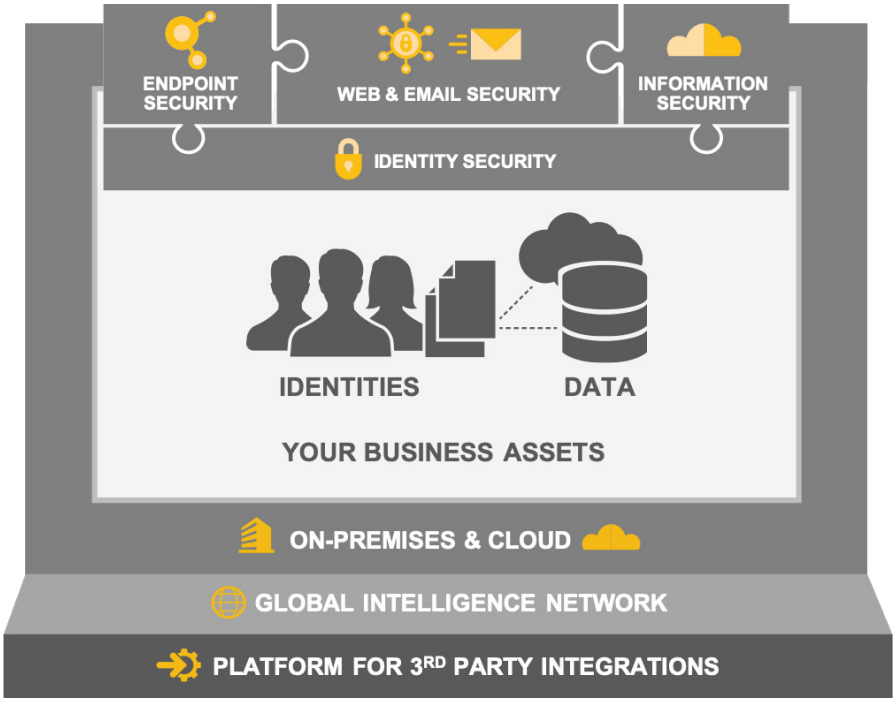
Symantec
A Division of Broadcom

Integrated Cyber Defense



The Symantec Integrated Cyber Defense (ICD) Platform delivers Endpoint Security, Information Security, Web & Email Security, and Identity Security across on-premises and cloud infrastructures, to provide the most comprehensive threat protection and compliance for your enterprise.

ENDPOINT SECURITY

Endpoint Security is the critical last line of defense in protecting user devices from cyber-attacks and keeping the sensitive information stored on those devices from falling into the wrong hands. Also includes solutions for storage and data center devices.

INFORMATION SECURITY

Sensitive documents and proprietary information should never fall into the wrong hands. Symantec offers a tightly integrated set of data protection and cloud security solutions to help organizations protect their data wherever it resides.

WEB & EMAIL SECURITY

Email and web access are the lifeblood and essential communication means for every modern organization. Symantec has a full array of web and email security solutions, as well as a shared set of advanced threat protection technologies.

IDENTITY SECURITY

Users and applications are a primary point of attack in any organization. Identity Security strengthens digital relationships by seamlessly connecting trusted users to trusted applications, all while preventing fraudulent access and session hijacking.

Symantec Endpoint Security

Employees access data and applications from billions of devices with different capabilities, applications, and operating systems. Endpoint Security is the critical last line of defense in preventing those devices from being used as part of a cyber attack and from keeping the sensitive information stored on those devices from falling into the wrong hands. Symantec offers solutions for end-user endpoints as well as for storage and data center devices.

Endpoint

Symantec Endpoint Protection (SEP)

SEP is a market-leading endpoint protection solution using technologies like anti-virus, firewall, and IPS to detect and block attacks against devices. SEP is a standalone product with on-premises and hybrid.

Endpoint Security Enterprise

The core endpoint security offering, delivering protection and detection in a single solution along with breach assessment and prevention capabilities. Endpoint Security Enterprise protects all endpoints (workstations, and mobile devices) across all major operating systems, is easy to deploy with single agent installation, and provides flexible management options (cloud, on-premises, and hybrid).

Endpoint Security Complete

The enhanced endpoint security offering, delivering attack surface reduction along with detection and response capabilities alongside all of the capabilities of Endpoint Security Enterprise.

Endpoint Detection and Response (EDR) / Managed EDR

Exposes persistent attacks with precision detections and global threat intelligence, minimizing false positives and helping to ensure high levels of productivity for security teams. EDR is available as a standalone or part of Endpoint Security Complete. Organizations can also opt for Symantec's end-to-end Managed EDR service.

