SOLUTION BRIEF

CHALLENGE

As organizations accelerate digital transformation, the expanding attack surface and evolving cyber threats make securing sensitive data throughout its lifecycle increasingly complex.

OPPORTUNITY

Implementing a comprehensive data protection strategy—encompassing data discovery, encryption, Zero Trust access, and automated security controls—ensures robust security across on-premises, cloud, and hybrid environments.

BENEFITS

By safeguarding data at rest and in motion, organizations can mitigate breaches, maintain regulatory compliance, and build customer trust, ultimately strengthening their competitive edge in the digital economy.

Safeguarding Data in the Digital Economy

Overview

Technology has long been a cornerstone of business strategy and growth, but the emergence of the Fourth Industrial Revolution—the digital economy—has fundamentally reshaped the landscape. This revolution is global, responsive, customer focused, and technology driven, with data at its core.

While data drives innovation and revenue generation, its value also makes it a prime target for cyber threats. Modernizing IT environments to support digital transformation has expanded the attack surface, increasing security gaps and amplifying risks. This brief highlights critical security technologies that can safeguard data throughout its entire lifecycle.

The Data Lifecycle: Balancing Access and Security

Organizations face a crucial challenge: ensuring data is accessible for business use while securing it against theft. Data must be discovered, classified, stored, accessed, and, when necessary, securely deleted. However, any data with business value also has currency on the dark web, making it a target for cyber criminals.

This brief outlines best practices for protecting data in its two primary states: data at rest and data in motion.

Protect Data at Rest

Understand the Risk

Bank robber Willie Sutton famously said, "I rob banks because that's where the money is." Likewise, cyber criminals target stored data because it represents a lucrative prize. File servers, databases, and repositories are primary attack points, and securing them requires a multilayered defense strategy.

Key Protection Strategies

1. **Data Discovery, Classification, and Consolidation**

   The first step in data protection is knowing what data exists and where it resides. Data spreads rapidly across an organization, making securing difficult to secure without proper tracking. Implementing Data Loss Prevention (DLP) technology enables organizations to discover, monitor, and protect data across their environments.

   Organizations should also consolidate redundant data repositories to reduce risk exposure. Symantec® DLP applies a unified policy framework across various storage environments, including Microsoft and non-Microsoft platforms, while Symantec Directory provides carrier-grade reliability, ensuring better data management and security.

2. Data Encryption

Despite advanced security measures, breaches can still occur. Encryption serves as the last line of defense, ensuring that even if adversaries gain access, they cannot exploit sensitive data.

Symantec PGP® Encryption Suite provides comprehensive encryption solutions, including Symantec Endpoint Encryption for full-disk and removable media security and Symantec PGP File Share Encryption to safeguard shared files. These solutions ensure that sensitive data remains secure, even when transferred or stored across multiple environments.

3. Zero Trust Access Enforcement

A Zero Trust approach mandates continuous verification of user identities and enforcement of least-privileged access.

Symantec VIP Authentication Hub supports multi-factor authentication (MFA) and phishing-resistant credentials to prevent unauthorized access, aligning with Zero Trust principles. This ensures seamless, secure access to data while reducing friction in business operations.

4. Repository Maintenance and Hardening

Endpoints and servers must be hardened to prevent exploitation by cyber criminals. Many successful attacks leverage unpatched vulnerabilities, underscoring the need for continuous system maintenance.

Symantec IT Management Suite enhances security posture by identifying and remediating vulnerabilities while optimizing operational efficiency. Symantec PAM Server Control Agents also provide granular access controls, safeguarding critical assets even against privileged insider threats.

Protect Data in Motion

Understand the Risk

Data moving across networks becomes vulnerable to interception, leakage, and unauthorized access. Organizations must address security risks stemming from human error and automated processes to ensure that sensitive information remains protected in transit.

Key Protection Strategies

1. Prevent Human Error in Data Sharing

The rise of remote work and cloud-based collaboration has increased the risk of accidental data exposure. Email, a fundamental business communication tool, is a primary source of unintentional data breaches.

A Ponemon Institute study found that 60% of organizations experienced data loss due to employee email errors in the past year. Symantec PGP Encryption Suite mitigates this risk through Symantec Desktop Email Encryption, automatically encrypting emails based on policy rules. Symantec Gateway Email Encryption secures communications without requiring client-side installation.

2. Secure Automated Data Transfers

Many enterprises rely on automated processes for data exchange between internal systems, cloud services, suppliers, and customers. However, traditional file transfer protocols often lack robust security features.

Symantec PGP Command Line offers high-level protection for bulk data transfers by embedding encryption scripts into automated workflows. This eliminates the need for complex VPNs while ensuring data remains secure, even within dynamic DevOps environments.

Conclusion

The digital economy has made data an invaluable asset, but it has also increased the complexity of securing it. Organizations must adopt a comprehensive approach to protect data at every stage of its lifecycle. Businesses can enhance security, ensure regulatory compliance, and earn customer trust by leveraging data discovery, encryption, Zero Trust access controls, and secure automation.

The Symantec suite of solutions provides a powerful, integrated defense against evolving cyber threats, enabling enterprises to navigate today's digital landscape confidently.

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

BROADCOM®
connecting everything®

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

SGD-TL-SB101 March 17, 2025