TOP FIVE TAKEAWAYS

BROADCOM
connecting everything®

How to **Stop Firefighting** and **Make Security Strategic**

Day to day firefighting of enterprise security issues can shift focus away from a vital objective – ensuring your mainframe is secure. The truth is that threats evolve and environments shift rapidly and maintaining focus is tough when we are buried in the day-to-day chaos of putting out fires. Amidst the blazes, how can we find time to be strategic and pull ahead of the next firefight and prevent it?

1 Complex, hybrid IT infrastructure demands an adaptable, enterprise-wide security strategy

- **Digital transformation integrates business operations** across the enterprise to a much deeper extent to improve customer experience.
- This level of **integration requires a more complex, hybrid IT structure and leverages all platforms in the infrastructure.** Silos can negatively impact success, whether in application design or security policies.
- Complex infrastructures open **new threat vectors** and require a comprehensive, enterprise-wide **security strategy that is adaptable but not chaotic** and response-driven.

As much as 80% of the world's mission-critical data resides on mainframes[1]. That data is crucial to the success of business and digital transformation efforts.

"CA mainframe security solutions provide us with insights and control for our ever-changing environment. We are able to detect, respond and support security events and needs at a level that brings greater benefit to the organization."

— IT Administrator | Global 500 insurance company

2

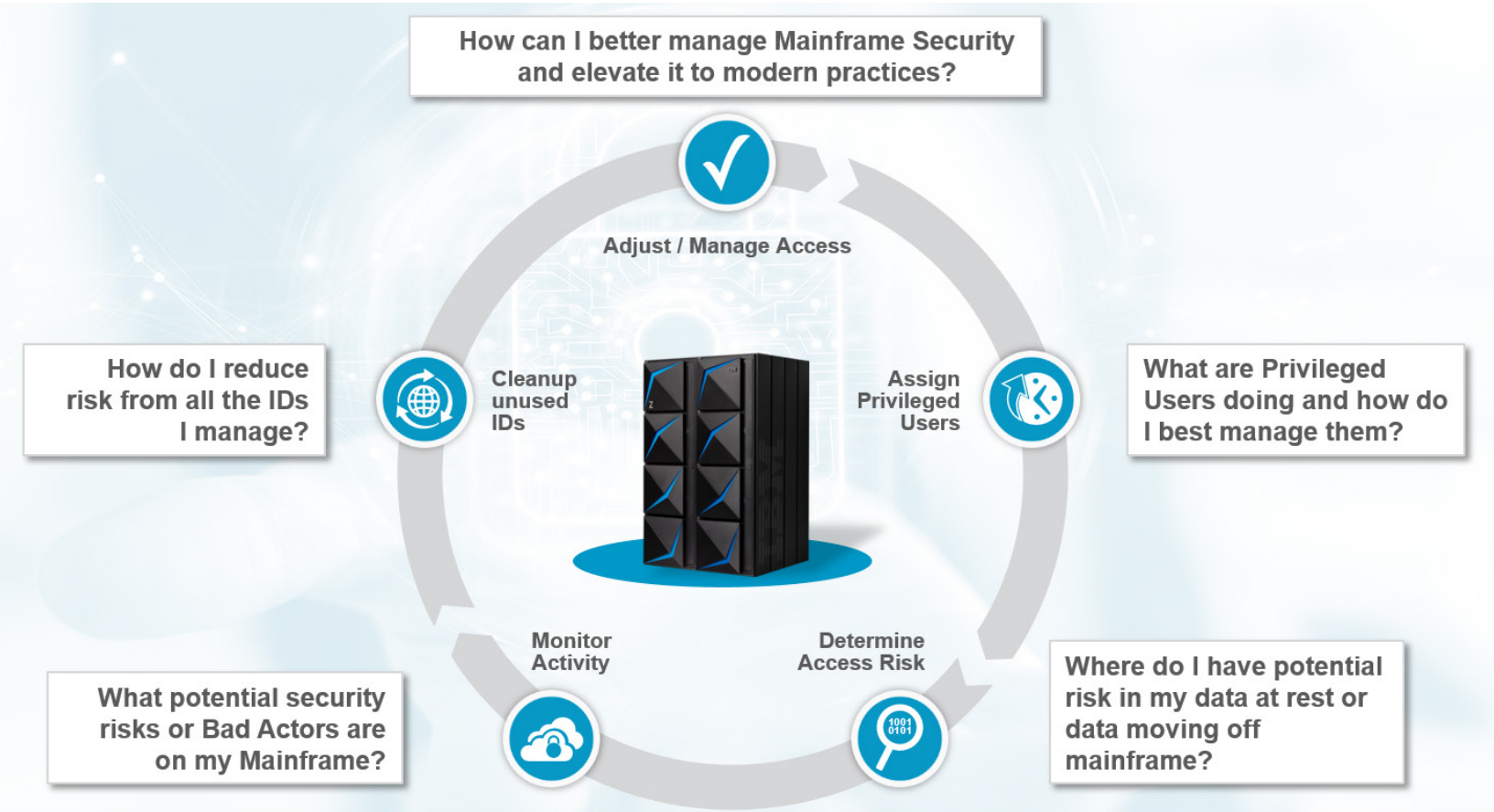
Today's risks are driven by the latest technologies—modernize security to match

- The mainframe is no longer the machine behind the curtain! Business **transformation has it connected** in ways it was not in years past and **new threat vectors need a modern security approach** and tools.
- Are my users properly authenticated? **What are privileged users doing** and how can I best manage them? **Have I identified all of the PII** on my system or is there potential risk in my data? **What insider threat**s am I facing?
- Mainframe solutions are available to address risks introduced by expanded connectivity and innovations in attack technology. **Reevaluating mainframe security** will highlight modernization efforts that **can deliver a savings in time and a reduction in risk** in the digitally transformed world.

