Solution Brief

BROADCOM
MAINFRAME SOFTWARE

Extending Broadcom® Zero Trust to the Mainframe

Challenge

The primary emphasis of the Zero Trust approach has been focused on the diminishing capabilities of perimeter defenses to scale and to meet today's challenges. Integration of cloud capabilities and exposing more infrastructure to public clouds have exacerbated the problem. However, it is critical that this security model be focused on the entire enterprise, not just the risk of the week. For many, the mainframe is still a crucial system that manages most of their data, runs most of their transactions, and therefore, must be integrated into their enterprise Zero Trust Architecture.

Opportunity

Zero Trust offers a comprehensive framework that secures your current and future applications across the hybrid environment. In many cases, organizations already have many of the building blocks necessary to achieve Zero Trust, including their mainframe environment, but these security tools and technologies often exist within their own silos. The Broadcom® Zero Trust approach enhances the security that already exists on the mainframe by integrating these silos together.

Benefits

A comprehensive approach, embracing and extending the key principles of Zero Trust, will protect data regardless of where it is used or stored: on the mainframe, other on-premises servers, or in the cloud. Our identity solutions create the foundation for a modern Zero Trust Architecture, which ensures that consistent security processes and policies are applied across your hybrid enterprise to help address and demonstrate compliance with internal audits and regulatory mandates.

The Zero Trust model is founded on the belief that an organization should not automatically trust anything inside or outside its perimeters and must verify everything trying to connect to its resources before granting access—based on identity, context, and trustworthiness. To accomplish this goal, you must build an integrated strategy and platform that shares information across different security technologies.

Introduction

The concepts of Zero Trust are not new; they have been around for years. However, three recent developments are making Zero Trust more relevant and its adoption more important than ever:

- **Cloud:** The spread of cloud technologies is changing every facet of modern IT, including reshaping the way we develop and use applications. Organizations embracing the cloud are enjoying a range of business gains, but cloud adoption is also introducing new security challenges. Traditional security tools were not designed to adapt to the dynamic nature of these cloud environments.
- **Secure DevOps:** At its most fundamental level, DevOps applies Agile methodologies to increase the speed and quality at which innovation can be introduced into applications. One of the key facets of DevOps is automation; however, traditional security processes and tools are still heavily dependent on human configuration and effort. As a result, security often is being ignored because it impacts the delivery of apps to the market.
- **Remote Workforce:** The modern enterprise was already facing an issue with *Bring Your Own Device* movements within their workforce, but this issue was compounded by the rapid shift to remote and off-site work. Traditional perimeter defenses, such as firewalls and VPNs, could not scale to handle the large number of employees suddenly forced to work remotely, many of whom may have been forced to access corporate resources with personal devices.

Although each of these challenges may look unique and different, the reality is that a Zero Trust Architecture (ZTA) addresses them all. Unfortunately, most vendors focus their approach exclusively on these use cases, and completely ignore that organizations require an integrated strategy and need to extend and apply Zero Trust across their entire IT infrastructure, including their mainframe environment.

A Closer Look at the Mainframe

Although the concepts of Zero Trust are not new, you could argue that the mainframe was implementing these concepts long before the term Zero Trust was coined in 1994. In fact, mainframes have historically been very secure and are considered by many to be the most secure system within the data center. Because of this sentiment, organizations have often deprioritized enhancing the security of the mainframe, assuming that it is already naturally secure. Its reputation for reliability, availability, and security often make it overlooked within the enterprise but this is a mistake—no system is so secure that it cannot be improved. The reality is that for organizations running mainframes, it is a crucial technology to their business. In most cases, it is running most of their business transactions and houses most of their sensitive data, and when integrated with cloud and other on-premises systems, needs the same kind of security focus that other distributed systems have.

As organizations continue to modernize their applications and environments, the mainframe cannot and should not be viewed as its own silo; it must be integrated into the overall enterprise ZTA.

Extending Zero Trust to the Mainframe

The following sections describe how the Broadcom security tools can be leveraged to establish and extend Zero Trust to your mainframe.

Identifying Every User and Device Requesting Access
The first basic principle of Zero Trust is to verify the identity of every user and device requesting access to an application, data, or system in your environment. Addressing this principle begins with authentication—the process that positively identifies a legitimate user from a fraudulent one. This is a foundational step as you cannot effectively enforce access control policies and ensure least privileged access if you don't know who is requesting the access.

