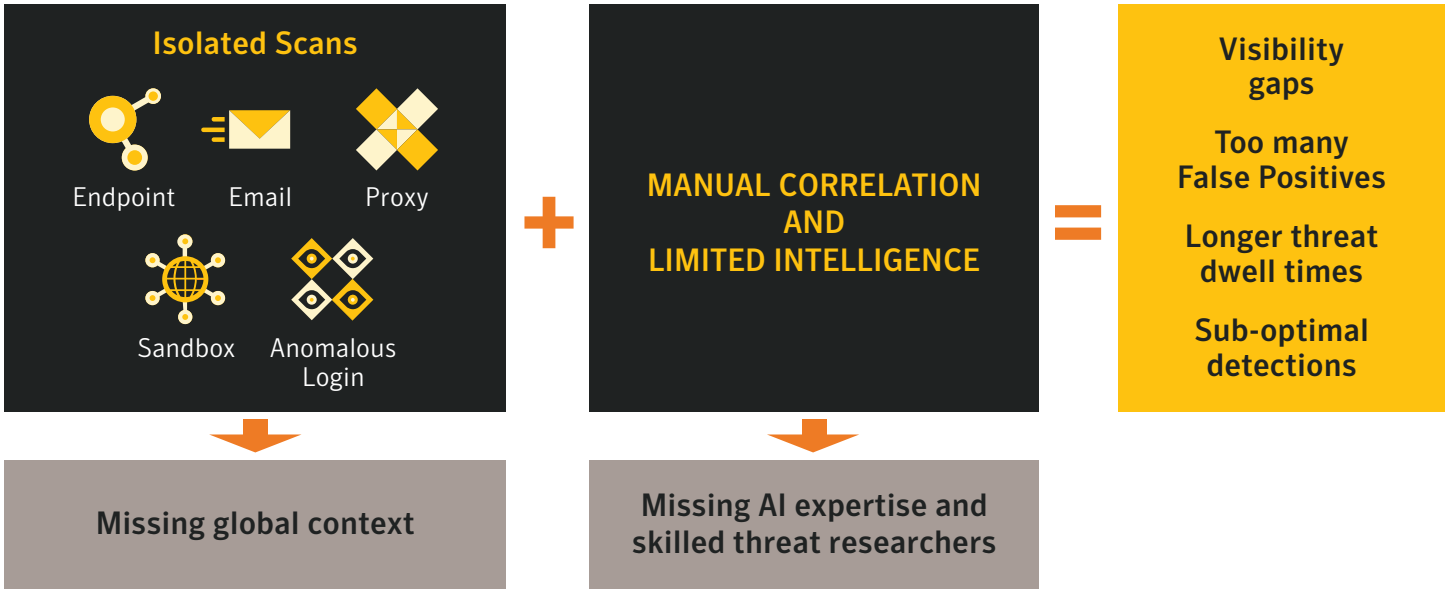


Our breach detection model is based on known application and network behaviors that compromise machines, enabling Symantec to alert customers on machines exhibiting similar behaviors.