Mainframe environments often process over 100,000 security calls per second! That's a lot of reasons supporting an enterprise-wide security strategy and a reevaluation of your efforts.

"Data classification will be useful in complying with the new California data protection regulations, as well as looking for exposed production data on test."

— Dir. Mainframe Security | National financial services firm



3 Automating routine, simple tasks enables security staff to focus on higher-value activities

- **Shifting away from security "firefighting"** and response-driven activities affords security teams the **time to implement capabilities that mitigate larger security risks** and drive more long-term value.
- Cybersecurity **automation helps address the shortage of skilled security workers** by having tools handle the work and by **supporting less-experienced staff with best practices** and insight.
- Automating and modernizing security **across all systems** in the enterprise **minimizes risk** and ensures consistency and predictability to **simplify audit and compliance**.

Automating a routine security health check yielded a 94% reduction in the time it took a customer to monitor and check their security configuration settings.

"Big topic for our organization is modernization. Broadcom is one of the best companies for us to work with in this area. In mainframe security we have the ability to modernize because you have available multi-factor solutions, privileged user management and data classification tools which help us work efficiently and keep pace with changing and additional regulations"

— Director, Information Security | Large insurance company

---

4 Skills are a critical factor in eliminating risk and ensuring compliance

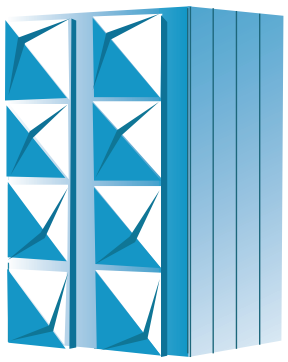
- **Broadcom invests in customer success** and takes steps to **help organizations upskill**. Our Mainframe Product Web-based Training is available at no cost for active maintenance customers. See this video for access instructions.
- Learning opportunities are also available from Broadcom and Customer experts through the Broadcom Mainframe Software Community as well. **Build skills based on the experience and mentorship of others**.
- The **ultimate in training offers skills and experience simultaneously.** The Broadcom Mainframe Vitality Program helps you find, train and mentor new employees. We hire people and train them to be mainframe experts in our products working at Broadcom and at your location. Once trained with initial experience, they transition and become one of your employees fully certified in our solutions.

ISACA's State of Cybersecurity 2019 survey revealed that 58% of organizations have unfilled security positions and 32% said it would take at least six months to fill those open jobs. And many candidates that apply aren't really qualified. MIT Technology Review found qualified security candidates are fewer than one in four.

"Broadcom's Mainframe Vitality Program took one of my employees and trained her at their expense and returned to me a master DBA. The benefits of the program are enormous. For the skills gap, we now have somebody who is trained as a master DBA. It would take years to accomplish that. Broadcom has done it in 14 weeks. I now have a master DBA."

— LInda Hagedorn | Guardian

Reduce risk with a comprehensive modern mainframe strategy



5

- **Securing the world's most securable platform involves more than simply setting a few IDs** and passwords. Inspect the security database for high usage and unused IDs. Identify and classify regulated, sensitive (PII) data. Ensure proper access with multi-factor authentication. Automate privileged access. Examine events for suspicious activity.
- **Advance your mainframe protection with modern security capabilities.** Broadcom's extensive mainframe security portfolio addresses that workflow around managing and maintaining modern mainframe security for all three CA ACF2, CA Top Secret, and IBM RACF.
- Conduct an **automated mainframe security health check** quickly and simply with **MRI Security Essentials** as a base security evaluation. It's easy to get started, just **request a free assessment** today – mainframe.broadcom.com/trymri-securityessentials.

Sixty-none percent of all data breaches are perpetrated by using stolen credentials to carry out the attack. Approximately 33% of data-loss breaches involved internal actors such as System Admins, Developers, Managers and End Users among others. Mainframe – and all other systems – are especially vulnerable to insiders, that intentionally abuse or unintentionally misuse or make mistakes when using their credentials.[2]

"The ability to understand, allow, and monitor all mainframe resources and ensure only those resources, based on business need, are allowed to authorized users. In addition to this, it allows us to identify and remove resources that are not used, which results in the elimination of many risks to the company."

— Vice President | Global enterprise banking company

1. Over 50 years after their introduction, as much as 80 percent of the world's corporate data still resides on mainframes. They are used by 71 percent of the Fortune 100, and not just for residual workloads that IT departments haven't yet offloaded into some newer storage and processing system.
   – Mainframes Are Still at the Heart of the Modern Tech World, Harvey Tessler, September 29, 2015, http://enterprisesystemsmedia.com/article/mainframes-are-still-at-the-heart-of-the-modern-tech-world#&ts=undefined
2. Source: Verizon 2018 data Breach Investigations Report https://enterprise.verizon.com/resources/reports/dbir/

About Broadcom Mainframe Software Division

Broadcom Mainframe Software Division continues to drive the next evolution of open, cross-platform, enterprise innovation. We specialize in DevOps, Security, AIOps, and Infrastructure software solutions that allow customers to embrace open tools and technologies, make Mainframe an integral part of their cloud, and enable innovation that drives business forward. We are committed to forging deep relationships with our clients at all levels. This goes beyond products and technology to partner in creative ways that support customer success.