Solution Brief

# Secure the Cloud with Symantec™

## Challenge

Over the last decade, we've seen a growing adoption of cloud computing. Millions of active customers are using SaaS apps and IaaS platforms, and more moving every year to provide better business agility and greater flexibility, but this cloud migration has also expanded the attack surface and new threats and vulnerabilities have emerged.

## Opportunity

Cloud migration offers unlimited opportunities and will require new security tools and approaches, but this should result in the creation of a new security silo within the enterprise. In many cases, cloud computing augments existing on-premise data center, and this hybrid environment requires a consolidated security solution. Organizations that seamlessly integrate their new cloud computing security solution with existing on-premises security tools will reap the rewards that cloud computing offers with minimal risk and cost. Symantec can provide that bridge.

## Benefits

A comprehensive security approach, embracing the principles of both zero trust and secure access service edge models, will protect applications and data regardless of where is used or stored, on the mainframe, on-premises, or in the cloud. It also protects users and their devices which are capable from accessing resources from anywhere. The cloud requires a new security approach integrated into an existing security architecture to protect years of investment, shorten time-to-value, and enable analysis of event data to improve threat detection.

**Cloud adoption continues to increase within organizations and new agile development processes have become widespread. Along with these changes, new threats and vulnerabilities have emerged. You need a complete and comprehensive approach to address these threats without impacting the speed and agility of the business.**

## Introduction

The wide adoption of SaaS applications and IaaS platforms signals that we've entered the hybrid era, and that organizations are no longer just using the cloud for their test and development environments. Increasingly, they are migrating critical applications from their on-premises data centers, as well as deploying new cloud native applications.

The hybrid era has broken the boundaries of desktops and data centers to embrace the mobile, social, global, crowd-sourced, always-on realities of modern life. Not only has cloud computing altered the way people work, it has dramatically expanded the computing environment, upending traditional business and IT operations. Additionally, as cloud adoption increases and new agile development processes become widespread, new threats and vulnerabilities have emerged, and existing security tools and approaches are struggling to deal with these new security requirements.

The Symantec™ Integrated Cyber Defense Platform provides the critical capabilities necessary to protect a hybrid environment, integrating endpoint, identity, network, and data security. The following sections will describe how Symantec solutions can help secure cloud applications and environments, so organizations can experience all the advantages of the cloud while mitigating security risks.

## Securing the Cloud

While the cloud enables new levels of business productivity and agility, maintaining security and compliance remains paramount. These are two primary considerations for customers adopting the cloud with an ever-evolving threat landscape and an expanding attack surface due to enterprises now needing security within their datacenters and for workloads in the cloud. Organizations should rely on a highly-secure cloud provider (such as AWS or Azure) and then take the appropriate steps to help secure the data and workloads running in their environment.

## Securing the Cloud (con't)

Security and compliance in the cloud present new challenges for security, IT and DevOps teams. Applications in these environments are componentized, preconfigured and based on a library of templates. These applications are dynamic, mobile, orchestrated, and automated. Architectural differences between workloads in the cloud and on-premises infrastructures make it difficult to retrofit on-premises security solutions for public cloud environments. Traditional security solutions may not work well in the cloud, where infrastructure configuration and security policies need to be applied and enforced dynamically and may be based on aggregating traffic at the perimeter for threat detection, rather than building security into a distributed cloud architecture. Additionally, as your IT environment has evolved to include software-defined data centers and networks, the traditional way of approaching administration and management quickly falls apart—mainly because it fails to protect new attack surfaces like cloud provider management consoles and APIs. Cloud provider management consoles and APIs offer elevated access to the critical applications running in these environments. Understanding these differences and implementing security best practices that are optimized for cloud architectures are critical to providing the agility the business needs, while maintaining security.

## Shared Responsibility of Cloud Security

The concept of shared responsibility is a critical success factor for effective cloud security. Cloud security can't be outsourced—it requires collaboration across vendors and customers, and collaboration across security, IT and DevOps teams. There are four foundational principles when rethinking the security of a public cloud platform.

**Democratize Cloud Infrastructure**
When organizations move to the cloud, infrastructure responsibility gets distributed. Security practices need to morph to incorporate this shared responsibility model, where the cloud provider is responsible for securing the underlying infrastructure, while internal IT teams are responsible for how to configure and use the environment, including access controls, workload and storage configuration, user activity monitoring, threat protection, and application and data security.

**Decentralize Security Responsibility**
If moving to a public cloud, more than ever before application owners need to be trained on how to secure their services. It is wise to educate, instrument, and engage application owners that are going to be consuming cloud services, and provide them support from a centralized security model. Risk and compliance team should be engaged to establish requirements for meeting regulatory compliance, and the InfoSec team should be involved to adapt app security and data loss protection strategies to adjust for the cloud platforms.