Symantec EDR & TAA versus Traditional Breach Detection

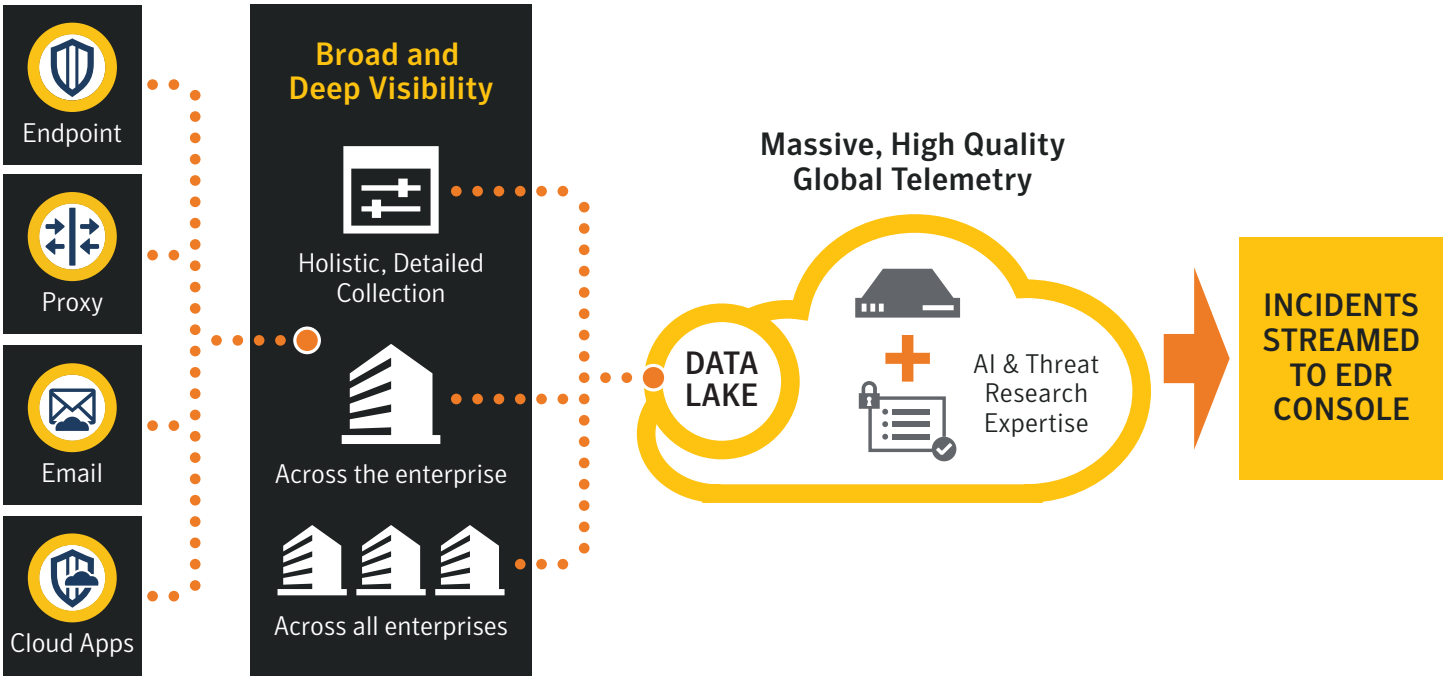
Traditional Breach Detection

Traditional breach detection captures isolated scans from organization-wide termination points. Because this approach doesn't provide global visibility into emerging threats, customers must manually correlate these scans and integrate them with limited threat intelligence sourced from external feeds. Also, because most organizations don't have the expertise to design artificial-intelligence algorithms, nor skilled threat researchers investigating attack groups, they incur threat visibility gaps, higher false positive rates, longer threat dwell times, and less precise detections. Traditional breach detection can easily miss the most dangerous threats to your organization.



Symantec EDR + TAA

By contrast, Symantec's authoritative data lake collects event data from all our customer termination points including Symantec Endpoint Protection, proxy, email, and cloud apps. Data scientists at our Center for Advanced Machine Learning continually develop new AI algorithms that run on this data lake. These algorithms detect suspicious activity, which Symantec researchers review for our affected customers. When Symantec finds a match, TAA creates a real-time incident—with a detailed analysis of the attacker, techniques, affected users, impacted machines, and remediation guidance—and streams it to the EDR (ATP: Endpoint) console. This approach streamlines the efforts of incident responders and enhances productivity for the entire SOC team.



Global Customer Base Telemetry

Symantec EDR with Targeted Attack Analytics parses global activity, the good and the bad, across all enterprises that comprise our telemetry set. Our modeling adapts to new attack techniques automatically. Since it uses both local data and our global intelligence network, it protects against more targeted attacks.

