

Endpoint Security Solutions

SOLUTION BRIEF

WHY IS ENDPOINT SECURITY IMPORTANT?

Endpoint security is moving quickly beyond malware:

- 33% increase in mobile ransomware
- 600% increase in IOT attacks
- 80% Increase in iOS and Android vulnerabilities
- 56% Increase in risky Wi-Fi networks
- 54% increase in mobile malware variants
- Linux is used to power 96.3% of the world's top servers and is vulnerable to attack
- 70+ million records stolen or leaked due to poor AWS configuration

Get the industry-leading endpoint security solution to help protect your business.

AWARDS

- Radicati APT Market Quadrant Top Player, 2023
- Radicati Endpoint Security Market Quadrant Top Player, 2023
- SE Labs Best Endpoint Enterprise Winner, 2023
- AV-Test Best Protection Winner (four times consecutively)
- SE Labs Best Enterprise Endpoint Winner; Highest AAA rating for 42 consecutive quarters
- SC Magazine Recommended "We love this product" Award
- Named to CRN's 2021 Mobile 100 List

Key Capabilities

The Most Comprehensive Protection

Symantec® industry-leading endpoint solutions secure all endpoints, including laptops, desktops, iOS phone and tablets, Android phones and tablets, servers, storage human-machine interface and operational technology, cloud workloads, containers, and cloud storage.

Cloud and Hybrid Options

While on-premises solutions remain the primary defense mechanisms for many data centers, the disappearance of the traditional network security perimeter, the need for cost reduction, and support for mobile and remote users has driven the need to move to security in the cloud. By offering endpoint solutions in the cloud, Symantec solutions offer options deployments on-premises, in the cloud, or a hybrid solution of both.

A Single Agent

Ponemon Institute found organizations install, on average, seven different endpoint agents to support IT management and security. Each agent operates independently with its own console and set of rules and policies—all of which need to be configured, rolled out, managed, and maintained. In addition to creating more IT overhead and costs, multiple products introduce defense gaps and errors, increasing the chances you'll miss a threat.

Symantec Endpoint Security deploys a single agent for protection, endpoint detection and response (EDR), and application control and isolation.

A Single Console

Symantec Endpoint Security allows an administrator to deploy and manage all endpoints through a single console with real-time threat visibility across laptops, desktops, mobile devices, servers, and cloud workloads.

The Only Solution with Integrated Breakthrough Security Technologies

Symantec Endpoint Security is the only solution with adaptive protection, full EDR, breach prevention, application isolation, and application control capabilities integrated with endpoint protection.

Autonomous Security Management

Symantec Endpoint Security delivers autonomous security management that learns from administrators, the organization, and the community to continuously assess and strengthen the security posture. It also uses AI-guided management to establish strong security policies with fewer misconfigurations to help improve overall security hygiene and posture.

Real-Time Threat Information

Symantec Endpoint Security leverages real-time threat information, threat analytics, content classification, and comprehensive threat-blocking data from the Symantec Global Intelligence Network.

Easy Endpoint Security Management

The Symantec Endpoint Security portfolio includes tools that help manage endpoint security deployments and workflows.

Endpoint Security Solutions

THE MOST AWARD-WINNING SOLUTION ON THE MARKET

The Symantec Endpoint Security Portfolio continues to get rave reviews and multiple awards for industry leadership, performance, efficacy.

“One of the biggest benefits of Symantec solutions is the ease of use. Everything is in a single console: you can deploy policies from the cloud down to on-prem, and still see what’s going on in the cloud while you do it.”

– Alan Roche, Technical Director, Threatscape

“Since integrating SES Complete, we are better equipped to defend, identify and prevent further targeted malware attacks. Due to the number of applications running at any given time within our network, the increased visibility into system behavior has allowed SOC teams to identify ransomware and other malware at much greater speeds, reducing the risk of major data breaches.”

– Manager, Endpoint Security and Analytics, Global Telecom Organization

A Look at the Portfolio

The Symantec Endpoint Security Portfolio helps prevent, harden, detect, and respond to emerging threats across laptops, desktops, tablets, mobile phones, servers, and cloud workloads. It protects businesses across the entire attack chain.

Pre-Attack: Attack Surface Reduction

- Breach assessment
- Adaptive protection
- Vulnerability remediation
- Device control
- Application control and isolation
- Endpoint security deployment and workflow management
- Human-machine interface and operational technology

Attack Prevention

- Malware prevention
- Exploit protection
- Behavior-based prevention
- Secure connection: Wi-Fi, network integrity, and smart VPN
- Storage protection
- Cloud workloads and container protection

Breach Prevention

- Deception
- Active directory defense
- Auto-managed policies
- Network firewall and intrusion prevention
- File integrity monitoring
- Storage protection
- Cloud workloads and container protection

Post-Breach: Detection and Response

- Targeted attack analytics
- Behavioral forensics
- Expert SOC investigator
- Threat hunting and rapid response
- Adaptive incidents
- XDR