CISCO
SECURE

Data sheet
Cisco public

Cisco Secure Endpoint

October 2020

The bridge to possible

Contents

Product overview

Cisco® Secure Endpoint (formerly AMP for Endpoints) integrates prevention, detection, threat hunting and response capabilities in a single solution, leveraging the power of cloud-based analytics. Secure Endpoint will protect your Windows, Mac, Linux, Android, and iOS devices through a public or private cloud deployment.

Benefits

In the rapidly evolving world of malware, threats are becoming harder and harder to detect. The most advanced 1% of these threats, those that will eventually enter and wreak havoc in your network, could potentially go undetected. However, Secure Endpoint provides comprehensive protection against that 1%. This security software prevents breaches, blocks malware at the point of entry, and continuously monitors and analyzes file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defenses.

Prevention

Stopping threats at the earliest point in time ensures minimal damage to endpoints and less downtime after a breach. Secure Endpoint employs a robust set of preventative technologies to stop malware, in real-time, protecting endpoints against today's most common attacks.

File reputation: Secure Endpoint contains a comprehensive database of every file that has ever been seen and a corresponding good or bad disposition. As a result, known malware is quickly and easily quarantined at the point of entry without any processor-intensive scanning.

Antivirus: Secure Endpoint includes constantly updated, definition-based antivirus engines for both Windows and Mac or Linux endpoints. All endpoints benefit from custom signature-based detection, allowing administrators to deliver robust control capabilities and enforce blacklists. The antivirus signature database resides locally on each endpoint, meaning it does not rely on cloud connectivity to operate. This ensures that your endpoints are protected both on- and offline.

Polymorphic malware detection: Malware actors will often write different variations of the same malware to avoid common detection techniques. Secure Endpoint can detect these variants, or polymorphic malware through loose fingerprinting. Loose fingerprinting will look for similarities between the suspicious file's content and the content of known malware families, and convict if there is a substantial match.

Machine learning analysis: Secure Endpoint is trained by algorithms to "learn" to identify malicious files and activity based on the attributes of known malware. Machine learning capabilities in Secure Endpoint are fed by the comprehensive data set of Cisco Talos™ to ensure a better, more accurate model. Together, the machine learning in Secure Endpoint can help detect never-before-seen malware at the point of entry.

Exploit prevention: Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes. The exploit prevention feature will defend endpoints from exploit-based, memory injection attacks.

Script Protection: Secure Endpoint provides enhanced visibility in Device Trajectory into scripts executing on your endpoints and helps protect against script-based attacks commonly used by malware. Script control provides additional protection by allowing the Exploit Prevention engine to prevent certain DLLs from being loaded by some commonly exploited desktop applications and their child processes.

Behavioral Protection: Secure Endpoint's enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by matching a stream of activity records against a set of attack activity patterns which are dynamically updated as threats evolve. For example, this enables granular control and protection from the malicious use of living-off-the-land tools.

Detection

Though malware prevention techniques are necessary for a complete next-generation endpoint security solution, combatting advanced threats requires additional measures. Secure Endpoint continuously monitors endpoints to help detect new and unknown threats.

Malicious activity protection: Secure Endpoint continually monitors all endpoint activity and provides run-time detection and blocking of abnormal behavior of a running program on the endpoint. For example, when endpoint behavior indicates ransomware, the offending processes are terminated, preventing endpoint encryption and stopping the attack.

Cloud-based indicators of compromise: Cisco's industry-leading threat intelligence organization, Talos, constantly analyzes malware to discover new threat types and build behavioral and forensic profiles for emerging threats, otherwise known as Indicators of Compromise (IoCs). The forensic data, such as file locations or modifications to registry key values, are all data that Secure Endpoint can use to help administrators identify systems that have been breached.

Host-based IoCs: Administrators can write their own custom IoCs for use in incident response to scan for post-compromise indicators across the entire endpoint deployment. Custom IoCs are written in an open standard format (OpenIOC) making it easy to leverage data from any existing intelligence feeds.

Vulnerabilities: Secure Endpoint identifies vulnerable software across your environment to help reduce the attack surface. Endpoints running vulnerable software are listed out and are given priority based on industry CVE (Common Vulnerabilities and Exposures) scoring: the more severe a vulnerability, the more prominent it will be on the list. This provides administrators with a list of all hosts that need to be patched to prevent future exploits.

