Symantec
A Division of Broadcom

Product Brief

Integrated Cyber Defense

Comprehensive Threat Protection

At a Glance

Every enterprise faces daunting challenges in protecting its business:

- Emerging and evolving threats
- Privacy and compliance regulations
- Increased risk that accompanies digital transformation

With 100s of point-solution vendors and cheap, ineffective tools, enterprises face a cyber security dilemma that only a truly integrated platform can resolve.

What Makes ICD a Platform?

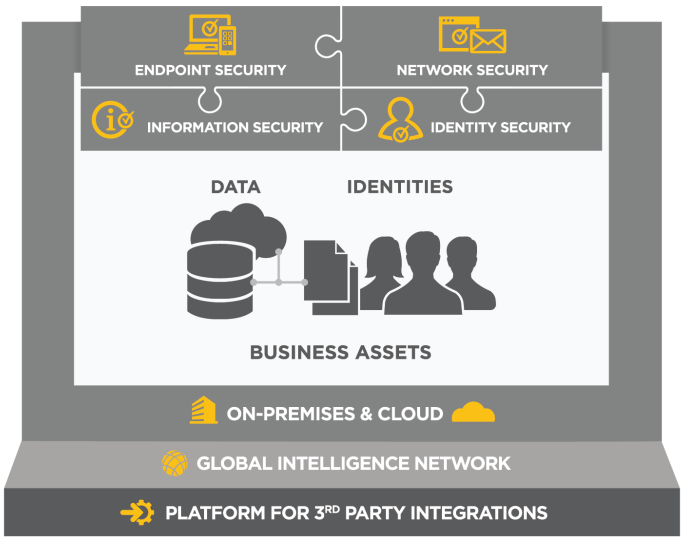
- Unifies on-premises and cloud solutions for seamless deployment and operations
- Orchestrates intelligence globally and dynamically, analyzing data from the world's largest civilian threat intelligence network
- Protects all attack points: Endpoint, Network, Information, and Identities
- Integrates critical security technologies, making it much quicker to adjust your security posture dynamically, when unexpected attacks occur

Industry-Leading Solutions Integrated into a Single Platform

Industry analysts across the globe have named Symantec a global leader in Endpoint Security, Web Security, Information Security, Email Security, and Privileged Access Management.

Overview

The Symantec™ Integrated Cyber Defense (ICD) platform delivers Endpoint Security, Information Security, Network 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 cyberattacks and keeping the sensitive information stored on those devices from falling into the wrong hands. Also includes solutions for servers 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.

Network Security

Email and web access are the lifeblood and essential communication means for every modern organization. Symantec has a full array of network security solutions to protect web, email, and web traffic as well as 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 cyberattack 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 servers and data-center devices.

Endpoint

Endpoint Security Complete

Our most complete endpoint security offering delivers protection, detection, and response in a single solution. Symantec Endpoint Security Complete addresses threats along the entire attack chain. It protects all endpoints (workstations, servers, iOS and Android mobile phones and tablets) across all major operating systems, is easy to deploy with a single-agent installation, and provides flexible management options (cloud, on-premises, and hybrid).

Endpoint Security Enterprise

A core endpoint security offering delivers multilayered protection and detection in a single solution covering workstations, servers, mobile phones, and tablets. Endpoint Security Enterprise includes innovative and advanced capabilities, all managed through a cloud-based console.

Symantec Endpoint Protection (SEP)

SEP is a market-leading endpoint protection solution that uses technologies like anti-virus, firewall, and IPS to detect and block attacks against devices. SEP is on-premises only.

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.

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, multilayer threat protection that delivers operationally efficient security for Virtual Desktop Infrastructure (VDI) deployments.

Cloud Workload Protection

Symantec Cloud Workload Protection (CWP) automates security for public cloud workloads, enabling business agility, risk reduction, and cost savings for organizations, while easing DevOps and IT administrative burdens. Rapid discovery, visibility, and elastic protection of public cloud workloads enable automated security policy enforcement to protect applications from unknown exploits. Cloud-native integration allows DevOps to build security directly into application deployment workflows, while support for tools such as Chef and Puppet automates configuration, provisioning, and patching.

