SOLUTION BRIEF

Secure Your Move to the Cloud

Cloud-delivered network security—protecting the modern workforce

Symantec™

Introduction

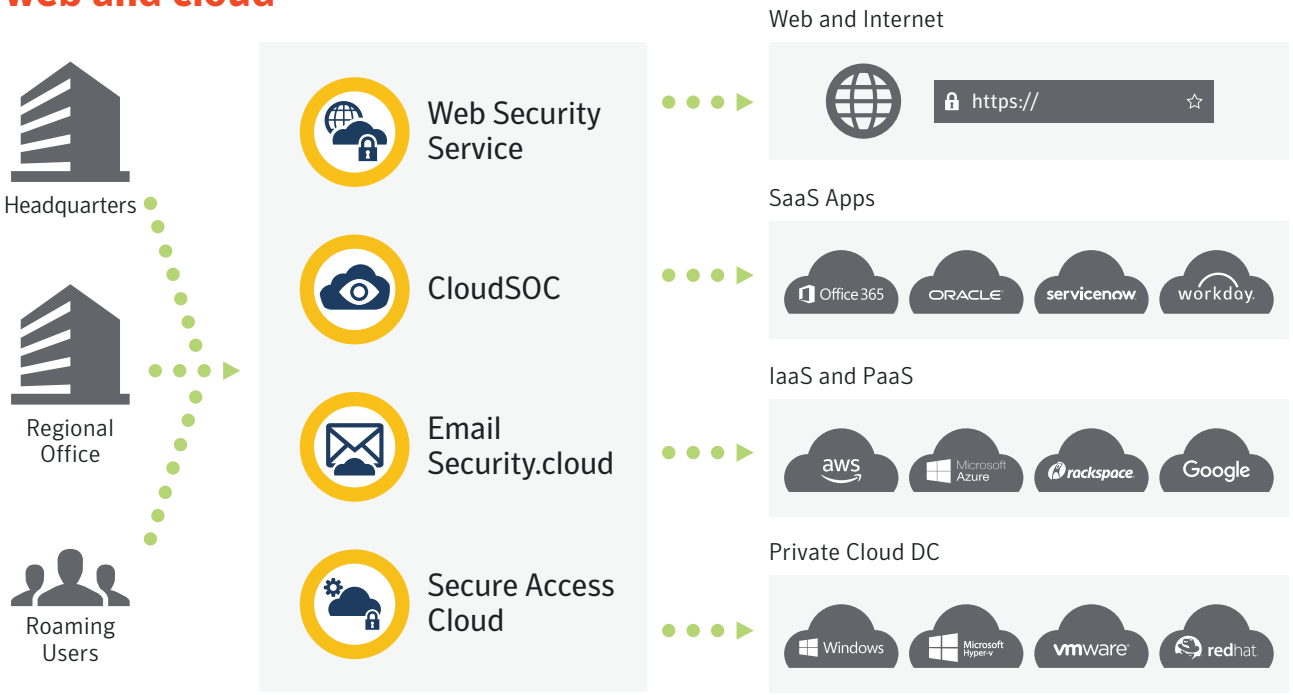
Digital transformation initiatives are causing many enterprises to rethink how they secure their operations. Adapting your business to the cloud is an opportunity to migrate to a security architecture that both improves protection and reduces complexity and expense. Answer the following to assess your cloud security readiness.

- Do you apply robust access security policies across all your users' cloud and web destinations? This includes SaaS apps, cloud email, and corporate apps on IaaS or in private clouds.
- Can you protect a workforce that includes employees, contract workers, and third parties accessing resources from managed and unmanaged devices across distributed locations?
- Do you have the visibility and monitoring capabilities you need to comply with internal and external regulations as your business is changing?
- Do your security tools work together seamlessly—and do they increase or decrease complexity?

Networks have evolved: Most user traffic now goes to corporate apps in Amazon Web Services (AWS) and Microsoft Azure; SaaS apps such as Office 365; cloud email; and the web. How do you enforce security controls in each of these areas? You could work with multiple security vendors. But sourcing, implementing, and managing such a hodgepodge is complicated, costly (especially if the technologies are not cloud-delivered), and, due to poor integration, not entirely effective.

Symantec solves for this with complete, integrated cloud security that protects all modern workflows—enabling users to safely access and use corporate apps in IaaS; SaaS apps such as Office 365 and Gmail; and the web—and simplifies implementation and operation.