Low prevalence: Secure Endpoint will automatically identify executables that exist in low numbers across your endpoints and analyze those samples in our cloud-based sandbox to uncover new threats. Targeted malware or advanced persistent threats will often fly under the radar and start on only a few endpoints, but with low prevalence, Secure Endpoint will automatically threat hunt to help easily uncover the 1% of threats that would have otherwise gone unnoticed.

Threat Hunting

SecureX Threat Hunting is a proactive analyst-centric approach to detecting hidden advanced threats. This capability is offered exclusively as part of the new Premier license tier within Secure Endpoint. It tells the incident responders a narrative of how an attack was spotted or how it evolved and what to do next in terms of response. The purpose is to discover and thwart attacks before they cause any damage. As a side-effect of leveraging a regular and continuous threat hunting, an organization increases their knowledge of vulnerabilities and risks which further allows the hardening of their security environment.

SecureX Threat Hunting leverages the expertise of both Talos and the Cisco Research and Efficacy Team to help identify threats found within the customer environment. Cisco delivers highly automated human-driven hunts based on playbooks producing high-fidelity alerts. The process uniquely combines the Orbital Advanced Search technology with expertise from elite threat hunters, with 20 years of industry experience, to proactively find more sophisticated threats.

The Secure Endpoint Premier license is available to order globally in all regions. However, the SecureX Threat Hunting infrastructure that processes the customer telemetry and executes hunts is currently available only in North America.

Response

As the number and variety of advanced threats designed to slip past preventative measures increase, the possibility of a breach should be treated as an eventuality. With that mindset, a powerful toolset should be deployed to help easily identify infected endpoints and understand the scope of an attack. In addition to multiple prevention and detection capabilities, Secure Endpoint offers granular endpoint visibility and response tools to handle security breaches quickly and efficiently.

Dashboards and inbox: Reports are not limited to event enumeration and aggregation. The actionable dashboards built into Secure Endpoint enable streamlined management and faster response. Events and endpoints are categorized by priority and tied into workflows to track progress during investigation.