Pre-Attack	Attack	Breach	Post Breach
ATTACK SURFACE REDUCTION	**ATTACK PREVENTION**	**BREACH PREVENTION**	**DETECTION & RESPONSE**
• Breach Assessment • Device Control • Application Control • Behavioral Isolation	• Machine Learning-driven Exploit and Malware Prevention • Behavior-based Prevention • Network Integrity, Wi-Fi Reputation, and Smart VPN	• Deception • Active Directory Defense • Auto-managed Policies • Network Firewall & Intrusion Prevention	• Flight Data Recorder • Behavioral Forensics • Threat Hunter with ML and Expert Analysis • Rapid Response

Symantec Network Security

Users are everywhere and need quick access to data and cloud applications around the clock. In the cloud, on-premises, or both, you need to stop inbound and outbound threats targeting your end users, information, and key infrastructure. Today's web and email protection must account for this new reality while balancing security, performance, complexity, and cost.

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 combine the capabilities of ProxySG and Content Analysis into a single platform. Web Security Service (WSS) is our cloud-delivered service that can be deployed along with on-premises gateways for a hybrid solution.

Intelligence Services
Real-time protection for web content, security categorization, and web application control is 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
Safe web browsing that protects against malware and phishing threats, even when inadvertently visiting uncategorized and risky websites. Remotely executing web sessions in a secured container stops malware downloads, and read-only browsing defeats phishing attacks. Available as a cloud service or on-premises virtual appliance, Web Isolation can be standalone or integrated with a proxy solution (for example, Proxy SG or WSS).

Reverse Proxy Web Application Firewall
Secure and accelerated delivery of hosted mobile and web applications to end users, customers, employees, and vendors with a solution based on the industry-leading ProxySG platform.

SSL Visibility Appliance
SSL Visibility Appliance extends 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.

Email

Symantec Messaging Gateway/Email Security.cloud
Market leading email security for on-premises, cloud (for example, 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 Security with Threat Detection 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.

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.

Symantec Network Security (continued)

Advanced Threats

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

Security Analytics
Advanced Network Traffic Analysis (NTA) and 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 does not 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.

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

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
Secure Access Cloud is a cloud- delivered service providing highly secure granular access management for enterprise applications deployed in IaaS clouds or on-premises data center environments. This SaaS platform eliminates the inbound connections to your network and creates a software-defined perimeter between users and corporate application and establishes application-level access. This zero-trust access service avoids the management complexity and security limitations of traditional remote access tools, ensuring that all corporate applications and services are completely cloaked—invisible to attackers, targeting Applications, Firewalls, and VPNs.

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 Management

SiteMinder

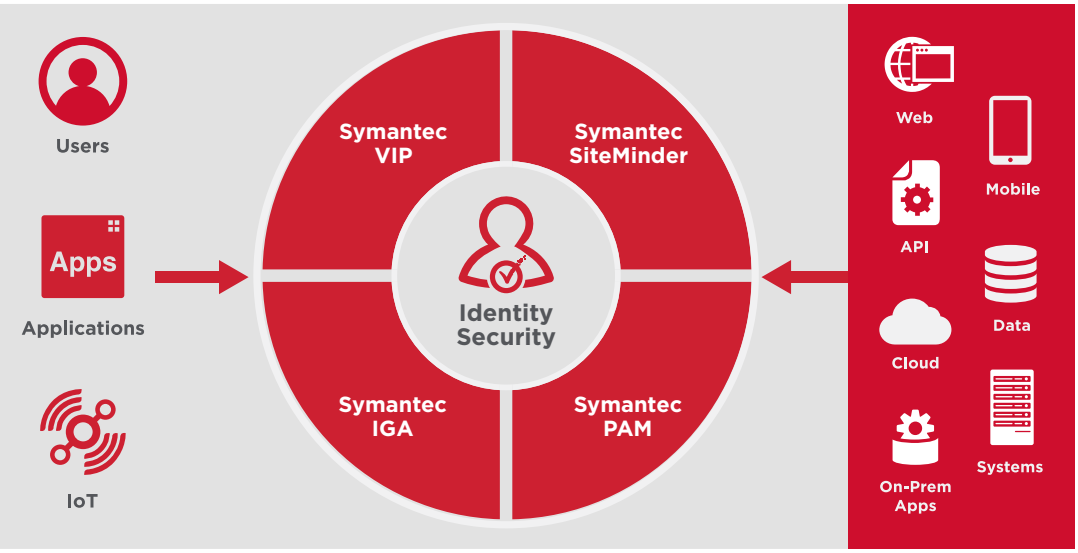
Comprehensive access management solution that provides authentication management, single sign-on, identity federation, authorization, and access control across multiple cloud, mobile, and hybrid environments. SiteMinder provides interoperability through open standards including OpenID Connect, OAuth, SAML, and WS-Federation. Granular security policies stop unauthorized access and explicitly grant or deny access to all protected applications and resources through security policies based on a user's profile attributes, group memberships, roles, and other criteria. Dynamic session assurance helps prevent session hijacking during the entire user session. Session management can be implemented with or without cookies, providing a clear audit trail of everything the user did during a session impeding hackers from hijacking legitimate sessions with stolen cookies. SiteMinder integrates with Symantec VIP and with partner applications and third-party services.

