

Symantec Endpoint Detection and Response

On-premises and Cloud-based EDR Solution

At a glance

Detect and Expose – Reduce time to breach discovery and quickly expose scope

- Apply Machine Learning and Behavioral Analytics to expose suspicious activity, detect and prioritize incidents
- Automatically identify and create incidents for suspicious scripts and memory exploits
- Expose memory-based attacks with analysis of process memory

Investigate and Contain – Increase incident responder productivity and ensure threat containment

- Ensure complete incident playback with continuous recording of endpoint activity, view specific endpoint processes
- Hunt for threats by searching for indicators of compromise across all endpoints in real-time
- Contain potentially compromised endpoints during investigation with endpoint quarantine

Resolve – Rapidly fix endpoints and ensure the threat does not return

- Delete malicious files and associated artifacts on all impacted endpoints
- Blacklist and whitelist files at the endpoint
- Enhanced reporting allows any table to be exported for incident resolution reports

Integrate and Automate – Unify investigator views, orchestrate data and work flows

- Easily integrate incident data and actions into existing SOC infrastructure including Splunk and ServiceNow
- Replicate the best practices and analysis of skilled investigators with automated incident playbook rules
- Gain in-depth visibility into endpoint activity with automated artifact collection

Enterprises are increasingly under threat from sophisticated attacks. In fact, research has found that threats dwell in a customer's environment an average of 190 days¹. These Advanced Persistent Threats use stealthy techniques to evade detection and bypass traditional security defenses. Once an advanced attack gains access to a customer environment the attacker has many tools to evade detection and begin to exploit valuable resources and data. Security teams face multiple challenges when attempting to detect and fully expose the extent of an advanced attack including manual searches through large and disparate data sources, lack of visibility into critical control points, alert fatigue from false positives, and difficulty identifying and fixing impacted endpoints.

Symantec EDR Solution

Symantec EDR exposes advanced attacks with precision machine learning and global threat intelligence minimizing false positives and helps ensure high levels of productivity for security teams. Symantec EDR capabilities allow incident responders to quickly search, identify and contain all impacted endpoints while investigating threats using a choice of on- premises and cloud-based sandboxing. Also, Symantec EDR enhances investigator productivity with automated incident playbook rules and user behavior analytics that brings the skills and best practices of the most experienced security analysts to any organization, resulting in significantly lower costs.

In addition, continuous and on-demand recording of system activity supports full endpoint visibility. Symantec EDR utilizes behavioral analytics at the endpoint and in the cloud to detect stealthy attacks such as breach detection, command and control beaoning, lateral movement and suspicious power shell executions.

Increase Investigator Productivity

Symantec EDR increases investigator productivity by prioritizing incidents by risk. And Symantec EDR automatically generates incidents for targeted attacks identified through Symantec's Target Attack Analytics and Dynamic Adversary Intelligence.

In addition, investigators can take advantage of Endpoint Activity Recording to hunt for Indicators of Attack and perform endpoint analysis. Symantec EDR supports continuous and on-demand retrieval for a wide range of events including session, process, module load point modifications, file and folder operations, registry changes and network connection activity.

According to Symantec Internet Safety and Threat Report (ISTR), more than 20% of the malware is VM-aware which means they evade detection in a traditional sandbox. Symantec EDR can detect such VM-aware threats by employing advanced techniques that include mimicking human behavior and if necessary using physical servers for detonation.



Symantec EDR provides smart incidents to enhance investigator productivity

Enterprise-focused Attack Analytics

Symantec EDR includes Targeted Attack Analytics (TAA). TAA parses global activity, the good and the bad, across all enterprises that comprise our telemetry set. Our cloud-based artificial intelligence algorithms and advanced machine learning adapts to new attack techniques automatically. 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 console. This approach streamlines the efforts of incident responders and enhances productivity for the entire security team (TAA is provided at no additional cost to Symantec customers using Advanced Threat Protection 3.1 or higher).

Hunt for Anomalies Across Endpoints

Symantec EDR simplifies the hunt for attackers within the environment by providing an across the board view of software, memory, user, and network baseline activity. When attackers operate in the environment, their malware and user activity stand out as anomalies or outliers.

Symantec EDR exposes outliers across the environment including:

- **Software outliers** – Expose endpoints that have uncommon software, build discrepancies, unpatched or old operating system (OS) releases
- **Memory outliers** – Detect memory-resident outliers using forensic examination of process memory, file and OS object, and system settings
- **User outliers** – User behavior analytics detect attackers acting as legitimate users performing unusual activity
- **Network outliers** – Leverage statistical analysis to identify anomalous IP addresses, reputation lookups identify IP addresses and domains associated with data exfiltration

