Executive Summary: Endpoint Detection and Response

8 Steps to Shore Up the Mainframe Against Ever-Increasing Cyberattacks
## Table of Contents

01  Introduction  
02  Cyberattacks Will Cost You  
03  8 Guidelines for Securing the Mainframe Against Possible Intrusion  
04  Conclusion
Mainframes are still in widespread use because of their reliability and security, but the shifting cybersecurity landscape has evolved new threats. Thanks to the vast number of endpoints that communicate across networks, the mainframe is closer to the internet than ever before.

Traditional defenses are no longer enough. Network access points can stretch to remote corners of the globe on employee devices, rendering firewalls almost entirely useless. Anti-virus solutions aren’t the end-all, offering defenses against only the most well-documented vulnerabilities and offering little in the way of protection against the cutting edge of cybercrime. With subpar defenses and distractions from the demands of day-to-day IT service management, a breach is not just a possibility, it’s inevitable. Proactive cyber defense across ALL threat vectors and real-time incident response is going to save you millions.
Cyberattacks Will Cost You

As the likelihood of a breach continues to rise, so too does the cost. Data from Ponemon put the average cost at $3.92 million in 2019,¹ which was a small increase from 2018 but a closer look reveals that the number of stolen sensitive consumer records increased an astounding 126%.² As regulators pass new laws governing data privacy, it’s becoming more difficult for CxOs to ensure compliance, exposing them to the additional costs associated with penalties and litigation. In some cases, the consequences from a few careless cybersecurity practices can add up to hundreds of millions of dollars, such as Uber’s 2016 violation of data breach notification laws and its attempted cover-up.³ Careers can also be at stake, as we witnessed in the Target breach of 2013 where several CxOs lost their jobs.

¹ https://www.ibm.com/security/data-breach
8 Guidelines for Securing the Mainframe Against Possible Intrusion

Because mainframes are an incredibly valuable source of data, they represent an ideal target to enterprising cybercriminals. While there’s no definitive singular action you can take to avoid a breach, the following 8 guidelines will go a long way toward mitigating some of your organization’s risk. You can find more details in the whitepaper, found here, that this executive summary was derived from:

1. **Count on Correlation:** Correlation paints a detailed picture of activity in your organization’s environment, and BMC’s correlation engine lets you spot anomalies that are outside the normal scope of day-to-day operations.

2. **Security Operations Center (SOC) Inclusion:** All too often, security is compromised because it’s separated into two different siloes: the mainframe world and the distributed world. A better solution is an SOC that grants security personnel a 360-degree view of all data.

3. **Monitor Privileged Users:** The mainframe is your most valuable IT asset, and privileged users have unrestricted access. When 500 IT decision-makers in Europe were asked about insider threats, only 9% indicated that they felt secure. Among respondents in the UK, 42 percent felt that privileged users were the biggest security risk faced by their companies.

4. **Rely on Real-time Mainframe Reporting:** Mainframe reporting typically happens on a nightly or weekly basis. Today’s SIEM must include information on mainframe security events – alongside WIN/UNIX/open source – in real-time. At the detection of anomalous behavior is detected, alerts should automatically go out to security admins and support staff.⁴

5. **Vet your Vendors:** Most security tools run on UNIX and open source systems and are managed by resources who have never even seen a mainframe. BMC has dealt with mainframe technologies for the last four decades, and our AMI for Security was designed specifically with mainframe protection in mind.

6. **Test Response Readiness:** A Ponemon Institute study sponsored by IBM recently revealed that a disappointing 77% of organizations lacked a cybersecurity incident response plan.⁵ Create a plan and then test it to ensure readiness. Responding to an attack within 30 days will save you a substantial sum – $1 million per incident on average.

7. **Lean on Your Legal Team:** Your legal team should have extensive experience with cybersecurity compliance regulations such as the GDPR and current U.S. states’ legislation, and they’ll also have information on the latest laws coming into effect in your operating area.

8. **Continuing Employee Cyber-Education:** Human error is inevitable. According to London consulting firm Willis Towers Watson, nearly 90% of all cyber insurance claims originate due to employee malice or negligence.⁶

⁵https://www.ibm.com/downloads/cas/GAVGOVNV
⁶https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/
Conclusion

Mainframe perimeters used to be physical, separate rooms secured by lock and key, and security measures needed to cover a few buildings at the most. Even if someone breached lock and key, they would have to be proficient in mainframe access to steal data and IP. Today, the proliferation of web-connected endpoints means the mainframe is no longer as insulated as it once was.

No defense is perfect, but it’s up to CxOs to ensure that mainframers are keeping up with the times.

Click here to download our whitepaper titled “Mitigating Mainframe Security Risks with Endpoint Detection and Response.” To learn more about AMI for Security, BMC’s latest mainframe security product family, please visit bmc.com or reach out to an expert today.