Directory

A battle-tested directory server that provides the scalability and reliability needed to support the most demanding on–premises, cloud, and IoT applications with minimal infrastructure and personnel resources. The solution's innovative design enables ultra high-speed performance as well as transparent load balancing, multi-master replication, and state-based recovery.

VIP

Secure, reliable, and scalable authentication service that provides risk-based and multi-factor authentication for all types of users. Risk-based authentication transparently collects data and assesses risk using a variety of attributes such as device identification, geolocation, user behavior, and threat information from the Symantec Global Intelligence Network (GIN). VIP provides multi-factor authentication using a broad range of authenticators such as Push, SMS or Voice OTP, FIDO U2F, and Fingerprint Biometric. This intelligent, layered, security approach prevents inappropriate access and online identity fraud without impacting the user experience. VIP also denies access to compromised devices before they can attempt authentication to your network and tracks advanced and persistent threats. An intuitive credential provisioning portal enables self-service that reduces help desk and administrator costs. An integration with Symantec CloudSOC protects against risky behavior even after application login.



Symantec VIP
Positively identify users, apps, and devices requesting access

Symantec SiteMinder
Enforce authorization policies and monitor user activity

Symantec PAM
Protect access to privileged accounts and credentials

Symantec IGA
Automate and streamline least privileged access processes

Governance and Administration

IGA

Delivers comprehensive access governance and management capabilities through an easy-to-use, business-oriented interface. Broad provisioning support for on-premises and cloud apps enables you to automate the granting of new entitlements and removal of unnecessary ones throughout the identity lifecycle. Self-service enables end users to request new access, manage their profile attributes, or reset a forgotten password to reduce burden on your help desk. Virtually all business-user functionality is provided in a single, mobile-optimized web portal, giving users access to accomplish tasks in the system, even when they are on the go. Access governance streamlines and simplifies the processes associated with reviewing and approving entitlements. Entitlements certification allows the business to examine and certify that privileges are appropriate. The Virtual Appliance form factor combines all components into a single appliance reducing time-to-value, license and services costs.

Privileged Access Management

PAM

PAM can minimize the risk of data breaches by continually protecting sensitive administrative credentials, controlling privileged user access, and monitoring and recording privileged user activity across virtual, cloud, and physical environments. PAM is quick to deploy, easy to maintain, and can process and record significantly more simultaneous requests with a fraction of the hardware compared to leading competitors. The solution also provides both network-based and agent-based architectures for flexibility. PAM includes a privileged credential vault, session recording, threat analytics, host-based access control for mission-critical servers, and application-to-application password management to address non-human actors, such as applications, configuration files, and scripts.

Privileged Access Governance

Ensures that all user access to privileged accounts and credentials is necessary and appropriate. Privileged access governance applies basic identity governance and administration processes to privileged users including: automated provisioning for new users based on group members or roles; automated deprovisioning when users leave the organization or change jobs; streamlined access request process that gathers appropriate approvals and checks for security violations before new privileged access is granted; periodic reviews and attestations to ensure that access to privileged accounts is still necessary. This solution requires both Symantec PAM and Symantec IGA. Together, these solutions significantly improve your security posture and help you provide proof to auditors that access to all privileged accounts has been properly reviewed and authorized.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-ICD-PB100 July 15, 2020