Symantec

DATA SHEET

Endpoint Detection and Response Cloud

Full Endpoint Visibility and Automated Threat Hunting

At a glance

Detection – Discover outliers that don't belong in the environment

- Detect software, memory, user and network outliers that stand out from baseline activity
- Use timeline and path analysis to detect multi-phased attacks
- Expose memory-based attacks with analysis of process memory

Automation – Leverage the best practices of skilled investigators

- 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
- Initiate cyber security functions and learn expert investigation methods with built-in playbooks

Visualization – Transform large amounts of cyber data into actionable results

- Understand the contextual relationship between unrelated data types with visual link analysis
- Use graphical alerts to quickly learn the source, timing, and impact of an incident
- Transform voluminous endpoint telemetry into interactive graphics to focus on relevant activity

Introduction

Security teams face sophisticated attacks that 'hide in plain sight' and often dwell in customer environments as long as 190 days[1]. And attackers increasingly employ stealthy techniques to move freely within a customer environment like using stolen credentials to masquerade as legitimate users. There has been a marginal decline in zero-day discoveries and an increase in 'living off the land' tactics that don't rely on the traditional combination of vulnerabilities followed by malware. These tactics are more difficult to detect since they make use of legitimate tools[1].

Organizations need new approaches to detect threats that would otherwise go unnoticed. Also, finding the skilled staff to conduct deep-dive investigations can be difficult and costly. And even if your organization has these skills in-house they can be hard to retain.

EDR Cloud Overview

Symantec Endpoint Detection and Response (EDR) Cloud delivers in-depth endpoint visibility, automated threat hunting and breach response across the entire enterprise. Symantec EDR Cloud is a cloud-based service that can be deployed in minutes and helps to strengthen a firm's security posture against cyber attacks. Symantec EDR Cloud enhances investigator productivity with extensive 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.

Using forensic analysis and built-in playbooks that support the detection of stealthy threats security teams can initiate investigations quickly with fully configurable point-in-time scans that don't require the deployment of an additional agent.

Discover outliers that don't belong in the environment

Symantec EDR Cloud 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 stands out as anomalies. Symantec EDR Cloud detects these 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 address and domains associated with data exfiltration

In addition, Symantec EDR Cloud includes multiple threat engines which risk score files, users accounts, network connections. Detection capabilities also include:

- Neural network based machine learning using millions of good and bad files
- Customer supplied and third-party threat intelligence sources
- Examination of registry changes and scheduled tasks help expose persistent threats
- Multiple anti-malware engines

Leverage the best practices of skilled investigators

Symantec EDR Cloud 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.

Transform large amounts of cyber data into actionable results

Symantec EDR Cloud is visually powerful. The system provides visual link analysis with interactive graphics to transform how security professionals use and relate to computer and network data.

Machine-assisted analysis allows interaction with all the relevant data at scale. Link analysis provides a fast conceptual association of complex relationships between disparate data types.

