SOLUTION BRIEF

CHALLENGE

Organizations must modernize their IT infrastructure to compete and operate effectively. However, these initiatives have also expanded the attack surface, exposing security gaps and amplifying the risk of data breaches.

OPPORTUNITY

A holistic approach that integrates traditional and modern security technologies can effectively safeguard customer and corporate data throughout its entire lifecycle.

BENEFITS

A comprehensive data protection strategy will assist companies in complying with privacy laws and regulations, thereby avoiding fines and qualifying for Safe Harbor.

Symantec by Broadcom

Safeguarding Data throughout Its Lifecycle

Overview

Technology has long played a pivotal role in business strategy and growth, but we are currently in the early stages of the Fourth Industrial Revolution—the digital economy. In terms of scale, scope, and complexity, this revolution is unlike anything we have previously experienced. The digital economy is global, responsive, customer-focused, and technology-driven—with data at the center of it all.

Deriving value from data is the goal of the digital revolution, but monetizing this data requires not only continually evolving in today's digital landscape but also earning trust by proving yourself a good custodian of this data. However, the IT modernization initiatives required to enable organizations to compete have also expanded the attack surface, exposing security gaps and amplifying the risk.

The purpose of this brief is to highlight the security technologies that can safeguard your data throughout its entire lifecycle.

The Data Lifecycle

Data drives business, and every year, exponentially more of it gets created and needs to be stored by the enterprise. To capture the full potential of this data, it must be accessed, used, and shared. However, it also needs to be available and protected. Once the organization is finished with it, or if the customer requests to be forgotten, the data needs to be destroyed.

Simplified Data Lifecycle

The dilemma facing organizations is striking the appropriate balance between availability and security because any data that holds value to the business unfortunately also has currency on the open market, making it a target for external hackers. They want the data and will exploit any security gaps to gain access to it.

The following sections will highlight the best practices for safeguarding data throughout its entire lifecycle, focusing on the two main modes of existence: data at rest and data in motion.

"I ROB BANKS BECAUSE THAT'S WHERE THE MONEY IS."

WILLIE SUTTON, BANK ROBBER

Protecting Data at Rest

It should be no surprise to anyone that data is most vulnerable when it is at rest—just sitting around, doing nothing. File share servers, directories, and databases are all prime targets for hackers because that is where the data is kept. Safeguarding the data that resides in these systems requires a layered defense that consists of the following steps:

- Data discovery, classification, and consolidation
- Data encryption
- Zero Trust access enforcement
- Repository maintenance and hardening

The following sections examine each of these steps in detail.

Data Discovery, Classification, and Consolidation.

The first step in protecting data at rest is knowing where the data is and what is important! Data is a living thing, and it can spread throughout an organization faster than a virus. To address this challenge, organizations need to implement Data Loss Prevention (DLP) technology to gain comprehensive discovery, monitoring, and protection capabilities. Once found, a DLP solution can also classify the data to prioritize protection efforts.

At this point, organizations can decide where and when to consolidate data into fewer repositories. It is common for new applications to deploy their user stores when implemented. However, each of these directories needs protection, and many often store the same data, creating more opportunities for misconfiguration or over-entitlement, putting the data at risk. A better approach is to consolidate this replicated data onto an enterprise backbone directory service, delivering superior availability, reliability, scalability, and performance.

Symantec® DLP applies a single set of policies across all components and integrations to protect data. This includes data stored in both Microsoft and non-Microsoft environments, applications, and files, covering structured data and images. Designed for and widely adopted by large enterprises, Symantec DLP offers a comprehensive risk-based solution suitable for any organization prioritizing data protection. Furthermore, Symantec Directory is a carrier-grade backbone directory providing a standards-based distribution and replication model, ensuring superior performance and reliability. Deployed in some of the largest and most demanding environments, it supports billions of transactions daily with minimal infrastructure and personnel resources, resulting in a lower cost of ownership. It is the ideal solution for organizations looking to consolidate multiple directories into one to reduce the threat surface.

Data Encryption

The easiest way to protect your data is also the last line of defense. The third tenet of Zero Trust is to assume breach. Despite all the security mechanisms and technologies you have deployed to protect your data, the adversaries may have gained access. What now?

A COMPREHENSIVE DATA PROTECTION STRATEGY ASSISTS WITH DATA PRIVACY COMPLIANCE AND HELPS QUALIFY FOR SAFE HARBOR.