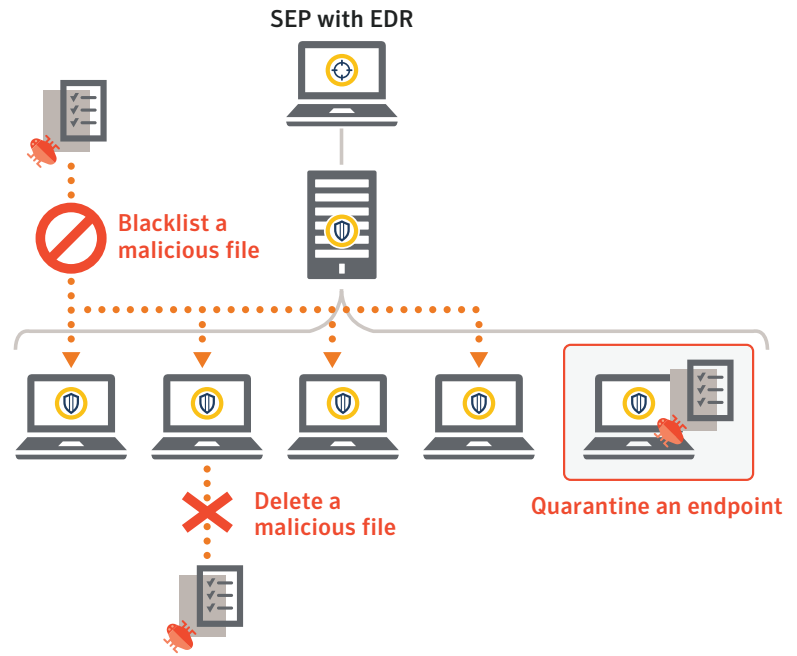
These outlier detections are provided via cloud-based service and are available using built-in playbooks that produce specific reports on wide variety of anomalous activity.

Rapidly Fix Endpoints

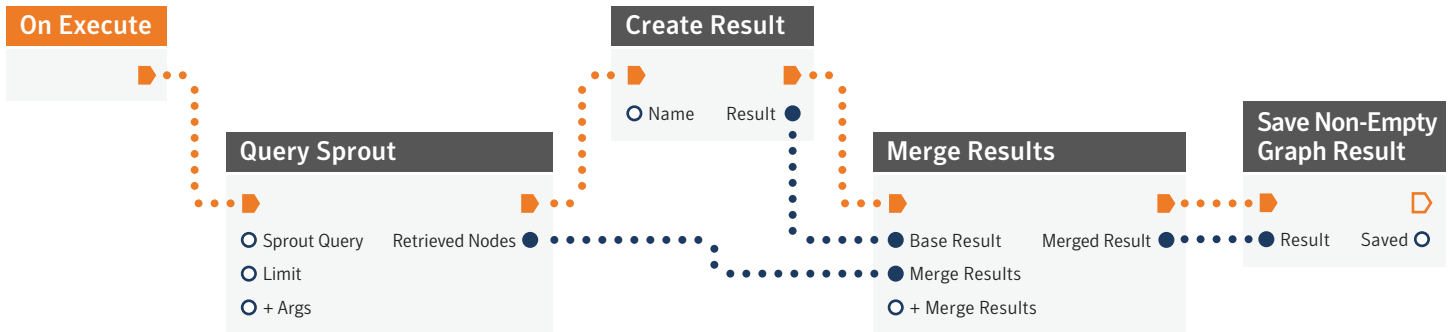
Symantec EDR supports rapid remediation of impacted endpoints including file deletion, blacklisting and endpoint quarantine. Using powerful eraser capabilities built into Symantec Endpoint Protection (SEP), responders can take action from a single console and with one click apply a fix across multiple endpoints.

Automate Skilled Investigator Practices

Symantec EDR supports playbooks that automate the complex, multi-step investigation workflows of security analysts. Built-in playbooks quickly expose suspicious behaviors, unknown threats, lateral movement and policy violations. The security team can view the playbooks to learn expert hunting and investigation techniques. In addition, Investigators can create their playbooks to automate best practices and document specific threat hunting scenarios.



Symantec EDR allows security teams to respond to advanced attacks in minutes



Symantec EDR has powerful cloud-based tools to automate artifact collection and investigator playbooks

Flexible Deployment Options

The Symantec EDR is a flexible solution that can be deployed on-premises or in the cloud. Symantec Endpoint Protection (SEP) customers can leverage integrated EDR capabilities in the SEP single agent architecture. Using the on-premises Advanced Threat Protection: Endpoint (ATP: Endpoint) appliance, organizations can quickly deploy EDR into existing SEP environments. In addition, customers can add modules that provide visibility and correlation of network and email events (Email module requires Symantec Email Security.cloud).

Endpoints with or without SEP installed can leverage the cloud-based portal for cyber data analytics, forensic analysis and incident playbook automation using a dissolvable client and on-premises collection server (or optional collection services agent). Symantec's cloud-based EDR capabilities deploys in minutes and quickly collects data from endpoints with no impact on end-user experience.

Enhance Security Investments

Symantec's Integrated Cyber Defense approach enhances your organizations existing investment in security infrastructure. Symantec EDR solutions integrate with security operations tools for event and incident management, ticketing, automation and orchestration including:

- Pre-built apps for Splunk, IBM QRadar and ServiceNow
- Integrated automation and orchestration using Phantom and Demisto
- Open APIs covering detection, investigation and response capabilities

Requirements

For complete requirements of Symantec EDR visit our system requirements page:

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

¹ 2017 Ponemon Cost of Data Breach Study

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](#).



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