SOLUTION BRIEF

Managed Cloud Defense

Most complete, integrated cloud IaaS and SaaS security monitoring service

At A Glance

Security Monitoring Expertise for the Cloud

- Security monitoring services 24 hours a day, 7 days a week
- Threat correlation across multiple clouds
- Integrated threat intelligence from the world's largest civilian threat database
- Remote incident investigation, containment, and threat hunting
- Real-time guidance from trained cloud cyber warriors

Introduction

The Cloud Generation has ushered in a complicated, fast-changing, and—to many security professionals—an unfamiliar security scenario. Switching to cloud apps and infrastructures means you're now facing a host of new challenges. These include an inability to see into workloads; an overburdened staff; disparate security policies and tools; a growing vulnerability to malicious attacks; and massive traffic to monitor, analyze, and protect.

How can you overcome these challenges? The answer: with a broad, deep, and unified view into all threats; native support for cloud apps and services; round-the-clock monitoring capabilities; cyber warrior expertise; far and wide threat intelligence; advanced analytics; and real-time detection and response. Welcome to Symantec Managed Cloud Defense.

What the Digital Transformation Means for Data Security

As businesses deliver a growing number of assets via IaaS and SaaS (infrastructure as a service and software as a service, respectively), the security tools and skills that worked for on-premises protection become less relevant. Two other factors are likely further complicating your organizations' cloud security efforts. One is the difficulty managing multiple clouds and vendors (a majority of organizations using public cloud infrastructures rely on multiple service providers). Another is the transformation in DevOps processes, which are being redefined to manage infrastructure in support of business agility.

Eyes Wide Open: Confronting the Challenges to Cloud Security

Securing the cloud environment requires a new approach—here's why.

Lack of visibility: When you use public clouds, your visibility into cloud workloads and cloud-resident data is diminished.

Lack of cloud security expertise: Cloud security requires cloud-specific skills and, often, additional trained staff. In fact, more than one-third of security decision-makers say lack of skilled staff counts as one of their biggest challenges.[1]

[1] Forrester, Data Global Business Technographics Survey, 2018

Ask Yourself...

- Can you maintain a consistent security posture across disparate environments?
- Does your organization have the skills needed to secure your cloud environment?
- Are you able to fully analyze, prioritize, and address all the alerts you receive?
- Are you able to address new vectors created by new DevOps processes in the cloud?
- Can you investigate incidents and actively hunt for emerging threats in the cloud?

Disparate security policies: Visibility suffers further, and security gaps appear, when you use multiple cloud infrastructures and tools. Maintaining a consistent security posture across disparate elements, including on-premises systems, is one of cyber security's biggest challenges. This brings varying levels of security and outputs that need to be analyzed and addressed.

Increased vulnerability: Simply put, your organization had less to worry about when all workloads had safe harbor 'inside the perimeter.' IaaS and SaaS cloud infrastructures and apps are more vulnerable to malicious activity and, since relatively few organizations have the capability to hunt threats in the cloud, you're constantly on the defensive.

DevOps data exposure: Fast-changing DevOps methods open new vectors to attack. For example, DevOps processes may result in improperly configured storage containers, which can leave critical data exposed and the lateral movement of malware undetected.

Threat overload: Operating in the cloud triggers a vast array of new incidents. You need additional resources (staff, tools, etc.) to investigate, analyze, prioritize, and respond to this unending wave of alerts.

What Cloud Threat Protection Looks Like

Many current IaaS and SaaS security and compliance tools do not show a full picture of your security environment. Only a completely integrated, cloud security and monitoring solution can meet the security challenges of the Cloud Generation.

Visibility: A broad, deep, and unified view into all threats across multiple clouds and on-premises environments.

Expertise: People with the right skills and focus to monitor and respond to threats—globally, 24x7.

Automation: Internal and external threat data automatically correlated across multiple platforms.

Intelligence: Threat intelligence to accurately predict, identify, and validate threats.

Speed: Real-time investigation and threat hunting to detect, and respond to, emerging and stealth attacks.