Over the years, significant advancements have been made to improve and strengthen authentication mechanisms and credentials, so that organizations can have greater confidence that the user is whom they claim to be. But to date, there is no magic bullet, no single solution that works for every situation, which means weaving in multiple types of credentials of differing strengths to cover all use cases. This is especially important for the mainframe, which has traditionally implemented its own authentication mechanisms that differ from those used to authenticate to the network.

How users are authenticated to the mainframe is controlled by the External Security Manager (ESM) security tool used (ACF2™, Top Secret™, or IBM RACF, as examples). These tools support many different login credentials, including some multifactor ones from third-party vendors. For example, Broadcom ACF2 and Top Secret both include Advanced Authentication for the Mainframe, which provides out-of-the-box support for RSA SecurID. Additionally, Broadcom also provides two alternative methods to support and deliver stronger authentication for the mainframe:

- **Symantec® VIP** is a cloud-based solution that provides a wide variety of software-based and hard token two-factor authentication credentials that are user-friendly and make logins more secure. VIP can also automatically and transparently collect data and assess login risk based on device identification (is this a known device or not?), geolocation (is user logging in from a new or risky location?), and user behavior (are user actions consistent with historic data?). Combining a contextual, real-time risk assessment with multi-factor credentials enables an intelligent, layered security approach to verifying a user's identity before granting them access.
- **Symantec Privileged Access Management (PAM)** is an easy-to-deploy solution that helps prevent breaches by protecting and controlling access to credentials for sensitive systems, such as the mainframe. Our US Federal customers have leveraged Symantec PAM to enforce HSPD-12 PIV card authentication for mainframe users. In this case, users authenticate to PAM with their government-issued smart card, and once authenticated, PAM logs the user directly into the mainframe; users are never given and do not know the actual password used by PAM to log them into the mainframe, making it impossible to steal.

In terms of verifying non-human devices, this is handled differently depending on how the devices are actually accessing the mainframe. For example, some apps leverage embedded credentials to log into the mainframe. Symantec PAM can eliminate these hard-coded, hard-to change passwords from applications and scripts, providing effective protection and management of these so-called *keys to the kingdom*. Using a feature called Application-to-Application Password Management (AAPM) or App-to-App Communication, these embedded credentials are moved from where they are today, and stored within the encrypted Symantec PAM vault. Applications that need these credentials must authenticate themselves to our solution before these are released. Additionally, Symantec PAM can also periodically rotate these credentials to comply with internal security policies (that is, changing a password every X days).

Another point of attack is the communications between devices and the mainframe, which may be done using APIs. Broadcom addresses this threat vector with its Layer7® API Management solution, which is lightweight, low-latency mobile gateway with integrated security and management controls designed for Broadcom Zero Trust Framework to help enterprises safely and reliably expose internal data and services running on the mainframe to developers and remote apps as APIs. Layer7 has Common Criteria Certification in two profiles, addressing the needs of regulated industries, as well as public sector requirements. In addition, it is FIPS 140-2 out of the box, and can be configured for both FIPS 140-3 and PCI-DSS compliance. Layer7 includes both OAuth and OpenID Connect (certified in four profiles), and includes over 100 built-in policies to protect against DoS and API attacks.

Enforcing Least Privileged Access

As post-mortem data breach investigations have been conducted, the role of compromised accounts and credentials has become clear, and regulatory bodies and auditors have focused their attention on the controls that organizations must implement to mitigate these risks. Thus, organizations are subject to an ever-expanding list of data security regulations and standards that mandate increased auditing and controls over users with privileged or elevated access to critical systems, especially those storing or processing sensitive data; in many organizations the mainframe is one of these critical systems.

Compliance with these regulations and audits generally focus on two points:

- Control the access of users to critical systems and the actions that they can perform on those systems.
- Govern the access of these users on an ongoing basis to make sure that they have only the level of access that they absolutely need.