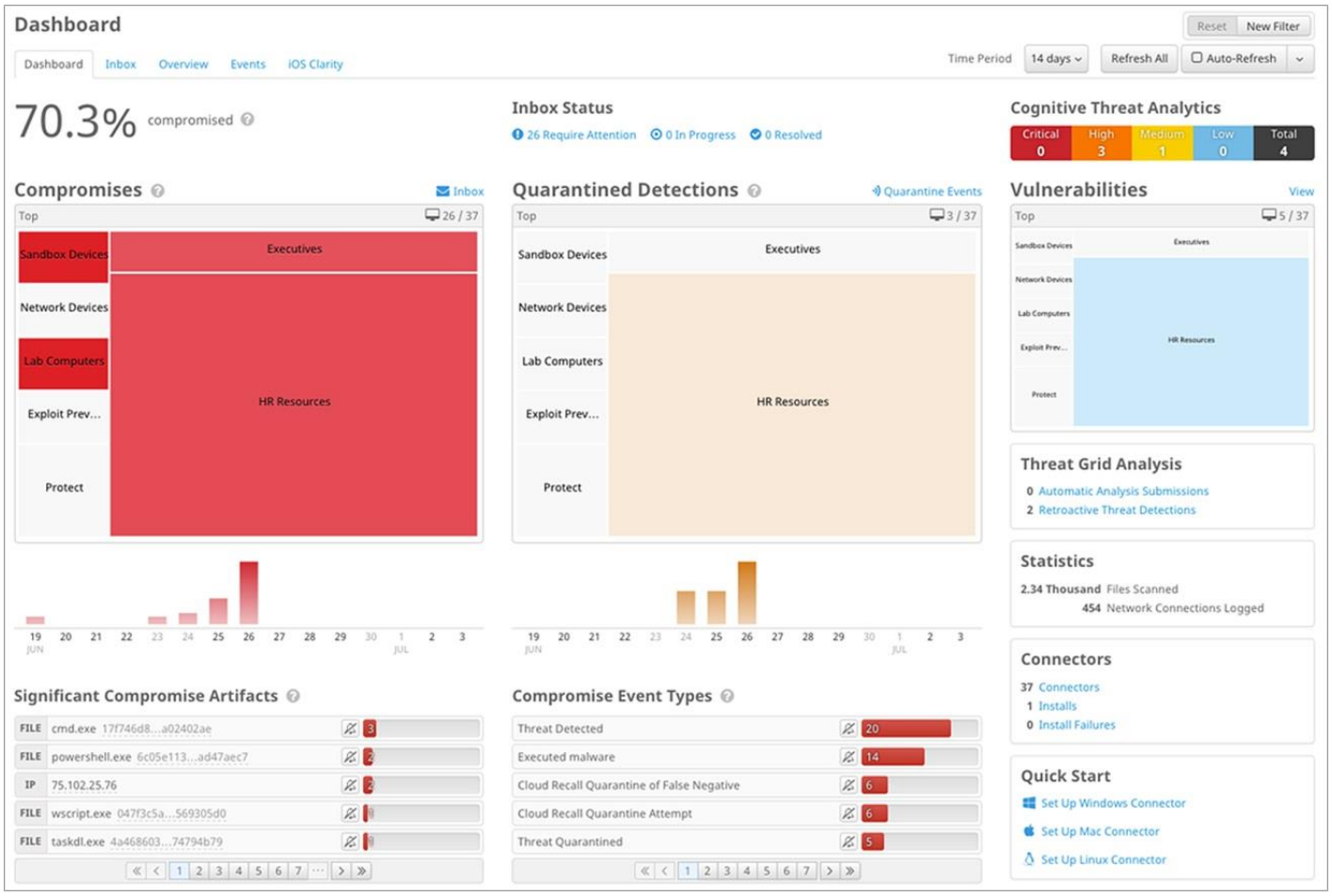

Figure 1.
Secure Endpoint dashboard

Endpoint forensics: Powerful tools like file trajectory and device trajectory use Secure Endpoint's continuous analysis capabilities to show you the full scope of a threat. Secure Endpoint identifies all affected applications, processes, and systems to pinpoint patient zero, as well as the method and point of entry. These capabilities help you quickly understand the scope of the problem by identifying malware gateways and the path that attackers are using to gain a foothold into other systems.

