WHITE PAPER

The Role of Enterprise Data Protection in the Zero Trust Security Framework

TABLE OF CONTENTS

Safeguard Critical Assets Across Complex Hybrid Cloud Environments

Traditional enterprise data protection solutions are exclusively designed to secure assets stored in data centers and other on-premises locations. However, the ongoing adoption of hybrid and multi-cloud strategies, rise in remote work, and rapid pace of innovation have created new data security challenges for IT professionals and leadership teams.

In response to these foundational changes to the cybersecurity landscape, organizations across industries are adopting the Zero Trust framework to govern their IT infrastructures. Zero Trust is rooted in a “Never Trust, Always Verify” approach to security, which prompts enterprises to verify every user and device before granting them privileged access to assets and applications.

Today’s IT leaders must ensure end-to-end data monitoring and protection in on-premises and cloud-based environments—even as this data continually passes between users, devices, applications, and storage locations.

Understand the Risks of Distributed Data Storage and Processing

As businesses leverage cloud-based applications and the remote workforce to develop new solutions quickly and meet demand, on-premises security software can no longer protect their sensitive data from ever-evolving cyber risks.

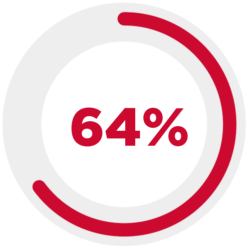
While hybrid and multi-cloud architectures pose endless opportunities for scalability and innovation, they also provide opportunities for cyber attackers. This is because users often operate within several applications simultaneously, transferring data and other resources across systems and devices in rapid succession.

Complexities only increase for remote workforces where some users operate on in-house operating systems while others rely on third-party technology to access confidential data via multiple devices and locations.

Traditional on-premises data security solutions monitor activities in specific data centers, but they do not extend to all of the remote applications needed to support distributed work.

Incomplete visibility leaves security teams scrambling to fill in the gaps by manually reviewing activity logs or parsing through data warehouses. It also makes it nearly impossible to establish consistent data quality standards and policies for data access, management, and migration.

The result? A disjointed data security strategy that puts sensitive company and customer data at risk.



64% of respondents

cited **data loss and leakage** as their top cloud security concern, as surveyed by Statista in their Biggest Cloud Security Concerns 2020-2021 report.

As cyber attacks become increasingly more sophisticated—and costly—organizations with suboptimal data security strategies are at significant risk of breaches and data loss through malware, ransomware, and identity-based attacks.

Enterprise security teams should avoid combining application-level solutions to protect critical infrastructure or locking down data so tightly that even authorized users cannot access it. Instead, they should implement solutions that enable seamless, comprehensive data protection.

Secure Customer and Enterprise Data Within the Zero Trust Framework

Zero Trust supports advanced data protection by protectively limiting access to sensitive assets and giving security teams comprehensive visibility into all network activities. Implementing Zero Trust requires more than deploying new security tools or data management policies.

Organizations must change how they approach data security to protect assets and develop a Zero Trust architecture.

Each enterprise should adopt a unified strategy that enables IT teams to make informed decisions about critical assets and the users who interact with them. To achieve this, IT teams will need to work with the business to understand what is critical and why.

There are several steps organizations can take to prioritize data security and protection within their Zero Trust implementation plans:

TO ACHIEVE ZERO TRUST, ENTERPRISES NEED COMPREHENSIVE, REAL-TIME VIEW OF ALL DATA ON-PREMISES AND IN THE CLOUD TO CLASSIFY, MONITOR, AND PROTECT IT.

Gain a Comprehensive View of Enterprise Data

Security teams cannot protect sensitive data without complete visibility into all of the data that exists within the enterprise. They need a comprehensive, real-time view of all data on-premises and in the cloud to classify, monitor, and protect it from internal and external threats.

End-to-end information security and data loss prevention (DLP) software gives security teams unparalleled data visibility across the enterprise, allowing them to identify and organize all assets, regardless of their location.

