MAINFRAME SECURITY SUITE

FULL MAINFRAME PROTECTION FOR THE ENTIRE SECURITY LIFECYCLE
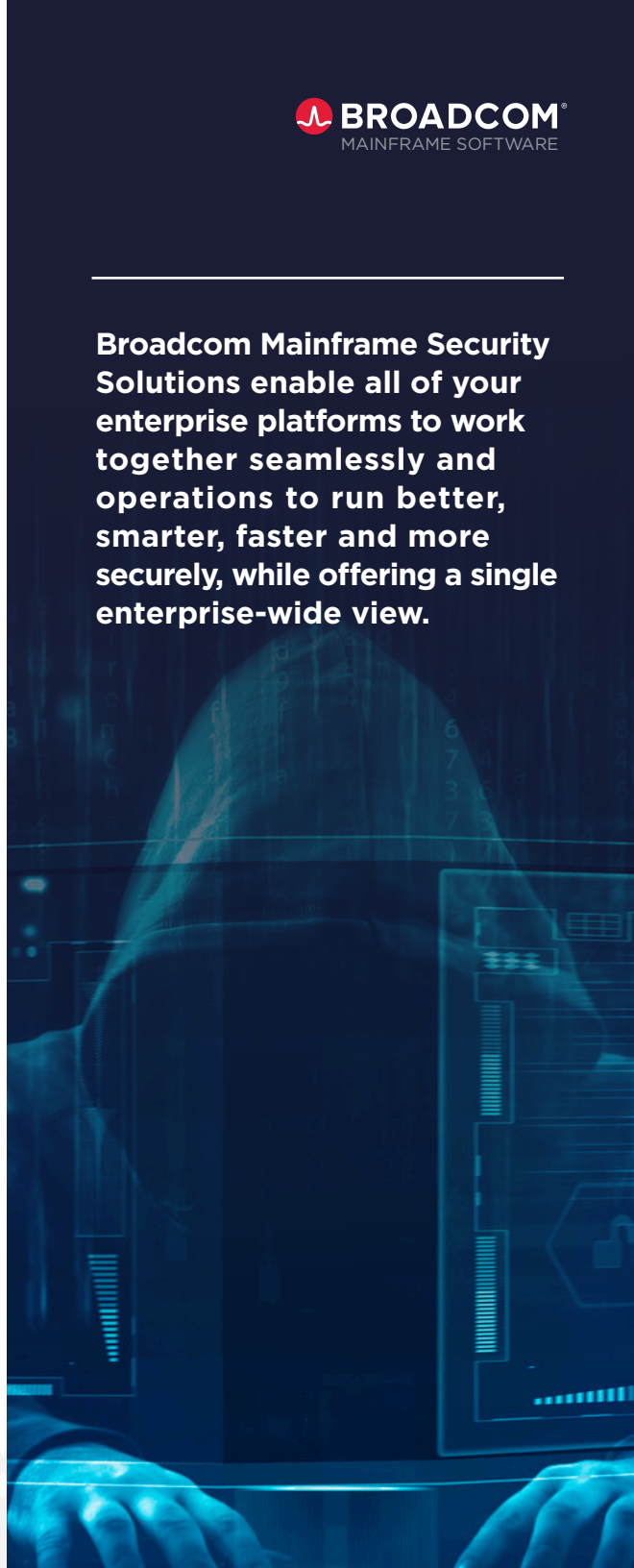
Digital Trust

In any business, whether it's B2B, B2C or P2P, trust is the foundation of all relationships and all transactions. It's vital that you build confidence in your customers—and your employees—that you can protect their data and privacy in your digital infrastructure, and that you will do so competently, with accountability and with ethics.

If you lose their trust, it's a guarantee you will lose their business.

To secure IT infrastructure and maintain safe environments, organizations today are required to comply with more and more regulations and standards. In spite of that, new and evolving security threats continue – from internal and external sources—in the form of insider data theft, social engineering, and even IoT devices.

Some examples:

- **A large European bank:** In 2012, attackers used social engineering phishing tactics to gain mainframe access at Swedish IT firm, Logica, and then the bank, stealing over $800,000. The criminals were caught not by security tools or processes but because they transferred a large a sum of money, which triggered an alert.

