Symantec Endpoint Detection and Response

Rapid Threat Discovery and Remediation

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 days[1]. 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 investigation playbooks 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.

[1] "Cost of a Data Breach Report, Ponemon 2018" https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&

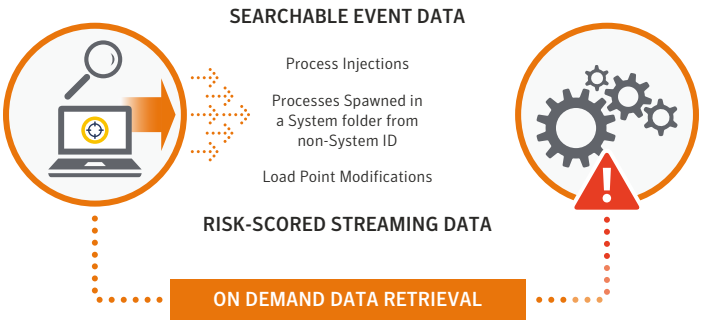
In addition, continuous and on-demand recording of system activity supports full endpoint visibility. Symantec EDR utilizes advanced attack detections at the endpoint and cloud-based analytics to detect targeted attacks such as breach detection, command and control beaconing, lateral movement and suspicious 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 alerts to enhance investigator productivity

Cloud-based Attack Analytics and Endpoint Advanced Attack Detections

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, 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).

Symantec EDR also leverages endpoint behavioral polices, continually updated by Symantec researchers, to detect advanced attack methods instantly at the endpoint (over 330 currently available). These detections detail activity that may indicate attacks in progress including file and registry changes, suspicious network and processes activity and use of specific Windows API's that can be used to start a malicious thread within an existing process.

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.

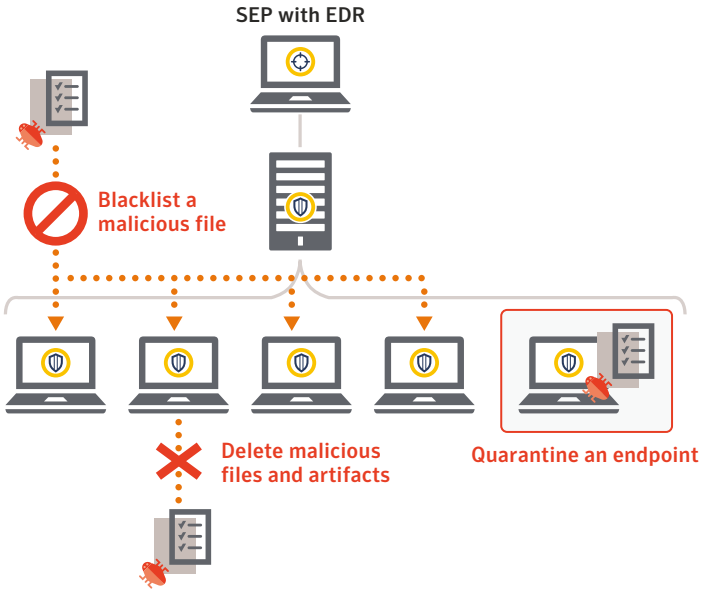
MITRE ATT&CK Event Enrichment and Cyber Analytics

Symantec EDR provides tools to detect and visualize the attack lifecycle based on the MITRE ATT&CK framework. The EDR tool describes attack methods based on the standard tactics and techniques in the ATT&CK matrix. In addition, quick filters make it easy for investigators to narrow results to one or more phases of the MITRE ATT&CK lifecycle including initial access, persistence, lateral movement and command and control.

Critically, Symantec EDR supports MITRE Cyber Analytics through automated investigation playbooks. MITRE recommends organizations implement a zero-trust approach to forensic collection and investigation by interrogating autorun differences, suspicious run locations, potential DDL injections and SMB event monitoring. Symantec EDR makes it easy to run scheduled sweeps across endpoints to determine if any attacks can be detected using common knowledge of the MITRE community of adversary models.