Once enterprises have established a comprehensive data collection and management system, they must create protection policies that dictate access controls and leverage automation to encrypt data based on location, risk level, and other dynamic factors.

From there, security teams can employ data activity monitoring solutions to continuously survey sensitive data and proactively execute the following tasks:

- Detect policy violations.
- Flag risky or unusual user behaviors.
- Block data transfers to unsanctioned devices.
- Take action against suspicious activities.
- Update protection policies across applications.

Ensure Compliance Without Compromising User Experience

Data security is highly complex, especially in industries with strict regulatory compliance requirements. Couple this hybrid work with its accompanying use-your-own-device policies, and many security teams feel that overly stringent data use policies are the only way to secure their critical data.

Unfortunately, some organizations choose to enhance their cybersecurity postures at the expense of their end users' experiences, which slows productivity and creates frustrating challenges for employees.

As organizations embrace Zero Trust, they should look to balance compliant data security controls with intentional considerations for the end-user experience. They can do this by implementing dynamic identity management solutions that simplify system access while verifying users' identities on the backend.

Beyond the solutions they deploy, enterprises should make security an integral part of users' experiences and give them an active role in data protection. Dictating clear access controls and data use policies, and then keeping end users up-to-date on the latest changes to policies and procedures, will help them understand their role in enterprise security—and how best to adhere to the safeguards currently in place.

ORGANIZATIONS MUST BALANCE THE IMPROVEMENTS TO THEIR CYBERSECURITY POSTURE WITH THE NEEDS OF THEIR END USERS INCLUDING PRODUCTIVITY AND SIMPLIFIED ACCESS CONTROLS.

Prioritize Platform Consolidation and Simplified Management

Today, users can access enterprise data from any location, on any device, at any time. To protect data across all of these variable touchpoints, security teams need dynamic, context-based solutions that bridge the gaps between the mainframe and the cloud, plus every point in between.

Organizations may attempt to piece together various point security solutions to safeguard their data. However, this approach creates complicated software deployments, redundancies, inconsistent data visibility for security teams, and other frustrating challenges that drive up IT costs and complexities.

To enhance data security and achieve Zero Trust at scale, enterprises should strengthen their point-based security software with comprehensive solutions that bring consistency and control to on-premises and cloud-based environments simultaneously.

These network security solutions enable scalable data monitoring and protection while simplifying platform management for security teams. Teams can leverage automation and advanced analytics to encrypt confidential information, classify data, flag suspicious activity, and continuously monitor all data.

What's more, single policy engine solutions enable security teams to roll out and update data usage and other security policies across on-premises and cloud environments in one step. This eliminates redundancies and ensures every user, device, and resource operates from a single source of cybersecurity truth.

SINGLE POLICY ENGINE SOLUTIONS ENABLE MORE EFFICIENT AND EFFECTIVE ROLL OUTS OF DATA USAGE AND OTHER SECURITY POLICIES.

Ensure Perimeter-Less Data Protection With a Trusted Software Partner

Zero Trust requires that businesses transform their entire approach to security by adopting a combination of new processes, technologies, and mindsets to secure all users, resources, and assets across complex environments.

Whether your organization is new to the world of Zero Trust or looking to advance its existing strategy, Broadcom® Software is here to serve as your trusted software partner.

The Broadcom Software portfolio includes Mainframe, Network, and Information Security software designed to ensure end-to-end monitoring and protection of business-critical data.

Our agile software enables our customers to seamlessly integrate modern, cloud-based solutions with their existing on-premises technology stack on their journey to support distributed work, protect sensitive data, and implement an enterprise-wide Zero Trust security strategy.

Connect with our sales team today to discover how we can support your Zero Trust strategy with software that will modernize, optimize, and protect your business from the data center to the edge.

BROADCOM® SOFTWARE

About Broadcom Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software has an extensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

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

BSG-ZT-Data-Protection-WP100 September 15, 2022 2:44 PM