- **An unnamed bank:** The first known ransomware attack combined spearphishing and keylogging to steal a mainframe programmer's credentials. Hackers then submitted job control language (JCL) statements to scan for sensitive data sets and encrypt them using ransomware.

- **A U.S. financial services firm:** Severe reputational damage was incurred after attackers accessed network resources, then elevated credentials to download from the mainframe personal identifiable information (PII) including customer account and credit card numbers. In addition to exposing customers to financial fraud, identity theft and related crimes, this firm also faces fines for non-compliance with data privacy regulations such as PCI DSS, GDPR and CCPA.

- **Additional high-profile attacks on Colonial Pipeline:** This attack cut the U.S. East Coast fuel supply in half. Attackers used a leaked, re-used password linked to a virtual private networking account. Network access was not guarded by multifactor authentication. All it took was one compromised login to set in motion a chain of unfortunate events.

- **JBS Foods:** Attackers sent phishing emails to approximately 3,000 accounts at more than 150 different organizations to gain access to critical operations. This attack forced approximately 20% of U.S. beef production offline.

Broadcom Mainframe Security Solutions enable all of your enterprise platforms to work together seamlessly and operations to run better, smarter, faster and more securely, while offering a single enterprise-wide view.

Today's environment requires a re-evaluation to ensure you have the tools and processes to deal with security issues strategically.

Mainframe Security in a Hybrid IT Infrastructure Environment

In the distributed/hybrid IT and cloud spaces, many security controls have been deployed that are proactive and automated to deal with increased threats to increased volumes of data.

But what about mainframe?

Today, there are increased opportunities for mainframe to deliver value through cloud and hybrid IT integration, from apps to DevOps to big data and more. But mainframe's low-risk profile and reputation for being inherently secure has led to underutilization of available advanced security controls.

Mainframe is exposed to the same new threat vectors and human error as other infrastructures (not to mention increased scrutiny from regulatory and governing agencies). Humans working on any platform are a potential target for a social engineering attack, and new connections can lead to security exposures externally or to the backend system.

Cloud
Utilization of Today's Distributed Security Controls

Extensive Security Policies
Identity and Access Administration
Complex Passwords
Multi-Factor Authentication
Configuration Compliance
Privileged User Management
Data Classification
Security Event Management
Vulnerability Scanning
Encryption

Mainframe
Utilization of Modern Mainframe Security Controls

Extensive Security Policies
Identity and Access Administration
Complex Passwords
Multi-Factor Authentication
Configuration Compliance
Privileged User Management
Data Classification
Security Event Management
Vulnerability Scanning
Encryption

Broadcom Mainframe Security Solutions

Broadcom Mainframe Security Solutions address new and evolving threat vectors on mainframes, with an industry-leading portfolio—the Mainframe Security Suite—that provides full mainframe protection for the entire security lifecycle.

Our extensive range of security solutions protect against new threat vectors using controls similar to those available for hybrid IT but designed specifically for mainframe. We tie best practices to each element of the lifecycle, identify security risks, and assess if proper security controls are in place.

Broadcom Mainframe Security Solutions enable all of your enterprise platforms to work together seamlessly and operations to run better, smarter, faster and more securely, while offering a single enterprise-wide view.

Using this approach, customers have seen:

- A 94% reduction in the time it took to monitor and check security configuration settings

- Audit needs met in 59% less time

- Identification of hidden Personally Identifiable Information – 5% of data records scanned were discovered to have unexpected PII data

- 63% lower cost for security assessments when automated with Broadcom tools vs. traditional efforts

ACF2 Top Secret
Advanced Authentication Mainframe

Mainframe Resource
Intelligence Security Essentials

Trusted Access
Manager for Z

Auditor

Cleanup

Compliance Event Manager

"Mainframes run 70% of the world's mission-critical applications, perform financial management for 93% of companies, and complete approximately 73% of customer transactions."