**Deploy DevSecOps**
DevSecOps is all about how to reengineer your software development lifecycle and how to morph that into a security practice. Security needs to be embedded within whatever software development lifecycle process that you are going to use when migrating to the cloud. Often, this cycle is referred to as continuous integration (CI) and continuous deployment (CD), and integrating your suite of security services into the CI and CD pipeline ensures that security is not an afterthought.

**Address Attack Vectors**
Cloud security isn't just about securing a specific machine or compute engine. It's about securing applications that run in your cloud environment. The entire fabric, ranging from where information is stored, to compute, to different service components and applications that you may consume from the cloud—needs to be addressed in the context of a holistic cloud security approach. Also consider how the cloud fits into your overall organizational security strategy and use of cloud services.

# Securing your Cloud Migration with Symantec Integrated Cyber Defense Platform

For organizations to succeed in their move to the cloud, it's critical to leverage advanced cloud security solutions like those from Symantec that help secure cloud access, cloud infrastructure and cloud applications, providing in-depth visibility and controls to safeguard users, information and workloads across public and private clouds.

## Securing Cloud Access

As the anchor of the Symantec™ Identity and Access Management (IAM) platform, Symantec™ SiteMinder has been the proven leader for over 20 years at managing access to your online resources. SiteMinder is currently deployed at hundreds of sites, verifying more than 750 million identities, protecting thousands of applications, and securing trillions of dollars in transactions. SiteMinder provides seamless single sign-on between cloud and on-premises applications, and is further enhanced through integration with Symantec™ VIP, a cloud-based service that provides multifactor credentials and contextual risk analysis where stronger authentication mechanisms are needed. In the cloud, where a traditional perimeter does not exist, SiteMinder and VIP fill the gap by helping organizations adopt cloud-based applications while maintaining proper risk management and compliance measures to help protect data and follow regulations.

Additionally, our IAM platform, starting with SiteMinder and VIP, is transforming in three key areas:

- **Convenience:** Leveraging passwordless authentication to increase user convenience and adoption to grow your business and optimize productivity.
- **Security:** Integrating advanced analytics and Symantec™ Global Threat Intelligence Network to enable just-in-time access to let in legitimate users while preventing unauthorized access.
- **Velocity:** Creating microservices so developers can easily embed IAM capabilities into apps and DevOps tool chains to increase security without impacting the speed the business needs to compete.

Furthermore, SiteMinder can be enhanced through integration and implementation of Symantec™ Secure Access Cloud. Cloud-delivered Secure Access Cloud manages granular access to enterprise applications in IaaS and PaaS environments or on-premises data centers. This zero trust network access solution eliminates the complexity and security limitations of traditional remote access tools, such as VPNs, and streamlines digital transformation with a simple, secure, and scalable application access. Also known as a Software Defined Perimeter solution, it creates a safe, temporary connection between the user's device and the requested application, and then monitors and logs every operation, creating a detailed audit trail. The solution is agentless and enables the definition of granular access control policies and controls based on user identity.

## Securing Cloud Communications

The traditional approach to enterprise security has been rendered obsolete by a perfect storm of mobile users, remote offices and home working, cloud apps, compliance obligations and evolving security threats. For example, the vast majority of malware threats are delivered by email (Verizon, Data Breach Investigations Report, 2020, p18), and email is a key mechanism in taking users to malicious Web pages for phishing, ransomware and business email compromise attacks.

There are two important elements of security to consider. The first is how to provide secure and compliant access to the Web, and the second relates to securing email and corresponding Web page access.

Providing Web connectivity that requires traffic to be backhauled to an enterprise datacenter to enforce security and policies is no longer effective. Network and Security teams need solutions that protect a remote workforce that needs to be connected around the clock and from any location. At the same time, they need a seamless and secure solution that improves the user experience and reduces the cost of backhauling. Symantec™ Web Security Service is a comprehensive cloud-delivered secure web gateway built upon an advanced proxy architecture. It provides superior security for data, apps and users—wherever they are. It offers protection from advanced threats, protection of sensitive information, and compliant cloud application use—all delivered with scale upon a resilient, high performance network backbone.

To protect against advanced email attacks which are delivered through SMTP (a different channel from most Internet Activity), dedicated email threat and data protection capabilities are needed. Email threats have evolved; no longer is traditional spam and anti-malware detection effective. With the rise of ransomware, phishing and business email compromise fraud, sophisticated detection, prevention and risk avoidance methods are needed. Symantec™ Email Security protects against advanced threats, risky URLs and impersonated email. Web isolation technology allows uncategorized or risky webpages to be opened in a secure, disposable container, stopping Web-delivered malware, or phishing sites from impacting users. In addition, email encryption that integrates with Symantec™ DLP extends an organization's data protection policies to the email channel.

### Securing Cloud Infrastructure

Most cloud infrastructure puts strong safeguards in place to help protect customer privacy. All data is stored in highly secure data centers, and that security scales with your cloud usage. No matter the size of an organization, the infrastructure is designed to help keep data safe.