For most organizations today, the primary motivation behind deploying an encryption solution is to protect customer privacy and mitigate the impact of a potential data breach. In today's mobile workforce, laptops and removable media devices capable of storing gigabytes of data provide the freedom to work from anywhere. However, with this freedom comes an increased risk of lost or stolen devices leading to a costly data breach. This risk is further amplified by cloud sync and share services, allowing employees to unknowingly carry a large amount of sensitive information.

Additionally, shared file servers have become central collaborative tools in today's workplace, and many companies now offer cloud-based file sharing, enabling users to access shared information anywhere. Without proper protection, this shared data becomes an easy target for those looking to maliciously gain sensitive information and a potential route for sensitive data to accidentally leak. A comprehensive encryption solution can address both scenarios, protecting external endpoints, internal servers, and third-party cloud environments.

The new Symantec PGP® Encryption Suite provides flexible data-at-rest protection through two product offerings. Symantec Endpoint Encryption combines strong full-disk and removable media encryption with an intuitive central management platform to protect sensitive data from loss or theft. It also helps administrators prove that a device was encrypted should it go missing. Symantec PGP File Share Encryption extends file server access controls to include robust end-to-end encryption. Administrators can set encryption policies for content such as documents, spreadsheets, presentations, videos, and audio. This content is automatically encrypted when created within selected applications or sent to specific folders. Once encrypted, files and folders can be moved without compromising their encrypted status, ensuring that only authorized users have access to sensitive data. Furthermore, the solution also provides secure archiving for sensitive data that must be kept to address regulatory compliance, and then secure deletion to fully destroy data when it is no longer needed.

Zero Trust Access Enforcement

So, now you have found the data that needs to be protected, consolidated it where possible, and encrypted it. What is next? Well, do you want to be able to use this data as part of your business operations? If so, the next step is to address access to the data.

Although the adoption of Zero Trust may require many different security tools and technologies, a modern identity fabric is the glue that brings these disparate systems together. In fact, two of the primary Zero Trust tenets are identity-based: verify the identity of every user and device requesting access, and enforce least privileged access. Building an identity fabric begins with a modern authentication service.

Effectively distinguishing legitimate users from fraudulent ones is a crucial step in enforcing access policy controls. However, verifying someone's email address or identity is just the baseline. Implementing current security protocols and standards is vital, and the service must adapt as security profiles evolve. A modern authentication service accelerates business operations by providing unified, frictionless access across diverse security layers within an organization, facilitating the seamless promotion of new applications and services.

SAFEGUARDING YOUR DATA MEANS ALSO SECURING THE SERVERS HOSTING THAT DATA.

Symantec VIP is a modern cloud-based multifactor and risk-based authentication service that protects networks and applications by verifying user and device identities, preventing unauthorized access. The service also enables convenient and frictionless two-factor authentication for consumer access to applications, as well as phishing-resistant credentials to support the recent Federal mandate, providing that extra layer of security against account takeover. Additionally, the service now offers a new deployment option. Leveraging a cloud-native architecture, the VIP Authentication Hub provides primary and secondary authentication, policy orchestration to control the authentication journey, and complete control over the solution. This enables organizations to strike the right balance between security and convenience, safeguarding resources against unauthorized access and aligning with Zero Trust initiatives.

Repository Maintenance and Hardening

The final step in protecting data at rest is to turn your attention to the endpoints and servers hosting this data. External attackers have learned to target end users and their devices, with the most successful attacks exploiting known vulnerabilities simply because endpoints were not properly configured or patched. These weaknesses exist because many organizations lack real-time visibility into the state and usage of their own endpoints and software.

Furthermore, protecting an organization's most sensitive electronic assets, such as customer databases, hospital patient records, or proprietary information, is challenging. Native operating system capabilities do not provide adequate protection against inadvertent or intentional attacks, nor do they offer reliable auditing of the entire server environment. Operating systems are also inherently incapable of ensuring the integrity of their own controls. All systems have privileged accounts that can change or bypass the system's security controls.

Symantec IT Management Suite enables you to meet this challenge by securely managing devices both inside and outside the perimeter. The solution improves your security posture by providing visibility into the hardware and software in your environment, identifying and remediating vulnerabilities, and ensuring compliance. It also increases productivity by automating the deployment and configuration of hardware and software while minimizing costs and optimizing operational efficiency.

