SOLUTION BRIEF

THREAT PREVENTION INNOVATIONS

- **Adaptive Protection**: Intelligent, automated attack surface reduction without disruption of normal business operations
- **Application Control**: Discovery and control of risky applications, including detailed risk assessments and smart recommendations for administrators
- **Active Directory Security**: Protection against initial access, privilege escalation, and credential theft used by attackers for lateral movement leveraging AI-driven obfuscation of Active Directory query results
- **Threat Hunter**: Expert threat hunters apply machine learning analytics and expert analysis to expose and notify customers of the early signs of stealth attacks that otherwise would evade detection
- **Dedicated IP Addresses**: Prevent the use of unassigned IP addresses by threat actors who want to gain unauthorized access to sensitive applications and conduct malicious activities
- **ZTNA Threat Prevention**: Cloud-native, multi-layered threat inspection and detection for zero trust network access (ZTNA) connections
- **Mobile Threat Defense**: Proactive protection for mobile devices from malware, network threats, and application or OS vulnerability exploits

Symantec by Broadcom

The Future of Threat Prevention and Data Protection

Mission-Critical Innovations Delivered Today

Overview

The attack surface of organizations continues to increase as the adoption of cloud applications, including generative AI increases. In addition, pressures to provide remote access to users continues despite post-pandemic hybrid work trends. All of these issues around digital transformation have also increased the pressure to meet new and existing regulatory requirements across multiple jurisdictions. Organizations must address all of these challenges in an environment of economic uncertainty and geopolitical tensions.

Figure 1: Modern Challenges for Global Enterprises

Broadcom understands the needs of global organizations and how the evolving threat landscape requires firms to continuously improve their threat prevention and data protection, all while simplifying IT and security staff operations. These two sets of capabilities are key to the success of enterprises that require the highest levels of security for important data assets. In addition, global organizations must demonstrate that regulated data meets multiple compliance standards requiring threat prevention and data protection that extends everywhere data resides.

Symantec® Enterprise Cloud delivers advanced threat and sensitive data detection across endpoint, email, web traffic, and cloud applications. This solution allows customers to discover and block targeted attacks and data breaches that would otherwise go undetected.

Our solution employs a modern approach that keeps our customers ahead of threats by protecting what attackers target and enterprises value most, critical data assets, and the devices and networks used to access this information.

This document describes the current Symantec software threat prevention and data protection innovations. These innovations are critical for customers today, and Symantec software innovations will continue to address evolving threats in the future.

DATA PROTECTION INNOVATIONS

- **Generative AI Protection**: Provide guardrails for users while enabling a productive and lower risk work environment
- **ZTNA Data Protection**: Enforce Data Loss Prevention (DLP) policies against private resources and corporate assets in the cloud
- **Risk-Aware Policies**: Create greater context for DLP policies so access and control can be adapted to users with higher risk scores
- **Fast File Scanning**: Dramatic increases in the scan rates for large data repositories ensures that static data can be scanned regularly with new and updated DLP policies
- **Leading Edge Data Detection**: New detection methods increase detection accuracy and reduce the rate of false positives

Customer-Focused Threat Prevention Innovations

Symantec software innovations are reshaping *threat prevention* strategies by driving a proactive approach to combat the modern tactics and techniques that attackers use today. Symantec Enterprise Cloud uses advanced artificial intelligence and machine learning to predict where the next attack might occur and block attacks before they are executed. Our threat prevention solution also provides insights into areas where attack vectors can be closed, eliminating these options from an attacker's tool chest. The combined effect of a reduced attack surface, enterprise-grade security controls, and our foundational Global Intelligence Network ensures that threat prevention is implemented with the highest levels of efficacy.

Key innovations for *threat prevention* within Symantec Enterprise Cloud include the following features:

- **Adaptive Protection** – Reduces the attack surface by blocking trusted application behaviors often used by attackers to execute living-off-the-land attacks. Attackers are frequently successful when they use an organization's known applications to execute an attack because they can hide their activities. This analytic technology can customize blocking adaptations based on its ability to continuously learn which apps, tools, and OS behaviors are used in the customer's environment—and which are not used. Adaptive Protection automatically restricts unused behaviors to reduce the attack surface and protect the organization. This feature is transformative in blocking threats from entering the environment without affecting normal business operations.
- **Application Control** – Discovers installed applications and their vulnerabilities, reputation and prevalence, and generates a risk score for addressing the security concerns associated with the broad use of *shadow IT*. Delivered with the risk score is a risk assessment, actionable insights, and smart recommendations for blocking or allowing an application to run. With Application Control, organizations can specify the apps they allow, and block the apps that are dangerous and unnecessary.
- **Active Directory Security** – Automatically learns about an organization's entire Active Directory structure and uses obfuscation to prevent attackers from stealing credentials and moving laterally within the organization. With obfuscation, the attacker gives itself away while interacting with fake assets or attempting the use of domain administrator credentials. It only takes one compromised endpoint connected to a corporate domain to jeopardize the entire organization. Active Directory Security provides critical protection from the endpoint to stop attackers as early as possible, on their first move.
- **Threat Hunter** – Assists security operations centers (SOCs) by combining Symantec's expert analyst research with advanced machine learning and global threat intelligence to provide alerts, insights, and guidance to stop attacks. Threat Hunter empowers security teams to quickly respond to incidents and stop breaches by bringing together three key elements: global and organizational data, artificial intelligence for data processing, and human threat experts and researchers to identify reconnaissance attempts before the breach has manifested.

