SOLUTION BRIEF

Symantec® Enterprise Cloud

Data-Centric Hybrid Security for the Large Enterprise

KEY BENEFITS

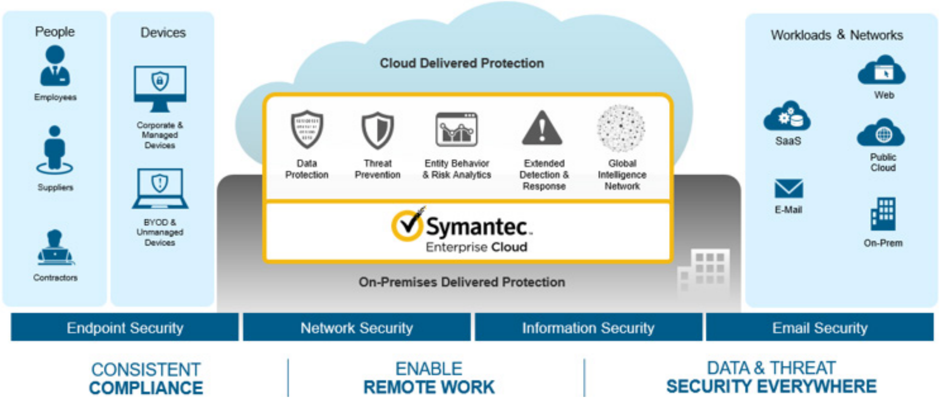
- **Consistent compliance:** Apply and manage compliance controls consistently across your infrastructure
- **Secure remote work:** Protect critical enterprise assets wherever they are and from wherever they are accessed
- **Data and Threat Protection Everywhere:** Unify intelligence across control points to detect, block, and remediate attacks

CRITICAL CAPABILITIES

- Delivers cross-control point security controls from a single platform
- Supports public cloud, private cloud, on-premises, and hybrid deployments
- Protects both managed and unmanaged devices
- Supports all major operating systems and platforms
- Powers one of the world's largest civilian-owned threat intelligence networks

Overview

Symantec® Enterprise Cloud, a Broadcom® cybersecurity solution, delivers data-centric hybrid security for the largest and most complex organizations in the world. It enables enterprises to meet legal, regulatory, and corporate data compliance requirements. It also empowers today's modern workforce to securely access sensitive company assets from anywhere. Symantec Enterprise Cloud unifies intelligence across control points, enabling organizations to detect, block, and remediate the newest generation of threats throughout their infrastructure. From remote devices to on-premises data centers to cloud-deployed applications, Symantec Enterprise Cloud solves the critical cybersecurity challenges facing the world's biggest multinational corporations.



Consistent Compliance across Your Infrastructure

Today's global organizations must adhere to numerous compliance regulations and implement appropriate policies everywhere that data may be stored on-premises, in private data centers, or in the cloud. Personal health information, customer payment data, and personally identifiable information are just a few examples of data that is subject to strict regulatory controls.

Managing and auditing compliance and applying consistent controls to every data repository across a large, distributed organization can be nearly impossible and the stakes are high. For example, companies paid more than $1 billion in fines in 2021 for GDPR violations globally[1].

[1] DLA Piper Survey 2022

SECURITY PORTFOLIOS

ENDPOINT SECURITY

Our endpoint security portfolio provides comprehensive protection across laptops, desktops, tablets, mobile phones, servers, and cloud workloads. The single unified agent provides a stack of prevention and detection capabilities, including Adaptive Security, Threat Protection for Active Directory, Mobile Threat Defense and Endpoint Detect and Response. Lock down devices with our Advanced Application Control functionality. Targeted Attack Analytics combined with our Threat Hunters uncover 100,000 new targeted attacks every month. Our extensive server security offerings protect business-critical servers whether deployed in private data centers or in the public cloud.

