Symantec Endpoint Security Solutions Overview

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.

Endpoints are a primary target of cyber attackers. Symantec Endpoint Security prevents, hardens, detects, and responds to emerging threats across laptops, desktops, tablets, mobile phones, servers, and cloud workloads.

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 organizations' 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 offers options for any deployment, on-premises, 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 & 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 Endpoint Detect and Response (EDR), Breach Prevention, App Isolation, and App Control capabilities integrated with Endpoint Protection.

Autonomous Security Management

Symantec Endpoint Security delivers autonomous security management that learns from admins, the organization, or the community to continuously assess and strengthen your security posture. It also uses Artificial intelligence (AI) guided management for establishing 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 you manage your endpoint security deployments and workflows.

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."
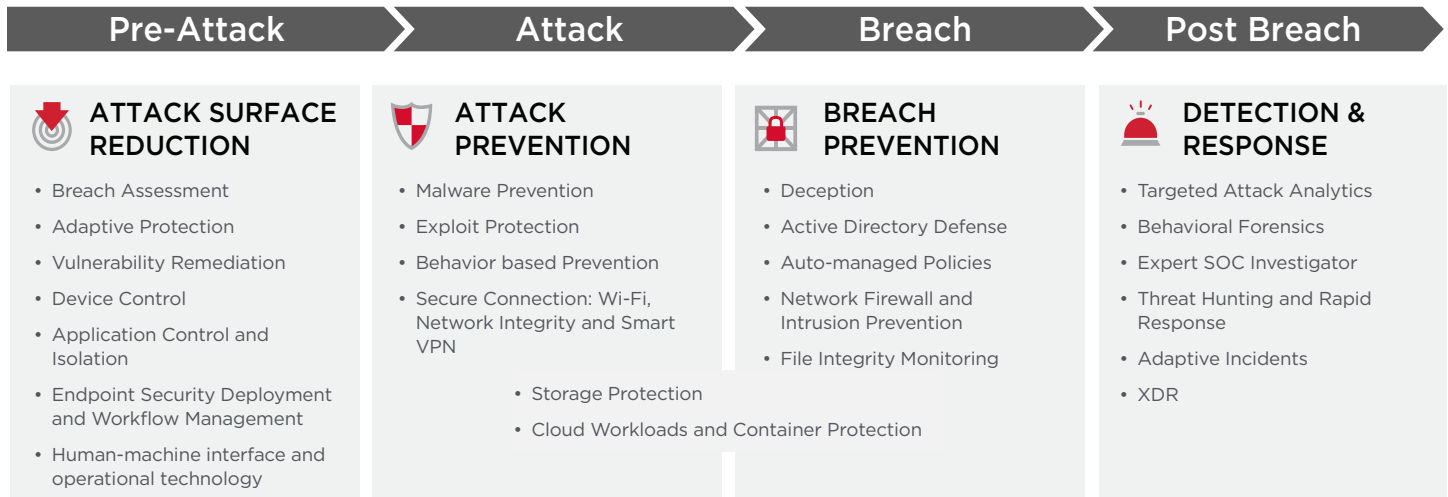
– Manager, Endpoint Security & Analytics | Global Telecom Organization

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

A Look at the Portfolio

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

Pre-Attack	Attack	Breach	Post Breach

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

DETECTION & RESPONSE

- Targeted Attack Analytics
- Behavioral Forensics
- Expert SOC Investigator
- Threat Hunting and Rapid Response
- Adaptive Incidents
- XDR

To learn more about these solutions and the Endpoint Security portfolio, go to Symantec.com or reach out to your Broadcom Sales Representative.