BRINGING THE MAINFRAME INTO ENTERPRISE-WIDE ZERO TRUST SECURITY

The days of siloed mainframe security—or a lack thereof—are over. Once upon a time, assumptions about the inherent security of the platform led to a certain amount of complacency in many organizations, even as they worked overtime to protect other types of systems from rising threats. Now, mainframe leaders recognize the vulnerability of critical mainframe data, and they're moving quickly to ensure that the right protections are in place. Just as importantly, they understand that this effort must take place in an enterprise-wide context, as part of a unified set of security strategies and processes across distributed and mainframe systems.

In a recent session at BMC Exchange, our premier customer-focused event, Mark Banwell, Senior Director of Product Management at BMC, explored the journey to extend enterprise-wide Zero Trust security to the mainframe. Highlights of his presentation follow.

Zeroing in on Zero Trust

The urgency of strengthening mainframe protection comes through loud and clear in the results of the 2022 BMC Mainframe Survey, in which the overall focus on mainframe security jumped to 67 percent from 61 percent the previous year. A full one-quarter of participating mainframe leaders named managing security across the enterprise as their top priority, as alignment of security strategies across platforms gains increased emphasis. Today, that means evolving to a Zero Trust model.

In simple terms, Zero Trust means eliminating implicit trust of users or devices, and instead continuously validating every stage of digital interaction between human or machine identities and the systems they seek to access. Offering dramatic reductions in both risk and cost, Zero Trust has quickly become the definitive strategy for organizations to meet their security and compliance goals.

As organizations seek to extend Zero Trust to their mainframe as part of an enterprise-wide approach to security, many turn to BMC to discuss their business use cases, explore their implementation options, and design a Zero Trust journey that aligns fully with the rest of the organization. This process encompasses five areas of the enterprise ecosystem: data, people, workloads, devices, and networks.

Data

Ensuring the security and integrity of mainframe data is a clear priority—and in most cases, there's considerable work to be done. In fact, in 15 years of performing the security assessments and penetration tests with which these engagements begin, BMC has never found an environment without significant security issues to be addressed. In many cases, BMC services teams work with customers to improve their security architecture, remediate any areas that need remediation, and use BMC tools to recover any data that has been corrupted or encrypted by a bad actor.

People

A core principle of Zero Trust is least privilege: users should be allowed only the minimum level of data access required to perform their job function. Most organizations already have a role-based access system that defines these privileges for users on distributed systems. By using a BMC connector to integrate this system with the mainframe, you can accelerate your Zero Trust implementation while ensuring consistency across platforms.

In addition to limiting data access, Zero Trust call for a real-time threat detection and response capability. This includes identifying bad actors using stolen credentials—or malicious insiders using their own credentials—to try to elevate their privileges and access unauthorized data. BMC enables organizations to monitor system and user activity;, spot suspect behavior as it happens; deliver this information to the security operations center (SOC); and address the threat in real time. When user behavior raises concerns but falls short of an immediate threat, real-time tracking can be activated to help audit and investigate this activity in order to determine an appropriate response.

Workloads

System activity can also signal a potential security issue. BMC command center products provide mainframe teams with real-time capture, enrichment, and analysis of operating system and subsystem data to help them understand what's happening—or what's happening that shouldn't be—in the mainframe environment. Integration with leading security information and event management (SIEM) tools helps security responders and operations teams shut the window of opportunity for attackers before it's too late.

Devices

Zero Trust applies to identities of all types—including both human and machine accounts. Managing

the thousands upon thousands of digital certificates used to verify device and service accounts across the enterprise can be a major challenge, and even one expired or misconfigured certificate can increase the risk of a breach or service outage. BMC now makes it possible to automate digital certificate management on the mainframe with the same Venafi tool already being used on most distributed platforms to enable efficient, consistent Zero Trust for machine identities across the mainframe.

Networks

Just as least privilege limits the amount of data a user can access, network micro-segmentation limits the systems and data that can be reached—another key element of the way Zero Trust shrinks the attack surface. BMC enables a unified approach to network micro-segmentation across mainframe and distributed systems by providing a two-way interface between the mainframe and the Illumio Zero Trust segmentation platform. Even if a breach does occur, the hacker or malware is unable to move laterally to other mainframe or distributed systems.

To learn more about bringing the mainframe into enterprise-wide Zero Trust, including the role of automation and analytics, stream the replay of the entire BMC Exchange session here.