Complete and Rapid Endpoint Repair

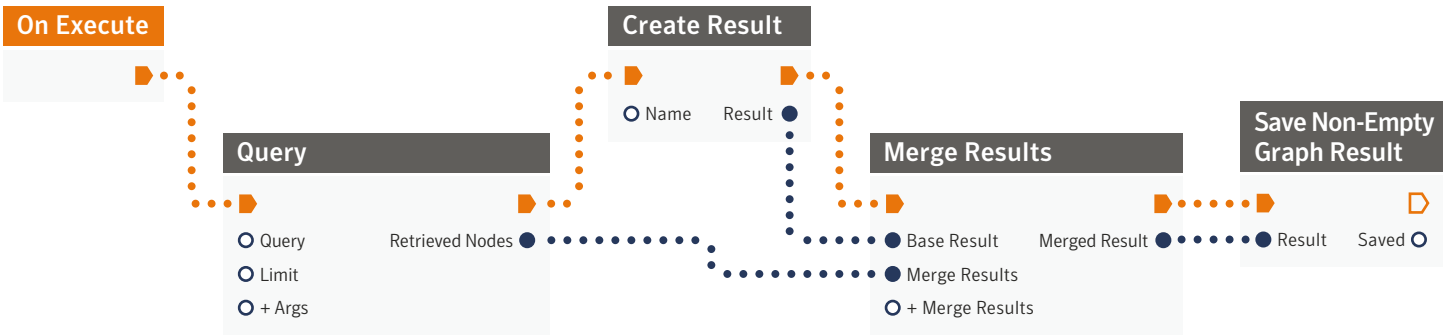
Symantec EDR supports rapid remediation of impacted endpoints including file deletion, blacklisting and endpoint quarantine. Using powerful eraser capabilities built into Symantec Endpoint Protection (SEP), responders can take action from a single console and with one click apply a fix across multiple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



Symantec EDR ensures endpoints are returned to a pre-infection state

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 own playbooks to automate best practices and document specific threat hunting scenarios.



Symantec EDR has powerful, automated playbooks for artifact collection, investigation and response

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 EDR 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 investigation 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.

Extend Your SOC Team

Symantec Managed Endpoint Detection and Response is a 24x7 forensics investigation and threat hunting service that employs Symantec SOC analysts to actively detect stealthy attacks and expertly examine suspicious activity. These analysts use Symantec Endpoint Detection and Response (EDR) coupled with machine learning analytics and Symantec Global Intelligence Network correlation.

In addition, Symantec EDR customers can receive incident triage and guidance from Symantec GIAC-certified SOC Analysts at no additional cost (Available as "Engage an Incident Responder" from the EDR console).

Symantec's Managed EDR delivers unmatched expertise and global scale that fortifies security teams with:

- GIAC-certified Symantec SOC analysts assigned to every customer
- Powered by Symantec Endpoint Detection and Response
- Forensics investigations on-premises and in the cloud
- Proactive, managed threat hunting of emerging IoCs, TTPs, and MITRE ATT&CK tactics
- Pre-authorized containment of compromised endpoints
- Big data analytics and Symantec Global Intelligence Network correlation
- Rapid, no-cost onboarding and continuous customer engagement

In combination with Symantec EDR tools, Managed EDR adds additional expertise and global coverage many SOC teams require.

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, Demisto and CyberSponse
- Open APIs covering detection, investigation and response capabilities

About Threatscape

Threatscape is the trusted security partner of enterprise clients who rely on us to secure critical IT assets in over 100 countries around the world. Our mission is to create a secure and certain future for our clients. Keeping them protected so that they can go about their business is how we know we're delivering on our promise. To do this, our expert team of engineers and consultants use their skills alongside best-in-class solutions to protect, detect and respond to the growing threat of cyberattacks.

Threatscape

To learn more, contact us via info@threatscape.com or on 0203 653 0000 (UK) or 01 901 7000 (Ireland) | www.threatscape.com

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

Copyright ©2018 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

19C199684_ds_EDR_EN