Managed Cloud Defense from Symantec Managed Security Services

Managed Cloud Defense offers the most complete and best integrated security monitoring services available for SaaS and IaaS apps and infrastructures. These services, provided by Symantec Managed Security Services (MSS) experts, deliver 24x7 monitoring with threat hunting, threat correlation across multiple clouds, remote incident investigation and prioritization, and real-time guidance from trained cloud cyber warriors across six global security operations centers (SOCs).

Visibility—Deeply inspect cloud infrastructure and platforms.

- Collects and analyzes data from key cloud native services offered by Amazon Web Services and Azure (without reliance on other tools)
- Monitors the Cloud Workload Protection platform

Survey Says...

As reported in *Forrester, Data Global Business Technographics Survey, 2018*, security leaders have the following concerns.

64% say it's a top priority to take advantage of a cloud-based security services provider within the next 12 months.

37% say they count lack of skilled staff as one of their biggest security challenges.

57% say they're worried about risks that can be introduced into their environments when using IaaS or SaaS.

46% say they do not have enough tools, or the right tools, to enforce security policies related to DevOps.

61% say it's a top priority to improve incident response and forensics capabilities within the next 12 months.

Expertise—Symantec cloud cyber warriors are on the job around the clock, providing:

- Incident validation
- Guidance on handling and prioritizing critical incidents
- Customer-designated teams based on industry and region
- Customized alert severity and incident escalation
- Ongoing reporting on incidents, risk posture, regulatory compliance, and more

Integrated Security Processes—Eliminate security gaps and silos with unified security monitoring across the entire IT estate.

- Monitor Symantec and third-party SaaS and IaaS security tools for threats and Shadow IT
- Monitor Microsoft Office 365 Cloud App Security
- Consolidate multiple findings and correlate them with data from other security tools across cloud and on-premises environments

DevOps Process Management—Monitor Amazon Simple Storage Service (S3) permissions.

- Protect critical data storage
- Identify unsafe configurations

Threat Intelligence—Based on correlated threat data from the Symantec Global Intelligence Network (GIN), the world's largest civilian threat database.

- Threat intelligence correlated with data from multiple clouds
- Analysis that identifies true threats and accelerates incident handling
- Analyst-curated threat research that provides perspective and context

Rapid Threat Response—The leader in cloud security delivers:

- Investigation of suspicious threat activity in virtualized environments
- Automated threat hunting to get ahead of emerging threats
- Containment via endpoint protection deployed in the cloud
- Rapid incident response

Use Case Example

Consider this real-world (and all too common) development.

The scenario: An attacker accesses a corporate, cloud-hosted application.

Managed Cloud Defense response:

- The client's CASB provides an alert to MSS and notes a brute force login attempt
- Incident data is fed into MSS analytic engines and correlated with data from the client's other security devices and with the Symantec GIN
- MSS validates the incident and determines that there were multiple applications where access was attempted by the same attacker
- The incident is presented to the designated MSS cyber warrior team
- A remote investigation is initiated into the cloud instance and forensics are analyzed to determine if there is malicious activity
- If applicable, the MSS analyst will perform system containment

- The designated MSS analyst contacts the client and provides:
  - Information on the initially compromised endpoint including the IP address and hostname
  - The date and time that the attacker performed key steps
  - Details for any unusual and anomalous activity on the network and endpoints
  - Potential attack attribution and remediation guidance
  - Visibility and context to help understand the attack timeline and how to minimize the impact to your business
  - Information and artifacts to incident responders, if required, for deeper investigation, large scale containment, and threat eradication

Summary

When it comes to cloud security, you have too few resources, too much to do, and the stakes are too high.

Symantec Managed Cloud Defense takes on your organization's monitoring vigilance for cloud and on-premises security, freeing you to focus on other priorities.

As your organization increasingly moves its operations to the cloud, you may struggle with a lack of visibility and new vulnerabilities and threats. Improve your response with visibility into workloads, additional cloud security expertise, proven security policies and processes that close security gaps, and a dedicated team of cyber warriors who understand your industry and the threat activity in your region.

Symantec Managed Cloud Defense takes care of your full cloud and on-premises security monitoring picture, ensuring your organization detects, prioritizes, and deters critical threats and advanced attacks—24 hours a day, every day.

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 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

19B186186_SB_MSS_MANAGED_CLOUD_EN