NETWORK SECURITY

Our network security portfolio blocks inbound and outbound threats that target end users, both in the office or on the road, sensitive information, and key infrastructure. Our offerings include both on-premises and cloud-deployed Secure Web Gateway (SWG) products, Advanced Threat Intelligence, Content Analysis, Management and Reporting, Zero Trust Network Access (ZTNA), Sandboxing, and Web Isolation. The Symantec network portfolio provides complete security controls for organizations implementing a modern Secure Access Service Edge (SASE) architecture.

Symantec Enterprise Cloud provides pre-built templates for all major compliance regulations and allows compliance policies to be rolled out wherever enterprise data lives: both on-premises in private data centers or in the cloud. Symantec products across Broadcom portfolios support pre-built templates. This means that compliance controls can be applied consistently across an organization, and a single governance team can manage all data risk and perform audits from one platform.

Symantec Enterprise Cloud can enforce company-specific policies as well using advanced policy engines. Organizational policies such as blocking attempts to copy sensitive data outside the organization, providing additional security when an employee visits an unknown website, or forbidding access to an unauthorized domain, can all be enforced using Symantec Enterprise Cloud. Policies can be pushed out on a per-employee basis and managed consistently from a single platform. As an organization migrates to the cloud, existing policies can easily be migrated from on-premises enforcement points to cloud-based enforcement.

Compliance controls can be applied consistently across the organization, and a single governance team can manage all data risk and perform audits from one platform migrated from on-premises enforcement points to a cloud-based enforcement.

Secure Remote Work

A confluence of factors has made it more challenging than ever for large enterprises to support secure access to sensitive resources for remote employees, while at the same time ensuring a positive user experience for these remote workers.

Enterprise data today is everywhere—in corporate-owned data centers, in the public cloud, and in third-party SaaS apps, often outside the direct control of the enterprise itself.

Furthermore, there is no longer any sense of being *inside* or *outside* the enterprise network in today's modern corporation, and this perimeter has disappeared forever. Almost every employee works remotely at least some of the time—a phenomenon that was massively accelerated by the COVID-19 pandemic.

Also, it is not just full-time employees who access sensitive enterprise assets. Contractors, third-party suppliers, and partners (many of whom connect on devices that are not controlled by the enterprise) all must securely and efficiently connect to enterprise data and applications to do their jobs.

SECURITY PORTFOLIOS (CONT.)

INFORMATION SECURITY

Our information security portfolio keeps sensitive enterprise data secure no matter where it lives—on-devices, on-premises, in private data centers, in the cloud, and on the road. Our solutions provide comprehensive discovery, monitoring, and protection capabilities, ensuring that you have complete visibility and control over your information everywhere it goes and can apply consistent data protection policies everywhere. We also help ensure that your data adheres to regulatory compliance requirements.

EMAIL SECURITY

Symantec email security offerings provide comprehensive protection against email-delivered malware and ransomware, malicious URLs, and business email compromise (BEC) fraud. Capabilities includes sender authentication, fraud detection, link protection, web isolation, and security awareness training. Stop sophisticated malware attacks with click-time URL link following and sandboxing. Email Threat Isolation defends against web-hosted malware and fake, credential stealing websites. Email analytics provide accelerated detection, complete visibility, and automated remediation.

Symantec Enterprise Cloud has visibility across the entire spectrum of users, devices, networks, applications, and data, both on-premises, and in the cloud. This gives Symantec Enterprise Cloud a bird's eye view of trust and allows an enterprise to enact appropriate controls for remote access. For example:

- Triggering two-factor authentication when a contractor attempts to access proprietary source code from the organization's code repository.
- Blocking access to sensitive information for a third-party vendor who is trying to log in from a location that is physically impossible for them to have moved to since they last logged in.
- Preventing an employee from uploading sensitive information from the company customer relationship portal into their personal file storage.

Symantec Enterprise Cloud enables the Broadcom data-centric SASE architecture that covers cloud and on-premises use cases equally, and includes the Secure Web Gateway, ZTNA, Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), and Endpoint products. This solution monitors every user interaction to make sure they are secure, compliant, and consistent with baseline behavior.