Customer-Focused Threat Prevention Innovations (cont.)

- **Dedicated IP Addresses** – Symantec Enterprise Cloud has added Dedicated IP Addresses to our service. Some cloud-hosted third-party applications and services require a user to come from an IP address that is specifically identified as the customer's IP address. This feature reduces that attack surface, and it prevents actors from using unassigned IP addresses to gain unauthorized access to sensitive applications and conduct malicious activities.
- **ZTNA Threat Prevention** – Sophisticated attacks come in many forms. All traffic, even traffic traversing a secure ZTNA connection, should receive thorough interrogation to prevent malicious activity. Symantec utilizes cloud-native, multi-layered threat inspection and detection to reduce the number of alerts that SOC and incident response teams need to address. Symantec Enterprise Cloud provides the following services:
  - Analyzes unknown files through advanced machine learning and static code file analysis
  - Scans content with dual anti-malware engines for greater detection accuracy
  - Detonates unknown files through sophisticated sandboxing
  - Provides a single entry point for all threat scanning across the entire Symantec portfolio
  - Leverages Symantec File Reputation services to block known threats
- **Mobile Threat Defense** – Provides predictive technology in a layered approach that leverages crowd-sourced threat intelligence, in addition to device and server-based analysis, to proactively protect mobile devices from malware, network threats, and application or OS vulnerability exploits. Mobile Threat Defense delivers real-time visibility over the threats and attacks originating from public Wi-Fi and mobile networks, OS or app vulnerability exploits, malicious apps, and user behavior that might compromise company-owned and bring your own devices (BYODs). Symantec's multilevel approach provides mobile security to outpace well-funded, highly socialized hackers.

Customer-Focused Data Protection Innovations

Digital transformation has created myriad Data Protection challenges not the least of which is the emergence of widely available generative AI applications. Legacy solutions that do not address cloud-hybrid environments create risks for customers engaged in the cloud migration of numerous business and in-house applications, even while some business systems and processes remain within an enterprise. With data spread across cloud and on-premises environments, customers seek to simplify their data protection approaches to stop data leaks and demonstrate compliance with global regulations.

Global enterprises want to streamline operations with uniform data protection policies across all control channels (endpoint, network, cloud, and email). They also need adaptive and contextual technologies that give better insight into risk mitigation and data loss prevention. Symantec Enterprise Cloud permits customers to apply a single, risk-aware policy across multiple channels.

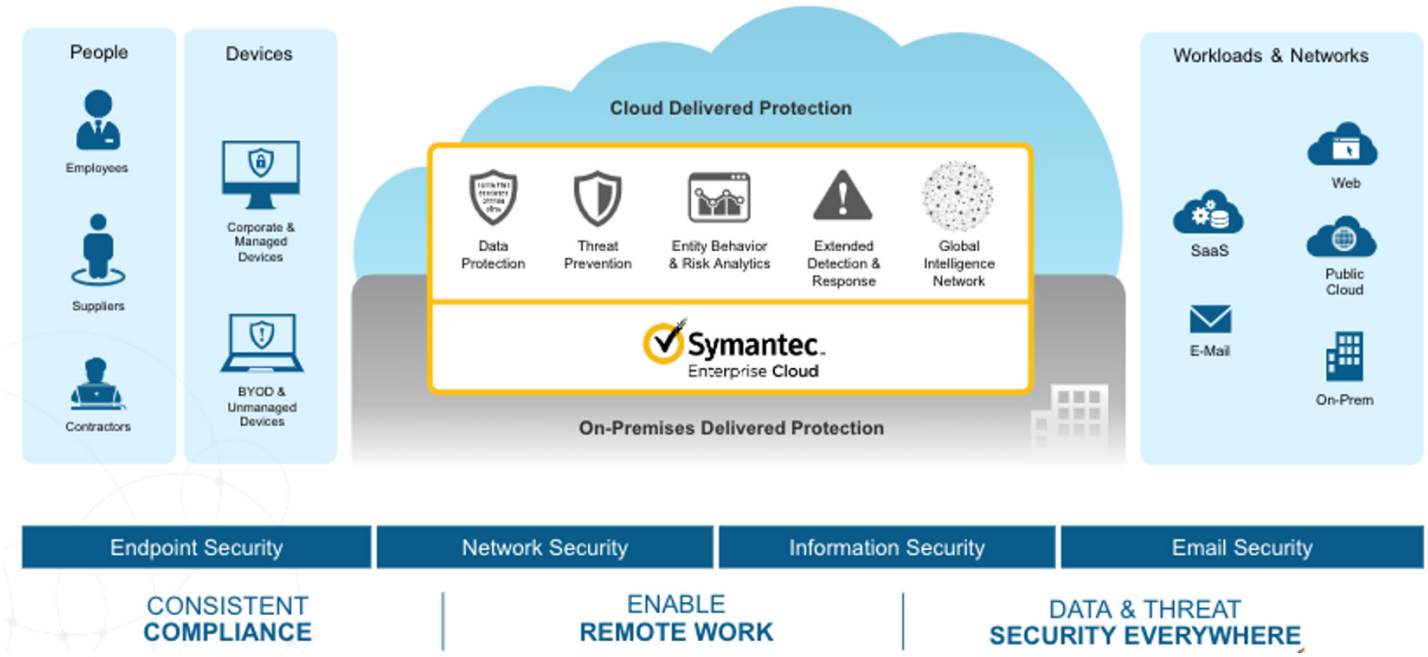
Broadcom continually invests in Symantec *data protection* innovations, including the following features:

- **Generative AI Protection** – Employees can easily expose sensitive and proprietary information when leveraging generative AI applications. As generative AI use increases, enterprises need to assess the risk of this category of applications and ensure a safe environment to understand how users leverage generative AI. Symantec's innovative approach to the discovery, analysis, monitoring, and control of these applications means each enterprise can manage the adoption of generative AI applications that conforms to their risk appetite.
- **ZTNA Data Protection** – Symantec Enterprise Cloud merges ZTNA and DLP capabilities. DLP policies can now be applied to private resources and corporate assets in the cloud to avoid unintentional or malicious data exfiltration, and ensure that your organization meets compliance and data privacy regulations. DLP enforces cloud storage, sharing, and access policies for HIPAA, PCI, PII, and other sensitive data. As organizations look to protect their assets in the cloud, they can ensure that protection with the DLP integration, their security and risk teams can meet those compliance obligations. Moreover, with the advantage of the DLP single-policy engine, you can extend the same DLP policies that you use in on-premises, cloud, and web environments. You can apply the policies to your corporate assets through a secure ZTNA connection to ensure that data is protected and does not leave the organization.

Customer-Focused Data Protection Innovations (cont.)

- **Risk-Aware Policies** – Customers seeking Adaptive DLP can create DLP policies that take user risk scores to define access and protection controls. For example, high-risk users might be granted read-only access with blocked print and copy functionality, whereas low-risk users get full access.
- **Fast File Scanning** – Compliance requirements mandate that organizations scan data repositories regularly to ensure that data audits are up to date. With organizations now managing large data repositories containing petabytes of data, the pressure to completely scan these repositories in a specific time window is high. Customers can now ensure that static data is regularly rescanned against updated DLP policies. Delivering this capability in Symantec DLP was the result of considerable engineering innovation for our grid scanning technology.
- **Leading Edge Data Detection** – Symantec DLP can further reduce the consequences of false detection with the following new features:
  - **Structured Data Matching** – Symantec DLP 16 introduces a new data discovery technique called Structured Data Matching. Using the insight that many collections of sensitive data (for example, PII, PCI, and PHI) are organized in tabular formats, Symantec DLP scans for data in this form before the deeper inspection to identify sensitive data. This feature not only helps customers find sensitive data accurately, it also simplifies the workflows and policy creation loads on DLP administrators.
  - **OCR and Form Recognition** – Symantec DLP utilizes OCR to find sensitive data in images. It can also identify *forms* and scan for areas that contain sensitive images.
  - **Exact Data Matching and Proximity Matching** – Symantec DLP includes highly specialized data discovery methods such as Exact Data Matching and Proximity Matching. These features increase the accuracy of detection, and the lower incidence of false positive or false negative alerts alleviates the workload on already stretched information protection teams.

Figure 2: Symantec Enterprise Cloud – A Modern Solution for Threat Prevention, Data Protection, and More



Conclusion

Symantec software products continue to lead the way in the two most critical areas of security capabilities: threat prevention and data protection. At their core, these innovations delivered in Symantec Enterprise Cloud give organizations the flexibility to adjust their threat prevention and data protection deployments for maximum efficiency and efficacy.

Symantec researchers have decades of expertise and global intelligence to decompose attack methods and model how motivated attackers use legitimate and malicious tools to exfiltrate data. Symantec Enterprise Cloud leverages this learning by delivering layered capabilities that allow our customers to secure their data assets with minimal impact on their users or business processes.

Broadcom has delivered Symantec threat prevention and data protection capabilities at an accelerated pace. Unlike other cybersecurity organizations, we focus on the needs of large and complex organizations with strict security and compliance requirements. Our modern approach, using leading-edge innovations, means streamlined security operations and continual improvement in an adopting organization's risk posture.

BROADCOM®
connecting everything®

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

FTP-DP-SB100 June 13, 2023