Securely access and use the web and cloud



SYMANTEC ACCESS SECURITY

Web Security Service—Protecting web use

Cloud-delivered Symantec Web Security enforces consistent web security and compliance policies for all users regardless of location or device. As a cloud service, it eliminates costly backhauling from remote locations to corporate data centers for inspection and control.

Access control

With its extensive web application controls and detailed reporting features, Web Security Service enables IT administrators to create and enforce granular policies for all covered users, whether onsite or roaming. It works seamlessly with Windows Active Directory and supports SAML 2.0 to efficiently identify and authenticate users. Connect Symantec Endpoint Protection (SEP) and SEP mobile users to the service without an additional agent, and connect your branch offices via the integrated SD-WAN-based SD-Cloud Connector.

Threat prevention

Web Security Service blocks malicious sites, malware-prone file types, and botnet traffic using real-time, global web ecosystem analysis combined with inline malware detection. The service keeps out malware with multilayer, dual antivirus and heuristic analysis, and file-reputation analysis, and it scans upstream to devices, preventing threats from reaching your network. It also detonates suspicious files, performs behavioral analysis to stop advanced threats, and provides complete visibility into SSL/TLS-encrypted network traffic to find hidden threats across your entire security stack.

In addition, a strong set of native cipher suites enable re-encryption that mirrors the browser preference. This allows you to scan SSL-encrypted traffic and stop malware at the gateway while using selective decryption to protect user privacy.

Symantec Web Isolation, integrated with Web Security Service, provides secure access to potentially risky websites by creating an execution environment between users and the web—sending only a safe visual stream to the users' browsers. Web Isolation keeps web-borne threats from ever reaching your users' machines.

Compliance

Web Security Service integrates with Symantec CloudSOC cloud access security broker (CASB) gateway to extend deep visibility into shadow IT via your existing Web Security Service management console. Identify the SaaS applications your users access, and evaluate the risk of over 30,000 clouds by examining 100+ attributes. This integration powers dynamic policy enforcement (using the latest app intelligence) to automate controls based on the app name.

Web Security Service also integrates with Symantec Data Loss Prevention Cloud, ensuring you protect enterprise web and cloud traffic with our market-leading DLP. This integration enforces all your privacy and data protection regulations, even on encrypted traffic.

Cloud-delivered Web Security Service enables users to access systems from remote locations while it continuously monitors information, inspects uploaded files, automatically blocks anything identified as out of bounds, and alerts administrators and data owners when data is at risk.

CloudSOC Cloud Access Security Broker—Protecting SaaS application use

Symantec CloudSOC CASB gateway keeps your workforce secure and compliant when using sanctioned and unsanctioned SaaS cloud applications and services. It detects intrusions, threats, and high-risk user actions; protects against data loss and compliance violations; and investigates historical account activity for post-incident analysis.

Access control

Apply CloudSOC granular controls at the user, device, or location level, ensuring users access and use SaaS applications in a secure and compliant way. A cloud-situated forward-proxy gateway controls managed devices that connect to sanctioned cloud applications. The new CloudSOC Mirror Gateway controls BYOD/unmanaged devices that connect to sanctioned applications. This unique, patent-pending capability offers the market's broadest BYOD support and dramatically simplifies how you manage user access to unmanaged endpoints.

Threat prevention

CloudSOC uses data science-driven user entity and behavior analysis (UEBA) to discover attacks, and to identify suspicious activity that indicates privilege misuse, compromised user accounts, or malicious insiders. It automatically learns normal patterns, and then identifies abnormal and potentially dangerous activities such as attempts to change security settings, upload sensitive data, and terminate instances.

CloudSOC also flexibly integrates with antimalware and advanced threat protection to identify and remediate malware infections. And it integrates with Symantec Advanced Threat Protection, enabling you to apply file reputation analysis, antivirus scanning, and advanced threat sandboxing to all your cloud content.

Compliance

CloudSOC ContentIQ identifies and classifies critical compliance-related data—such as personally identifiable information (PII), protected health information (PHI), and payment card industry (PCI) content—then monitors how that data is uploaded, downloaded, and shared in cloud apps. Apply policies controlling the way you manage this data, and track and follow up on attempted compliance violations. A complete audit trail of cloud app activity dramatically simplifies how you govern SaaS application use.