Symantec Enterprise Cloud also handles cases where remote users need to securely access public or private cloud applications from devices outside the purview of the enterprise (for example, BYOD). It also drives a single console and single agent experience, improving performance and simplifying manageability.

Data and Threat Protection Everywhere

There is a new and constantly evolving generation of highly sophisticated attacks targeting large enterprises. The proliferation of targeted ransomware, attacks that emerge through the software supply chain, and attacks that leverage perfectly legitimate software to hide their tracks (also known as Living off the Land attacks), are stretching security operations teams to their limits.

Symantec Enterprise Cloud powers a Global Intelligence Network (GIN), which is one of the largest civilian security threat intelligence networks in the world. Applying artificial intelligence to over eleven trillion elements of security telemetry, Symantec Enterprise Cloud has unparalleled visibility across endpoints, networks, email, and cloud applications, allowing you to discover, block, and remediate advanced attacks that would otherwise go undetected. The solution allows organizations to deploy consistent protection across every control point. Symantec Enterprise Cloud uncovers and informs customers of about 100,000 new targeted attacks every single month.

Thanks to Symantec Enterprise Cloud, products can share threat telemetry and intelligence with each other. If Symantec Enterprise Cloud discovers a new threat attempting to infiltrate an organization through one web proxy, it automatically shares this information with all proxy customers and with every endpoint and email security deployment as well. Each product makes the rest better, and a massive data lake combined with advanced analytics allows customers to find even the stealthiest attacks.

Data-Centric, Cross-Portfolio Use Cases

Symantec Enterprise Cloud enables numerous cross-product integrations to drive data-centric security:

DLP Everywhere

Symantec DLP integrates with products across every control point to protect critical data and enforce organizational policies throughout the infrastructure.

- DLP integrates with our Secure Web Gateway portfolio to block exfiltration of sensitive data via the public internet
- DLP integrates with Symantec ZTNA to block data exfiltration through private enterprise apps
- DLP and CloudSOC® CASB integrate to prevent sensitive data exfiltration using SaaS applications.
- DLP integrates with our Endpoint Security offerings to block untrustworthy applications from accessing sensitive data on the endpoint.

XDR

The Extended Detection and Response (XDR) offering shares suspicious events from CloudSOC CASB (for example, failed logins) with Symantec Endpoint Security, providing a much broader view into the risk associated with each endpoint in the environment.

Shared Threat Intelligence

Each of our portfolios leverage our Threat Intelligence API to gain a comprehensive picture of suspicious activities in the corporate environment.

Consolidated Agent

We have consolidated our endpoint security agent and cloud web gateway (WSS) agent to seamlessly provide both endpoint and network security for roaming endpoints. This significantly simplifies the path to implementing a Zero Trust architecture.

Evolve Your Security with Your Organization

Symantec Enterprise Cloud drives the most comprehensive set of security portfolios in the industry, across endpoint, network, information, and email security. It supports every platform from iOS and Android, to Windows, Mac, and Linux, and provides security for both managed and unmanaged devices.

Symantec Enterprise Cloud powers offerings wherever they are deployed: on-premises, in the cloud, or hybrid. As customers migrate their security from on-premises to the cloud, they simply move existing on-premises policies to the analogous cloud-based products, ensuring no change in protection or behavior of security controls. Organizations can license the Broadcom portfolio for whichever deployment model they choose and can migrate products between on-premises and the cloud anytime without any renewals, new contracts, or new SKUs.

Thanks to Symantec Enterprise Cloud, products apply enforcement policies at the closest point to the user for maximal efficacy, efficiency, and user experience. For on-premises deployments, Symantec Enterprise Cloud enforces policies directly at on-premises control points, without traffic having to be directed to the cloud and then back to the on-premises infrastructure first. Similarly, for cloud-based deployments, Symantec Enterprise Cloud enforces policy at the cloud control point, without any traffic needing to first go to an on-premises data center. This delivers the best possible combination of security and user experience.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com