On the mainframe, access management is provided via one of three solutions: ACF2, Top Secret (both from Broadcom), or IBM RACF. Within the ESM solutions, users are granted mainframe access entitlements through profiles, and these solutions either authenticate these users directly, or integrate with external identity providers to provide this verification. Multifactor authentication (Advanced Authentication Mainframe) is included on all three ESM's, enabling multifactor authentication on the mainframe. In most cases, the security provided by the ESM solutions address that first point mentioned above, but in all cases, this security can be enhanced via two solutions:

- **Symantec PAM** can enforce multifactor authentication for users attempting to login to the mainframe via a variety of credentials, including but not limited to HSPD-12 PIV cards, CAC cards, Symantec VIP (or any third-party MFA provider), and so on. Once authenticated, Symantec PAM can enforce policies that determine which mainframe profiles/accounts the user may access before logging the user directly into the mainframe. This provides an extra layer of protection.
- **Trusted Access Manager for z (TAMz)** is a privileged access management tool that runs on the mainframe and complements Symantec PAM by delivering just-in-time privilege business justified elevation capabilities on the mainframe. Whereas Symantec PAM controls access to the mainframe, TAMz enables users to elevate their privileges once they are on the mainframe. This enables you to only give users elevated access entitlements when they are needed and only for the length of time needed.

With regards to the second point, governing access, this is generally delivered by an identity governance and administration solution, which delivers the following processes:

- Automated provisioning and de-provisioning of access entitlements for users based on group members or roles when they join/leave an organization or change jobs.
- Automated collection of access entitlements and business interface to support periodic reviews and attestations to ensure that access to privileged accounts is still appropriate and necessary.

Symantec Identity Governance and Administration (IGA) provides broad provisioning support for both on-premises and cloud apps, including out-of-the-box connectors for the mainframe (ACF2, Top Secret, DB2 for z/OS, and RACF). These connectors enable you to automate the granting of new entitlements and the removal of unnecessary ones from users throughout their lifecycle. Additionally, Symantec IGA also delivers a governance engine that streamlines the processes associated with user, role, and resource certifications. Existing access privileges across a wide variety of IT systems and applications, including the mainframe, can be automatically gathered and correlated; these processes can be scheduled to run periodically or run on demand. Then certification campaigns can easily be filtered to run against a subset of the users, platforms, and entitlements, and can be based on the current entitlements, a historical snapshot, or differences since

last certification. Managers and application owners can then review and approve the assigned privileges, and if they are not approved, the solution can automatically de-provision the entitlements from the user.

Assuming Breach (and minimizing the damages associated with the breach)
The last principle of Zero Trust is to assume breach, which means that despite all of the security measures you put in place to protect against unauthorized access, you must plan for this event to occur. Your security strategy needs to consider three critical questions:

- **Breach Alert:** How do you identify a compromised account or malicious insider?
- **Access Restriction:** When potential breach is detected, how do you restrict or deny access?
- **Damage Control:** What would be stolen first? How would they steal it and can you stop them?

According to a 2021 IBM report, the average time to identify a breach from compromised credentials took, on average, 250 days compared to an overall average of 212 days; and compromised credentials were the most common method used as the entry point by attackers. Under this scenario, a hacker is long gone by time you discover the breach, and your only response is to calculate how much data was stolen and inform the public about the breach. So, the first step in addressing the Assume Breach tenet is to both significantly improve the time it takes for you to detect the breach occurring and minimize the damages that can be done once a breach has occured.