Email Security.cloud—Protecting email application use

Symantec Email Security.cloud complete email defense safeguards cloud email such as Office 365 and G Suite. Drawing insights from the world's largest civilian threat intelligence network, its multilayer protection blocks new and advanced email threats with the industry's highest effectiveness and accuracy.

Access control

Email Security.cloud authenticates users by enforcing sender authentication controls (DMARC, SPF, DKIM, and others), increasing user trust and preventing impersonation attacks. 'Set and forget' configuration limits maintenance while the Service Configuration Health tool shows administrators how to refine their company's security posture. Switch on browser isolation with a single click and reduce the risk of email impersonation by automatically applying meeting sender authentication standards.

Threat prevention

Block known bad emails and spear phishing with a multilayer defense that includes behavior and reputation analysis, multiple, proprietary antivirus engines, and threat protection, isolation, visibility, sender authentication, and user awareness technologies. Email Security.cloud also speeds your attack response with analytics that provide deep visibility into targeted attack campaigns. Its integrated Email Threat Isolation capability contains malicious activity by rendering suspicious URLs and attachments in a remote execution environment.

Compliance

Granular policy enforcement supports data protection policies, impersonation controls, and encryption policies. Email Security.cloud keeps emails secure and private with policy-based encryption controls, including the ability to automatically encrypt confidential emails via a secure PDF encryption or a web pickup portal.

Secure Access Cloud—Protecting IaaS and private cloud application use

Cloud-delivered Symantec Secure Access Cloud manages granular access to enterprise applications in IaaS clouds or on-premises data centers. Avoid the complexity and security limitations of traditional remote access tools (such as VPNs) with a Zero Trust service that cloaks all corporate applications and services, making them invisible to would-be attackers. Streamline your transition to the cloud with this simple, secure, and scalable app access service.

Access control

Give your workforce quick, simple, Zero Trust access to corporate apps regardless of user location, device type (managed or BYOD), or infrastructure. The service's agentless, software-defined perimeter approach eliminates the management complexity and security limitations of traditional remote access tools (such as VPNs). At the same time, Secure Access Cloud improves network security by ensuring all corporate applications and services are invisible to would-be attackers, enterprise resources are never exposed, and network-level access is not granted.

Threat prevention

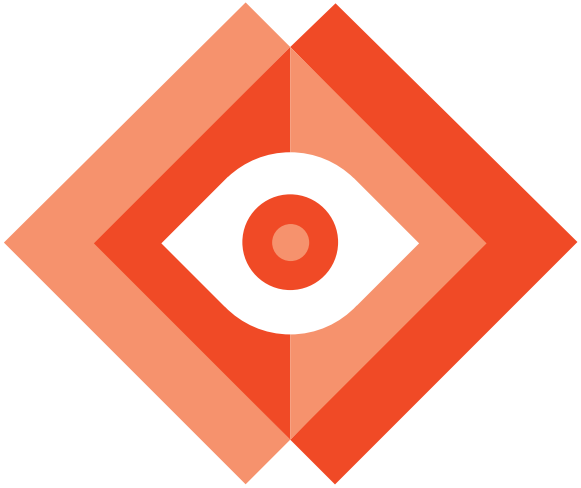
The service creates a safe, temporary connection between the user's device and the requested application. It then monitors and logs every operation, creating a detailed audit trail of each user's activity, and cloaks all corporate resources from external networks so attackers cannot see into your network devices.

Secure Access Cloud first authenticates users and, if required, validates the safety of the accessing device. A flexible, risk score-based engine authorizes application-level access, which does not expose the corporate network—even to authorized users. The connection terminates when the user completes the interaction.

Secure Access Cloud is bundled with Symantec Validation and Identity Protection, bringing multifactor authentication (MFA) to your organization's access policy controls.

Compliance

Use Secure Access Cloud to define granular polices and access controls, block secure shell (SSH) commands and downloads of sensitive files, and even restrict access to a specific set of URLs based on user identity.



Key integrations

Web Security Service with CloudSOC

These integrated services give you deep visibility into shadow IT and the ability to automate policy controls. (The Audit AppFeed provides rich cloud app information to Web Security Service.) Define the SaaS traffic you want to forward from Web Security Service to the CloudSOC CASB gateway, where you further inspect gatelets and enforce additional security and monitoring policy controls. The combined services streamline the user experience with simplified proxy chaining, unified authentication, automated log ingestion, and user interface integration.