Symantec Uncovers Return of Dragonfly

- Original Dragonfly campaigns started in 2011, targeting energy companies
- TAA spotted a significant increase in new Dragonfly activity in 2017
- Attacks targeted dozens of energy companies
- Dragonfly gained access to operational networks, infiltrating power distribution on American soil

We believe this was the first time attackers could control U.S. power systems operationally.

TAA Success

TREEHOPPER	DRAGONFLY 2.0	THRIP	SEEDWORM
Exposed by TAA: 3/2017	**EXPOSED BY TAA: 5/2017**	**EXPOSED BY TAA: 1/2018**	**EXPOSED BY TAA: 2/2018**
TARGET & MOTIVATION Government, Financial Industrial espionage, extortion	**TARGET & MOTIVATION** Energy Disruptive reconnaissance	**TARGET & MOTIVATION** Activist, Government Espionage	**TARGET & MOTIVATION** Government, Telecom, Energy Espionage
Have a thorough understanding of corporate networks, targeting IP and other commercially sensitive information.	The group uses several techniques to compromise victims including watering holes, update hijacks, and emails in conjunction with exploits against six known vulnerabilities.	The attackers have unique exploitation and compromise techniques, using an offensive Windows Management Instrumentation (WMI) technique known as 'WMIGhost' or 'Shadow.'	Seedworm (AKA MuddyWater) is an espionage group that uses a custom backdoor called W97M.Powermud (AKA POWERSTATS) that provides remote access.
TAA FINDINGS Network reconnaissance. Network domain resources dumped to a file. Local reconnaissance to check running processes.	**TAA FINDINGS** Covert communications channel. Download of implant. Enumeration of assets on local system.	**TAA FINDINGS** Lateral movement. Download and installation of malware implant. Network reconnaissance.	**TAA FINDINGS** Initial compromise via download and installation of malware implant.

Symantec Expertise

Symantec's analyst investigate and expose the most sophisticated and dangerous cyber attacks. The Attack Investigation Team tracks over one hundred advanced attack groups; AIT has uncovered major targeted attacks including Regin, Stuxnet, and Dragonfly, and used its expertise to automate discovery of new attacks.

The Symantec Center for Advanced Machine Learning makes use of the big data capability of our cloud data lake and over 70 years of machine learning experience, creating and training new security AI algorithms and machine learning models.

This unique combination—massive, high-quality telemetry from across termination points (endpoints, web, emails, and cloud apps) and hundreds of peerless researchers—gives us unmatched attack identification capabilities that are entirely analytics-based and attack- rather than machine-centric.

TAA Benefits

TAA delivers unique benefits to Advanced Threat Protection customers including:

- Multiple incidence of attack detections combined with AI-driven and human analysis customized to each customer's environment
- Cloud-based analytics that automatically adapt to new attack techniques
- Continuously delivered attack detections plus the ongoing addition of new attack analytics
- Holistic view of activity across the customer's enterprise as well as across hundreds of millions of Symantec global customer control points

Conclusion

The integration of Targeted Attack Analytics with EDR will solve your critical security challenges. EDR (ATP: Endpoint) customers combine local and global telemetry, intelligence, and attack research to expose attacks that would otherwise evade detection.

ATP customers benefit from Symantec's global visibility, world-class threat researchers, and data scientists to identify attacks in early stages. As targeted attacks increase in sophistication and volume, enterprises need to reduce the overall number of incidents analysts have to investigate and ensure responders are focused on the highest priority incidents.

Using TAA, EDR customers benefit from ongoing delivery of new attack analytics and generation of custom incidents, covering detailed analysis of attacker methods, impacted machines, and remediation guidance—all at no additional cost.

Contact your Symantec Product Specialist or partner representative for more information or to request a demo or trial.

Learn more about Symantec Endpoint Detection and Response:

https://www.symantec.com/products/endpoint-detection-and-response

Learn more about Symantec Integrated Cyber Defense:

https://www.symantec.com/theme/integrated-cyber-defense

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19A166470_SYMC_WP_ATP_TAA_EN_v1