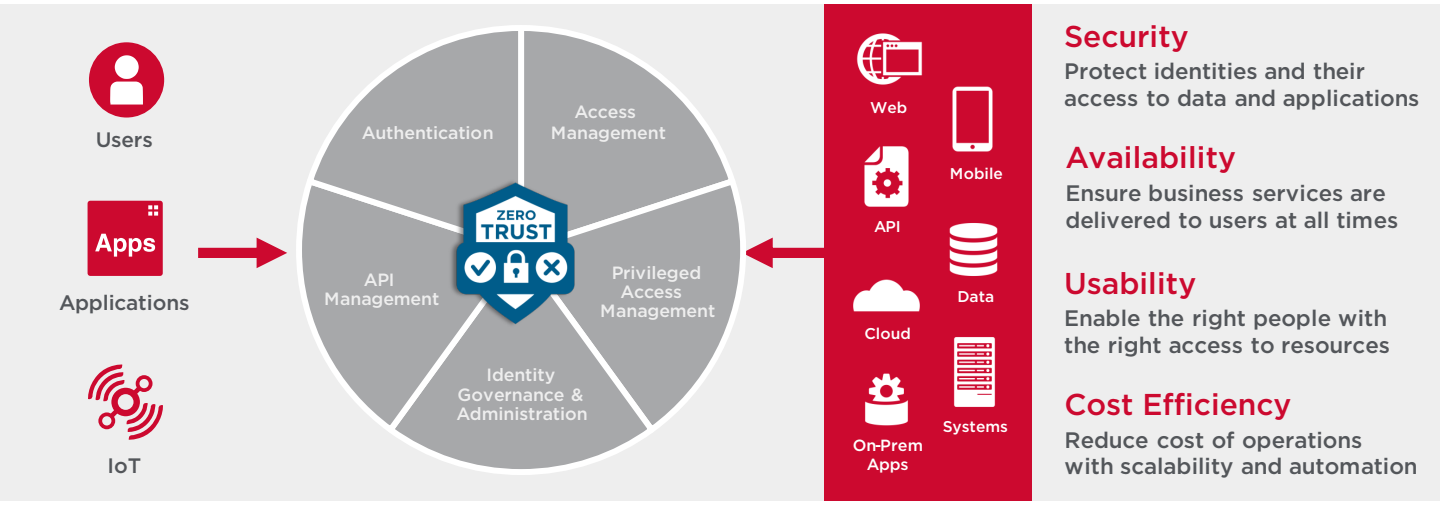
To address detection, User and Entity Behavior Analytics (UEBA) tools enable you to monitor user actions and activities and model "normal" behavior based on usage patterns. Over time, internal users, whether they be employees or contractors, will exhibit daily patterns that are nearly impossible to mimic by an external hacker. In fact, an external hacker will most likely not even attempt to mimic the user whose account they compromised; they will be too busy exploring the limits of access granted to the account to see if they can use it to carry out their attack, or find another account they can compromise that may have more entitlements. Symantec PAM provides UEBA capabilities through its Threat Analytics module, which is included free of charge. Threat Analytics continuously assesses the behavior of privileged users and compares their actions to historical observations and the behavior of other users. In this way, the solution accurately identifies attacks and high-risk activities, such as users observed surveying an environment in search of high-value assets or those who try to exfiltrate data off sensitive servers. Additionally, Threat Analytics mitigates detected risks by automatically triggering controls to stop attacks and limit damage. Mainframe events fold easily into enterprise monitoring. **Compliance Event Manager (CEM)** monitors user driven events as well as events against files and configurations. These events can be folded together with other enterprise events by way of a SIEM platform to ensure monitoring capabilities throughout the enterprise.

In terms of restricting access entitlements, Symantec PAM also provides in-depth protection of critical servers to enforce host-based, fine-grained access controls to resources, enforcement of separation of duties policies for superusers, and management of system resources and secure task delegation (sudo). These fine-grained access controls can be applied to privileged user access to files, folders, processes, and registries, enabling accountability and additional controls over the UNIX and Linux root accounts and Windows administrators. Similarly, TAMz provides the same level of control over users attempting to elevate their privileges on the mainframe.

Finally, you can further protect your data with Symantec DLP and Data Content Discovery on Mainframe (DCD), which gives you complete visibility and control over your information wherever it lives and travels, and prevents insiders from exfiltrating sensitive data. Symantec DLP can discover and identify sensitive information types using flexible predefined policy templates and an extensive library of data identifiers. Once found, DLP will monitor for policy violations and risky user behavior across control points at all times. This prevents and deters users from maliciously stealing or accidentally leaking data with real-time blocking, quarantining, and alerts. As data moves off the mainframe, Symantec DLP protects. On the mainframe, CEM can establish continuous data security and compliance by monitoring users, security settings, and system files, and then sending real-time alerts and notifications of changes and suspicious activity for complete oversight of your security systems and data.

Summary

Achieving Zero Trust is a journey and requires the integration of many types of security tools that have traditionally operated in their own silos. Many of these tools already exist within your enterprise, some delivering value but many with the potential to integrate with your mainframe to deliver even more. Customers need a partner to weave all of these disparate systems together; a partner who can also fill in the gaps where they exist.



The Critical Identity Services Need for a Zero Trust Architecture

Broadcom is that strategic partner. Not only does the portfolio deliver the critical identity services and capabilities needed to build a strong foundation for your Zero Trust Architecture, but it also offers complementary Endpoint, Network, and Information security software across on-premise, off-premise, mainframe, distributed systems, cloud apps, and infrastructures to provide the most complete and effective Zero Trust solution in the industry.

To learn more, visit mainframe.broadcom.com/security/zero-trust

BROADCOM®
MAINFRAME SOFTWARE

For more product information: broadcom.com

ZT-Mainframe-SB102 November 10, 2023