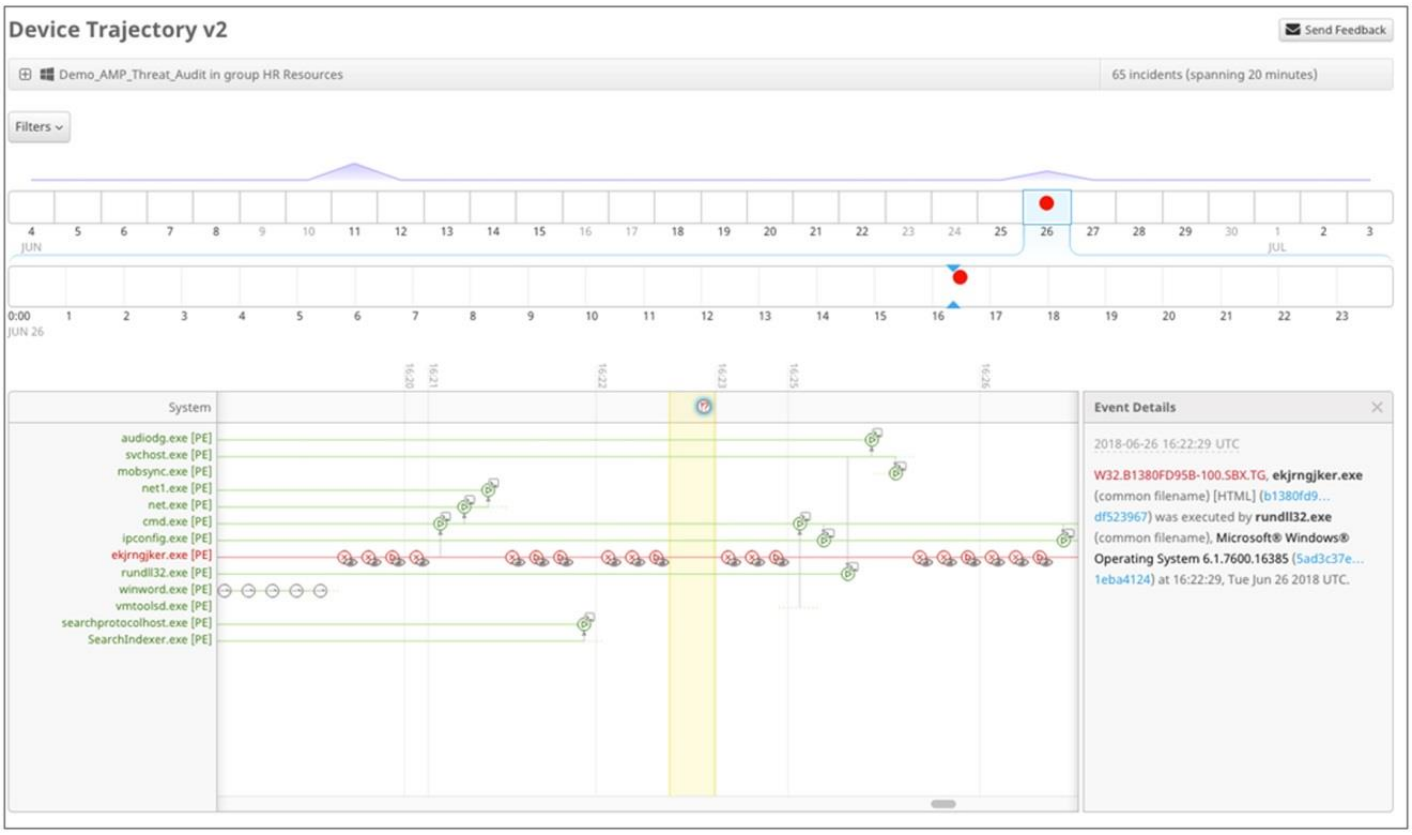

Figure 2.
Secure Endpoint device trajectory

Dynamic analysis: Secure Endpoint includes a built-in, highly secure sandboxing environment, powered by Cisco Threat Grid, to analyze the behavior of suspect files. File analysis produces detailed information on files, including the severity of behaviors, the original file name, screenshots of the malware executing, and sample packet captures. Armed with this information, you'll have a better understanding of what is necessary to contain the outbreak and block future attacks.

Retrospective security: Secure Endpoint employs patented technology that automatically uncovers advanced threats that have entered your environment. Powered by continuous monitoring, Secure Endpoint correlates new threat information with your past history and automatically quarantines files the moment they start to exhibit malicious behavior. This automated response to the latest threats provides a faster time to detection and greatly reduces the proliferation of the malware.

Command line visibility: Gaining visibility into command line arguments helps to determine if legitimate applications, including Windows utilities, are being used for malicious purposes. Secure Endpoint can uncover hard-to-detect behavior, such as the use of vssadmin to delete shadow copies or disable safe boots; PowerShell-based exploits; privilege escalation; modifications of access control lists; and attempts to enumerate systems.

Endpoint isolation: It is critical to isolate endpoints that have been compromised to stop threats from spreading and prevent them from communicating with their C&C while at the same time allowing information exchange with trusted resources such as the Secure Endpoint cloud. Endpoint Isolation allows one-click isolation of an infected endpoint along with the ability to whitelist trusted network resources. The endpoint can be de-isolated by a single click by the admin or through an unlock code by the user.

Advanced search: Advanced Search is an advanced capability in Cisco Secure Endpoint designed to make security investigation and threat hunting simple by providing over a hundred pre-canned queries, allowing you to quickly run complex queries on any or all endpoints. This enables you to gain deeper visibility on what happened to any endpoint at any given time by taking a snapshot of its current state. Whether you are doing an investigation as part of incident response, threat hunting, IT operations, or vulnerability and compliance, Advanced Search gets you the answers you need about your endpoints fast.

Cisco Secure Endpoint independent third-party tests

Platform support and compatibility

Secure Endpoint is compatible with the following operating systems

- Microsoft
  - Windows 8, 8.1
  - Windows 10
  - Windows Server 2012, 2012 R2, 2016, 2019
- Linux
  - Red Hat Enterprise Linux or CentOS 6.9, 6.10, 7.4-7.8, 8.1, 8.2
  - Oracle Linux (Red Hat Compatible Kernel) 6.10, 7.7, 7.8, 8.1, 8.2
- Android
  - Android 6.0 (Marshmallow) and above
- Apple
  - iOS 11.3 and above
  - macOS 10.13, 10.14, 10.15

Warranty information

Find warranty information on the Cisco.com Product Warranties page.

Ordering information

Find the ordering guide here.

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital® can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce capital expenditures, accelerate your growth, and optimize your investment dollars and return on investment. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For more information

For more information, please visit the following link:

Cisco Secure Endpoint

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.