Data Loss Prevention with Web Security Service, CloudSOC, and Email Security.cloud

Decrypt (using Web Security Service) and quickly and accurately analyze (using Symantec Data Loss Prevention Cloud) SSL traffic. Scan (offline) accounts in applications such as Box and Dropbox, catching anything your employees may have put (intentionally or inadvertently) into corporate accounts. Apply privacy and data-protection policies to all web traffic (including for remote users), accurately analyzing SSL-encrypted traffic while continuously monitoring and auditing uploaded files and automatically enforcing policy controls.

Email Security.cloud also integrates with Data Loss Prevention, preventing data loss across your entire environment. The CloudSOC and Data Loss Prevention integration safeguards data in cloud apps using the same DLP policies and response workflows you use for your endpoints, networks, and data centers.

Prevent classes of data leakage (either accidental or malicious) by identifying confidential data and controlling user cloud app transactions.

Symantec is the only CASB vendor with integrated cloud app security offerings—CASB, DLP, and threat protection—that are Gartner Magic Quadrant Leaders.

Symantec Validation and Identify Protection with CloudSOC and Secure Access Cloud

Verifying the identity of whoever is trying to connect to your network resources is a critical first step in protecting all access paths. Symantec Validation and Identify Protection establishes user trust with intelligent and multifactor authentication—now included for Symantec Secure Access Cloud customers.

Symantec CloudSOC CASB gateway also integrates with Validation and Identify Protection, providing granular policy controls throughout a cloud session based on adaptive MFA. Other vendors' CASB solutions offer only single sign-on/MFA integrations for initial login.

Web Security Service with Secure Access Cloud

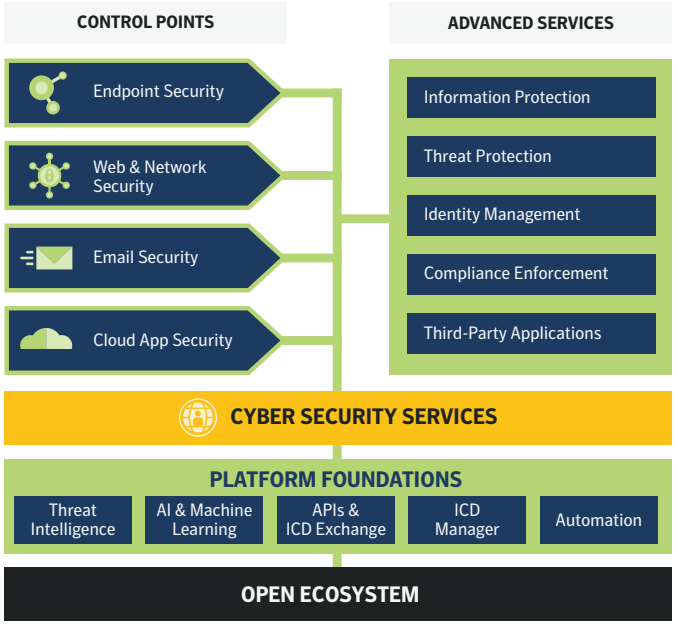
Secure Access Cloud integrates with Web Security Service, delivering enhanced contextual awareness when using our software-defined perimeter technology. For example, if Web Security Service authorizes a managed device, and the user requests a corporate application in AWS, the service automatically connects to Secure Access Cloud. Secure Access Cloud then enforces additional access controls because it recognizes the request was made by a Web Security Service-authenticated device.

Improving Security While Reducing Complexity and Expense

Symantec is the only vendor providing enterprises with complete, integrated, cloud-delivered access security services across all modern cloud and web workflows (cloud applications, email, and web). These services enforce key security and compliance controls that simply support digital transformation initiatives. Moving your security infrastructure to the cloud eliminates costly backhauling, reduces architectural complexity, improves performance, and centralizes management. No single gateway solves all modern access issues. However, there is a single vendor with the integrated services you need to secure your business-critical workflows.

Symantec Integrated Cyber Defense Platform

Symantec cloud-delivered network security services are key components of our Integrated Cyber Defense Platform, which unifies cloud and on-premises security. Symantec Integrated Cyber Defense protects across endpoints, networks, applications, and clouds, driving down cyber security costs and complexity while improving incident response times.



Take the next step

Learn more about Symantec network security products and services. Visit https://go.symantec.com/secureaccess.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527-8000 | +1 (800) 721-3934 | www.symantec.com

20A242362_SB_NETWORKSECURITY_EN