Threat Hunting Center

Analytics and threat detection platform that correlates all logs against active threat intelligence to expose previously unknown threats in an enterprise, reducing the potential impact of incidents and data breaches.

Threat Defense for Active Directory

Contains attacks before they can persist on the domain by disrupting AD reconnaissance activity, Domain Admin credential theft, and lateral movement.

Endpoint Protection Mobile

Provides strong protection and visibility for mobile-related threats on iOS and Android devices.

Endpoint Management

Securely manages the entire lifecycle of desktops, laptops, and servers across Windows, Mac, Linux, Unix, and virtual environments, including deployment, asset management, and patch management to reduce costs and increase productivity.

Storage & Data Center

Data Center Security

Secures, hardens, and monitors the compliance posture of server systems for on-premises, public, and private cloud data centers.

Endpoint Protection for VDI

Combines agentless anti-malware protection with agent-based, multi-layer threat protection deliver operationally efficient security for Virtual Desktop Infrastructure (VDI) deployments.

Protection Engine for Storage

Provides scalable, high-performance threat detection services to protect valuable data stored on network attached storage (NAS) devices.

= Key product as part of our ICD portfolio

Symantec Web & Email Security

The web and email are the lifeblood of almost every modern organization, and form the basis of how they communicate with the outside world. Web and email also happen to be the main vectors exploited in cyber attacks, so keeping them safe is essential in reducing security risk and maintaining business continuity. Symantec has a broad portfolio of web and email security solutions, strengthened by a shared set of advanced threat protection technologies.

Web

Secure Web Gateway: ProxySG / Advanced Secure Gateway / Web Security Service

High-performance web security proxy that sits between users and the internet to identify malicious payloads and to control sensitive content. The proxy consolidates a broad set of security and compliance features to authenticate users, filter web traffic, identify cloud application usage, provide data loss prevention, deliver threat prevention, and ensure visibility into encrypted traffic. Available as on-premises , cloud, or hybrid deployments. On-premises products include ProxySG and ASG (Advanced Secure Gateway), which combines the capabilities of ProxySG and Content Analysis into a single platform. Web Security Service (WSS) is our cloud-delivered service and can be deployed along with on-premises gateways for a hybrid solution.

WebFilter / Intelligence Services

Real-time protection for web content, security categorization, and web application control, powered by the Symantec Global Intelligence Network. Customized threat risk control policies can eliminate high-risk web traffic, while allowing access to sanctioned websites and applications.

Web Isolation

Creates a secure browsing environment for web users by executing sessions remotely and only sending safe rendering information to users' browsers, preventing any web-borne threats from reaching users' devices.

Reverse Proxy / Web Application Firewall

Secure and accelerate delivery of hosted mobile and web applications to end users, customers, employees and vendors with a solution based on the industry-leading ProxySG platform.

Encrypted Traffic Management / SSL Visibility Appliance

Symantec SWG and SSL Visibility Appliance extend security policy to encrypted traffic by decrypting traffic, sharing it with other tools to ensure security and compliance, and then re-encrypting it to preserve privacy.

Reporter

Scalable log collection and storage that helps create intuitive reports and obtain a holistic security posture by correlating logs between ProxySG, Advanced Secure Gateway, Web Security Service, Content Analysis, and Reverse Proxy/Web Application Firewall deployments.

Management Center

A unified management platform that gives customers centralized visibility and control over ProxySG, ASG, Web Security Service, SSL Visibility Appliance, Content Analysis, Malware Analysis, Reporter, MACH5 and PacketShaper.

Performance Optimization: PacketShaper, MACH5

Improve user and customer experience by understanding, optimizing and accelerating web and application performance.

Email

Symantec Messaging Gateway / Email Security.cloud

Market leading email security for on-premises, cloud (e.g. Office 365 or G Suite) or hybrid messaging environments. Protects email from a wide range of threats including spam, advanced attacks, fraudulent email and sensitive data loss. Symantec Messaging Gateway is our on-premises solution, while Email Security.cloud is our cloud-delivered service; the two can also be deployed together for a hybrid solution.

Email Threat Detection and Response

Adds advanced detection technologies such as cloud-based sandboxing and click-time URL protection to the Symantec Email Security.cloud service. Equips security teams with comprehensive analytics to enable proactive and fast threat remediation. Similar capabilities can be added to the Symantec Messaging Gateway.