Source: IBM: IBV Application modernization on the mainframe

Modernizing Mainframe Security Has Literally Turned Full-Circle

Broadcom's extensive portfolio helps you:

- Manage access and ensure proper authentication

- Manage privileged users

- Simplify regulatory compliance and streamline audits through advanced compliance management and threat detection

- Monitor activity; identify and respond to risk in real time

- Automate cleanup of unused IDs and entitlements

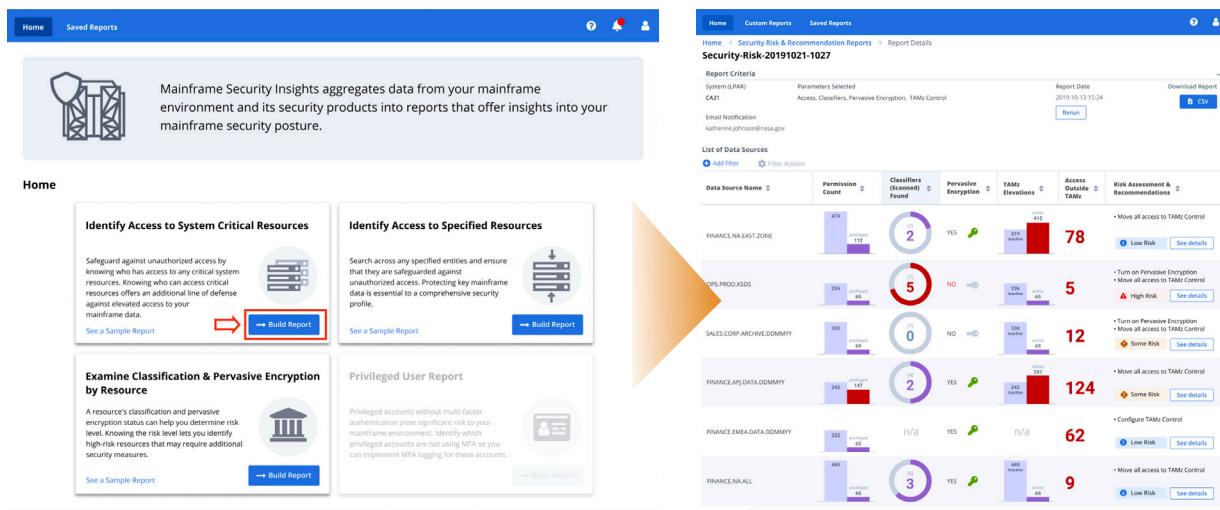- Analyze and adjust security controls

- Enable self-service audit reports

Deepen trust in user identities using enhanced verification

Advanced Authentication Mainframe / ESM

Automatically eliminate unused IDs and entitlements

Cleanup

Trusted Access Manager for z

Reduce unlimited access for privileged users with just in time access

Security Insights Auditor, MRI

Compliance Event Manager

Identify security exposures and reduce audit risk

Continuously monitor to identify and respond to security risks

Broadcom Customers Say

"With machine learning and pattern analysis, our mainframe management team can access and identify data much faster…. We've avoided hiring probably 250- 300 staff members as a result."

A North American financial services organization

Bringing It All Together With Our Security Insights Platform

Leveraging data from the modern security lifecycle, our new Mainframe Security Insights Platform (Security Insights) identifies and assesses security risk. This software enables aggregation of data across many sources, interpreting lifecycleand environmental data, analyzing data and enabling visibility into mainframe security posture.

Security Insights integrates with enterprise security operations to provide a single view through a Security Information and Event Manager (SIEM) and eliminates the manual effort of aggregation and analysis.

The result: Greater ROI with a time-saving solution that augments the skills of your staff by enabling less experienced employees to perform more meaningful work.

Broadcom Customers Say

"We've improved business results as the result of our mainframe initiatives … … we aggregate data faster … make decisions that much faster … and make more money — probably 10–15% higher revenue."

An EMEA insurance company

Putting Broadcom Mainframe Solutions to Work

Getting started is as simple as running a no-cost analysis of your environment. Mainframe Resource Intelligence Security Essentials delivers findings and recommendations based on industry best practices. It provides you with the critical information needed to understand your mainframe security environment and make informed, data-driven decisions on how to improve, helping you pinpoint where you are experiencing risk, and what you should tackle first.