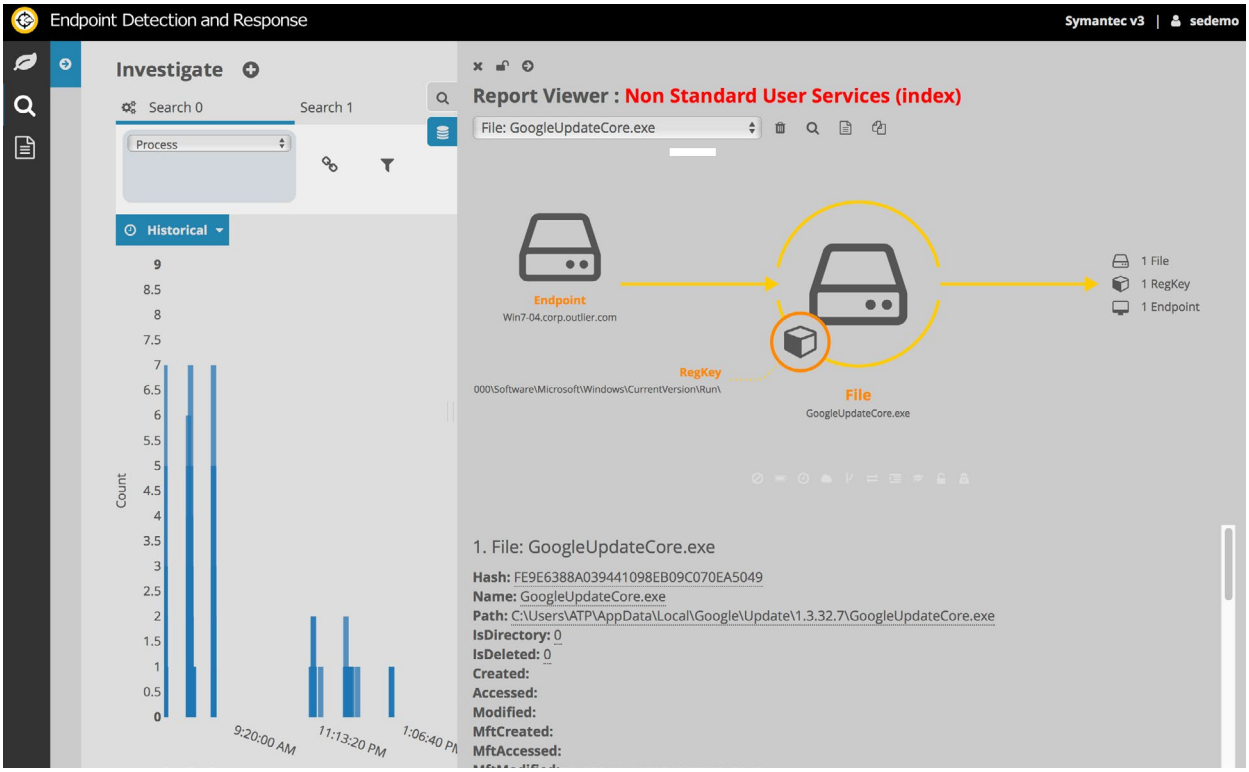
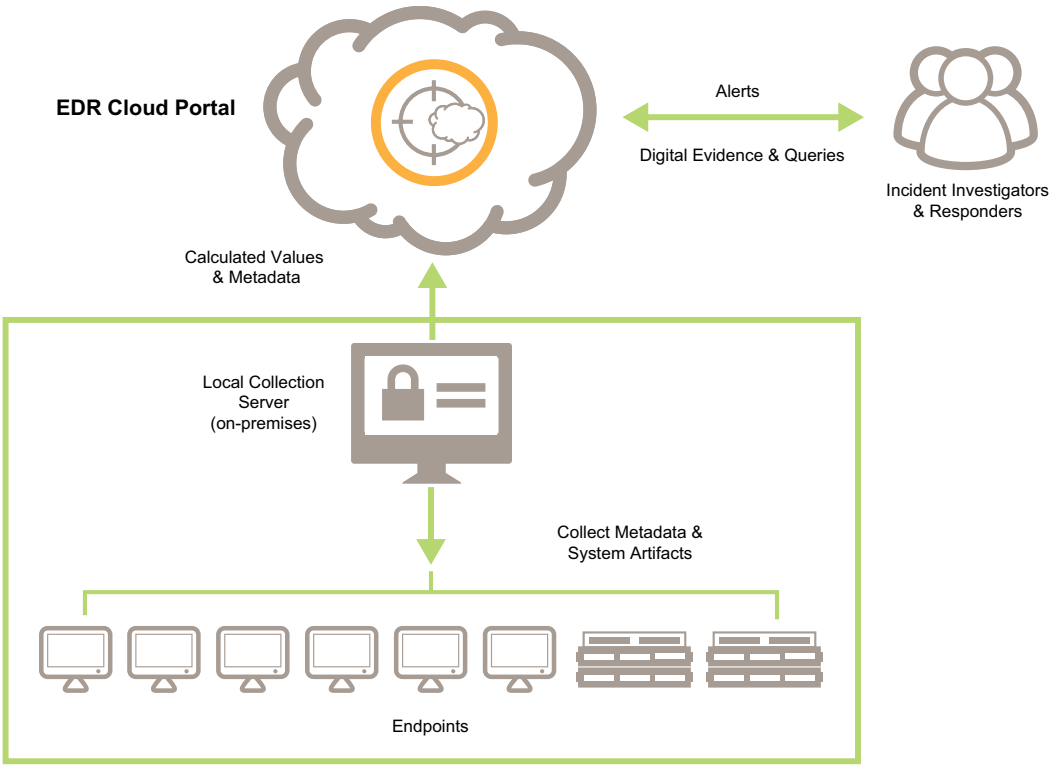


Figure 1. Symantec EDR Cloud has powerful tools to visualize complex cyber data

How it works

As shown in the diagram below, Symantec EDR Cloud consists of an investigator portal and one or more collection servers. The portal provides the investigator interface and performs security analytics. The solution collects data from endpoints, analyzes the data for detection, and provides tools to query the enterprise and remediate compromised systems.

Endpoint Detection and Response Cloud



The on-premises server continually collects vital forensic data from computers. Collected data includes unknown files, process metadata, programs, services, modules, files, autoruns, user behaviors, network connections, and timelines. Data collection is passive, occurs within 60 seconds and has no impact on the end-user experience.

Requirements

Browser UI Requirements

Version 2.9 depends on Silverlight and requires Microsoft Internet Explorer 11 or later

Version 3.0 also supports Mozilla Firefox 26 or later and Google Chrome 32 or later

Collection Server Requirements (Data Vault)

Windows 7 through Windows server 2016

Virtual support for VMware, HyperV

Endpoint Requirements

Windows XP and higher

macOS Sierra, El Capitan, Yosemite

Redhat Linux 7.0 and higher, 32 and 64-bit versions

CentOS, Mint, Cinnamon, 32 and 64-bit versions

References:

1. Symantec Internet Security Threat Report Vol. 22

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**

SYMC-DS-EDR_Cloud-EN-v1