Email Threat Isolation

Insulates users from spear phishing, credential theft, and ransomware attacks by isolating malicious links, attachments and downloads, while safely rendering webpages in read-only mode.

= Key product as part of our ICD portfolio

Symantec Web & Email Security

Email Fraud Protection

Cloud-based service that combats Business Email Compromise and other fraudulent email attacks. Simplifies and automates compliance with email sender authentication standards.

Advanced Threats

Content Analysis

Multi-layer inspection platform that works with ProxySG, Symantec Endpoint Protection, Symantec Messaging Gateway, Security Analytics and other tools to protect against known threats, sources and signatures. Works in conjunction with Malware Analysis to identify and block unknown threats.

Malware Analysis

Sophisticated sandboxing solution that works in conjunction with Content Analysis to identify unidentified malware before it ever reaches a user.

Security Analytics

Advanced network security forensics solution that performs full-packet capture to provide complete network security visibility, anomaly detection, and real-time content inspection for all network traffic to help detect and resolve security incidents more quickly and thoroughly.

Symantec Information Security

Knowing where all your sensitive documents, spreadsheets, and other proprietary information lives, and making sure it doesn't fall into the wrong hands, is fundamental to maintaining security and compliance. An increasingly complex regulatory environment and the migration to the cloud, make this challenge even more daunting. Symantec offers a tightly integrated set of data protection and cloud security solutions to help organizations protect their data wherever it resides.

Data

Data Loss Prevention (DLP)

Discovers and remediates data loss based on content inspection and contextual analysis of data at rest, data in motion and data in use both on premises and in the cloud. Includes data classification and rights management capabilities. Prevents accidental and malicious exposure of confidential data outside of authorized channels. Addresses regulatory compliance, insider threats and cloud migrations.

Information Centric Analytics

User and entity behavior analytics identifies anomalous or suspicious activity to help discover potential insider threats and data exfiltration. Builds behavior profiles of users and entities. Correlates security event telemetry from many data sources, including DLP, Endpoint Protection, and ProxySG.

VIP

Strong, multi-factor authentication with single sign-on ensures only the right users on the right devices are able to access corporate resources. Prevents account takeover attacks and identity fraud. Authentication methods, such as push notifications, one-time passwords, biometrics.

Encryption

Encryption for laptop and desktop drives, removable media, files, and emails with cryptographic key management. Prevents unauthorized access to sensitive data on lost or stolen devices. Addresses data confidentiality/privacy and regulatory compliance.

Cloud

CloudSOC CASB

Cloud Access Security Broker (CASB) identifies all cloud apps in use, enforces cloud application management policies, detects and blocks unusual behavior, and integrates with other Symantec solutions including ProxySG, DLP, VIP, SAC, Email.cloud and more to extend network security policies to the cloud. Additional APIs for AWS and Azure also provide visibility and control of the management plane, along with cloud workload assurance for discovering new cloud deployments and monitoring them for critical misconfigurations.

Secure Access Cloud

Provides secure access to an enterprise's distributed resources and applications deployed in cloud IaaS environments or on-premises corporate datacenters.

= Key product as part of our ICD portfolio

Symantec Identity Security

Users and applications are a primary point of attack in any organization. Identity Security strengthens digital relationships by seamlessly connecting trusted users to trusted applications, all while preventing fraudulent access, session hijacking, and data breaches.

Access Control

Authentication

Provides greater assurance that users are who they claim to be through a combination of multi-factor credentials, contextual risk evaluation, and user behavior analysis. Built upon a unique three-way trust model that identifies the app, user, and device, and then monitors the relationship between the three.

Access Management

Provides a seamless digital experience by enabling single sign-on across apps and devices while also monitoring and protecting access to sensitive apps and data throughout the session. This is achieved through a combination of continuous user/device verification and risk-based policy enforcement.

Privileged Access Management

Prevents security breaches by addressing the highly exploited attack vector of privileged accounts. Leveraging a secure privileged credential vault, session recording, user behavior analytics, and app-to-app password management, the solution continuously controls and monitors all privileged access and activity across virtual, cloud and physical environments.

Access Governance

Identity Management

Provides comprehensive administration and governance over users and their access entitlements. Leveraging a business-oriented interface and broad integration support across on-prem and cloud-based apps, the solution automates and streamlines all user access request, fulfillment and certification across the user lifecycle.

 = Key product as part of our ICD portfolio

Symantec
A Division of Broadcom

For more product information: Symantec.com

November 1, 2019