SECURITY ASSESSMENTS

- Identify security gaps
- Automate & simplify health checks
- Ensure coverage

PROTECT ENTIRE SECURITY LIFECYCLE

Security insights identify risks and enable a single enterprise-wide view by leveraging data from the solutions with analytics and best practices guidance:

- Fill gaps in Security Lifecycle
- Utilize available solutions
- Ensure coverage identified in Assess phase

Zero Trust Access

Securely connect any user from any device

To any corporate application

Advanced Authentication Mainframe

✓ How do I deepen trust in user identity to ensure appropriate access?

Trusted Access Manager for Z

How do I reduce risk due to privileged users?

Compliance Event Manager

What potential security risks or bad actors are on my Mainframe?

One of the most effective methods for protecting your network, as well as your customers' and employees' information, is by using a "zero trust" model. And what is that, exactly? Well, zero trust access isn't actually a service that Broadcom offers; it's a security strategy many organizations are adopting that goes under the assumption that EVERYONE is a security threat until they prove otherwise.

A zero trust access solution asks that users inside and outside your network continually verify their identity. As they attempt to access any mainframe resource, multi-factor authentication will take place. This ensures that all resources (on premises or cloud-based) are controlled and protected from the inside out.

With Broadcom Mainframe Security Solutions, user authentication, identity validation, and privileged user management takes place throughout the process.

One way to grasp the philosophy of zero trust access is to picture a house with doors locked to every room inside. Your key may get you through the front door but entering any other room will require a separate key...and any closet or pantry within that room will require a key of its own. The idea is that users ONLY have access to the rooms or spaces for which they hold the key.

Reduce business risk and improve compliance with a comprehensive modern mainframe strategy—a best practices-based process that advances mainframe protection and moves security from firefighting to strategic value.

Benefits & Products

Broadcom Mainframe Security Solutions help you...

Manage access and ensure proper authentication
- Advanced Authentication Mainframe
- ACF2
- Top Secret

Automate cleanup of unused IDs and entitlements
- Cleanup

Manage privileged users
- Trusted Access Manager for Z

Analyze and adjust
- Mainframe Resource Intelligence, Security Essentials and Mainframe Security Insights Platform

Monitor activity and identify and respond in real time
- Compliance Event Manager

Enable self-service audit reports
- Auditor

Why Broadcom for Mainframe

When you chose Broadcom, you benefit from the most comprehensive portfolio available to support the Security Lifecycle. You'll receive:

- Solutions from the experts in mainframe security

- Complete Privileged User Management capability integrated into 3 ESMs, featuring the mainframe security-preferred Elevation method to improve traceability

- Critical data protection capability to mainframe datasets and structured databases

- Our comprehensive Security Event Management solution, providing awareness to security violations and user activity, with the ability to integrate into the SIEM tool of choice

- Automated solutions to identify and remove unused IDs and associated permissions, thereby reducing security personnel workload

- Continuous monitoring on the mainframe which will alert you to critical changes and security breaches that could lead to the compromise of your mainframe, applications and data. Non-compliance can result in out-of-control costs and a serious impact to the bottom line.

- Security analytics that help you ensure a trusted environment for your customers and employees by easily identifying and reducing risk from threats, augmenting skills and enabling a single enterprise view by integrating with SIEMs.

Don't Go It Alone

You can rely on **Broadcom as your trusted mainframe security partner** to work through complexities and provide the technologies, insights and support needed to protect mainframe applications and data.

In most cases, Broadcom's suite of cybersecurity solutions are part of mainframe customer software and services programs. **This means you're entitled to add these solutions at no additional cost.** Educational and planning services are also included to help you proactively add the latest cybersecurity protections to your mainframe, reducing risk.

Rely on Broadcom to keep your mainframe security, resilience and productivity at peak performance.

SCHEDULE A FREE ASSESSMENT

mainframe.broadcom.com/trymri-securityessentials

Questions?

Broadcom is here to help.

TALK TO A MAINFRAME EXPERT

About Broadcom Mainframe Software

Broadcom Mainframe Software empowers customers to amplify the value of their mainframe investments. Our commitment to partnership is grounded in delivering to customers greater success with the platform. It starts with embracing open technologies in ways that unite the mainframe and hybrid cloud environments. Our leading DevOps, AIOps, Security, Data Management, and Core Infrastructure software solutions and innovative value programs go beyond code to unlock the platform's full potential.

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

BROADCOM®
MAINFRAME SOFTWARE