Symantec solutions for securing the cloud infrastructure provide organizations with a comprehensive view into who is using the cloud and how they are using it. By deploying Symantec™ CloudSOC CASB, Symantec™ Cloud Workload Protection and Symantec™ Cloud Workload Assurance, organizations can help protect their cloud environments from misconfigurations, misuse, attacks, threats and data loss.

Additionally, Symantec™ PAM Server Control can help to harden the underlying operating systems within the containers running in cloud environments. These agents protect mission-critical servers with powerful, fine-grained security controls over system-level access and privileged user actions. They can protect and monitor files, folders, processes, registries, and connections to the Docker daemon. These agents can also manage who is allowed to run docker commands on a host.

Together, these solutions automate security for DevOps teams by embedding it into the front-end of the development process.

### Securing Cloud Applications

Symantec CloudSOC CASB empowers organizations to confidently enable cloud applications and services while helping them stay safe, secure and compliant. CloudSOC enables rapid detection and response to security issues for cloud apps and infrastructure all in one platform. CloudSOC can protect sanctioned and unsanctioned use of the cloud platform within your organization by:

- Monitoring, logging, and analyzing user and admin activity
- Enforcing access controls to prevent misconfigurations
- Detecting and remediating risky exposures in different cloud instances
- Defending cloud storage from advanced malware and APTs
- Detecting compromised accounts with user behavior analytics
- Detecting and restricting misuse and shadow cloud instances

### Securing Cloud Workloads

Symantec Cloud Workload Protection automates security for cloud workloads, enabling business agility, risk reduction, and cost savings for organizations, while easing DevOps and administrative burdens. Rapid discovery, visibility, and elastic protection of cloud workloads enable automated security policy enforcement to help protect applications from unknown exploits.

Cloud-native integration allows DevOps to build security directly into application deployment workflows, while support for Chef and Puppet automates configuration, provisioning, and patching. Access to the Symantec Global Intelligence Network helps protect workloads against the latest global attacks and vulnerabilities, providing peace of mind for large enterprises, mid-market companies and born-in-the-cloud businesses.

Organizations migrating workloads to the cloud benefit from:

- Visibility and control of cloud workloads
- Elastic security for their dynamic cloud infrastructure
- Mitigation of risk associated with public cloud adoption

In addition, with potentially thousands of cloud resources deployed across multiple regions and multiple clouds, Symantec Cloud Workload Assurance provides visibility into cloud environments, assessment of cloud security posture and enforcement of security and compliance policies. Organizations can also have visibility and control of the cloud management plane, which is used to manage and configure cloud resources such as launching virtual instances or configuring virtual networks. The solution continuously monitors a cloud environment for resource misconfigurations that can expose data to the public internet. It extends the ability to resolve issues quickly with easy-to-follow, guided remediation steps developed by security analysts and compliance experts. Finally, it generates compliance reports with a single click, while eliminating the taxing process of collecting evidence in spreadsheets.

**Securing Cloud Management Console and APIs**
Privileged user accounts are an organization's most valuable assets—and the most likely to be exploited by external hackers or insider threats. One compromised privileged account can cause irreparable damage to infrastructure, intellectual property and brand. What's more, the attack surface is expanding as with the migration to virtualized and cloud environments. In them users with access to the cloud management console have an unlimited ability to start, stop, copy, or destroy applications or data running in the cloud. Furthermore, as organizations adopt DevOps, these credentials are often being embedded into automation tools, and unfortunately, a single set of credentials is often used for all cloud management APIs across all automation initiatives, creating a single point for hackers to compromise.

Symantec PAM enhances the cloud platform's native security capabilities and adds fine-grained access control to the cloud environments. Specifically, Symantec PAM can:

- Automatically discover and protect cloud instances. Automatically establish and enforce policies across dynamic cloud resources by adding policy protections and access permissions in real time, as virtual instances are created.
- Enforce granular separation of duties for some management interfaces. Track or block privileged user activity at the command-level granularity for both manual and programmatic management by assigning users personal credentials and permissions, without rewriting automation scripts that use shared administrative privileges.
- Monitor, react and record everything. Log events, generate alerts and warnings, or even terminate sessions. Capture continuous, tamper-proof evidence logging and video recording of administrative sessions for all cloud management activity, including calls to and from the cloud management APIs.
- Manage privileged user credentials and simplify with single sign-on. Vault cloud platform credentials in an encrypted vault, and make these credentials available to DevOps tools to enable secure automation without embedding credentials.

Additionally, Symantec PAM is also available as a cloud instance.

## Summary

Moving to the cloud is liberating. But security in public and private clouds can be difficult and the pitfalls of making a hasty move to the cloud are many. Symantec can significantly minimize this risk with a series of integrated security solutions that help secure cloud access, cloud infrastructure, cloud applications and workloads, and cloud management consoles, providing in-depth visibility and controls to safeguard users, information and workloads across public and private clouds.

To learn more, visit: broadcom.com/products/cyber-security

Symantec™
A Division of Broadcom

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


SED-cloud-migr-SB100 December 10, 2020