Server hardening can be achieved using Symantec PAM server control agents which deliver the localized, fine-grained access controls required for regulatory compliance and risk management. Using centrally managed task delegation and platform-specific software restrictions, the server control agents provide file, directory, and resource-specific, kernel-level controls, registry protection, and other localized granular controls. This control ensures that high-value assets and resources hosted on critical servers are protected from damages caused either by malicious or accidental insider actions, even when using root or admin accounts.

"HE CAN TRACK A FALCON ON A CLOUDY DAY. HE CAN FIND YOU."

THE PRINCESS BRIDE (1987)

Protecting Data in Motion

Data drives your business, but to capture the full potential of this data, it needs to be accessed, used, and shared. However, when it is, it becomes vulnerable. Organizations may not need to fear hackers with Prince Humperdinck's legendary tracking skills to find their data, but they do need to protect their data while it is in motion. Safeguarding the data in motion needs to address two primary concerns:

- Human error
- Automated processes

The following sections examine each concern in detail.

Human Error

As the shift to a mobile and remote workforce has become the norm for many organizations, the freedom of being able to work from anywhere has created challenges. Collaboration across both internal teams and external business partners is even more critical when people are no longer working side by side. But how do you securely share data without incurring additional risk?

Many cloud-based options have emerged as potential solutions, offering widespread access from any device or location. When this option is used to share data, the new Symantec PGP Encryption Suite discussed previously can be employed to encrypt sensitive data as it is placed within shared folders. However, email also remains a fundamental communication channel for businesses to share data, posing the greatest security vulnerability. A recent study by the Ponemon Institute revealed that within the past year, 60 percent of organizations encountered instances of data loss or unauthorized data transfer because of employee errors in email communication.

The new Symantec PGP Encryption Suite also provides the option to secure email communications. Symantec Desktop Email Encryption is included in the bundle, and it offers automated encryption, decryption, digital signing, and message verification in alignment with centrally managed policies. This encryption process takes place at the client level, ensuring that communications remain secure prior to traversing internal networks or being stored within cloud repositories. For an alternative approach, Broadcom offers Symantec Gateway Email Encryption, which can be licensed separately. This product enables the encryption of messages based on highly customizable encryption rules, eliminating the need for client-side software installation. Furthermore, the combination of Gateway Email Encryption with Symantec Messaging Gateway allows users to harness the synergy of PGP encryption alongside the premier Symantec anti-virus, malware, and spam filtering. This integration serves to bolster the security of email communications, safeguarding against external threats.

DELIVER THE HIGHEST LEVEL OF PROTECTION TO SECURELY EXCHANGE LARGE VOLUMES OF INFORMATION INTERNALLY OR EXTERNALLY

Automated Processes

Automation has become the bedrock of the modern enterprise, aiming to reduce costs and increase agility. However, it does not come without risk. One threat vector occurs during the exchange of large volumes of information between internal systems, cloud-based environments, suppliers, and customers. Data transfer and processing systems lie at the heart of nearly every organization, and traditional file transfer and email protocols have been prone to security breaches because these systems lack built-in security. Additionally, organizations are rapidly undergoing IT modernizations to transform and accelerate their software delivery cycles and application development processes. These initiatives also leverage automation to create dynamic, and often unprotected, environments that are then populated with large amounts of sensitive data. Although these environments may not permanently exist, while they do, they are ripe for attack.

Symantec PGP Command Line delivers the highest level of protection to mitigate data breaches and compliance risks for organizations that need to securely exchange large volumes of information. By embedding command line scripts into an automated process, PGP® Command Line easily integrates with most commercial and home-grown data transfer and processing systems to safeguard data transfers and exchanges with any recipient, regardless of their technical capabilities. The solution is a convenient alternative to network layer encryption because it encrypts the data itself, eliminating the need for hard-to-manage VPNs. PGP® Command Line can also be used to encrypt large volumes of information stored on servers from unauthorized access. This encryption is especially useful for securing data being moved around in a DevOps environment.

Why Broadcom?

- Business Critical: Broadcom provides industry-leading data protection solutions that safeguard data across its entire lifecycle and scale to address the largest and most complex environments.
- Trusted: Broadcom delivers exceptional levels of technical expertise, commitment and solution support to ensure customer success.
- Innovative: Broadcom invests and enhances its software solutions to help organizations modernize, optimize, and protect their hybrid cloud infrastructure.

For more information, please visit broadcom.com/symantec-encryption

BROADCOM®
connecting everything®

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

SGD-TL-SB100 December 19, 2023