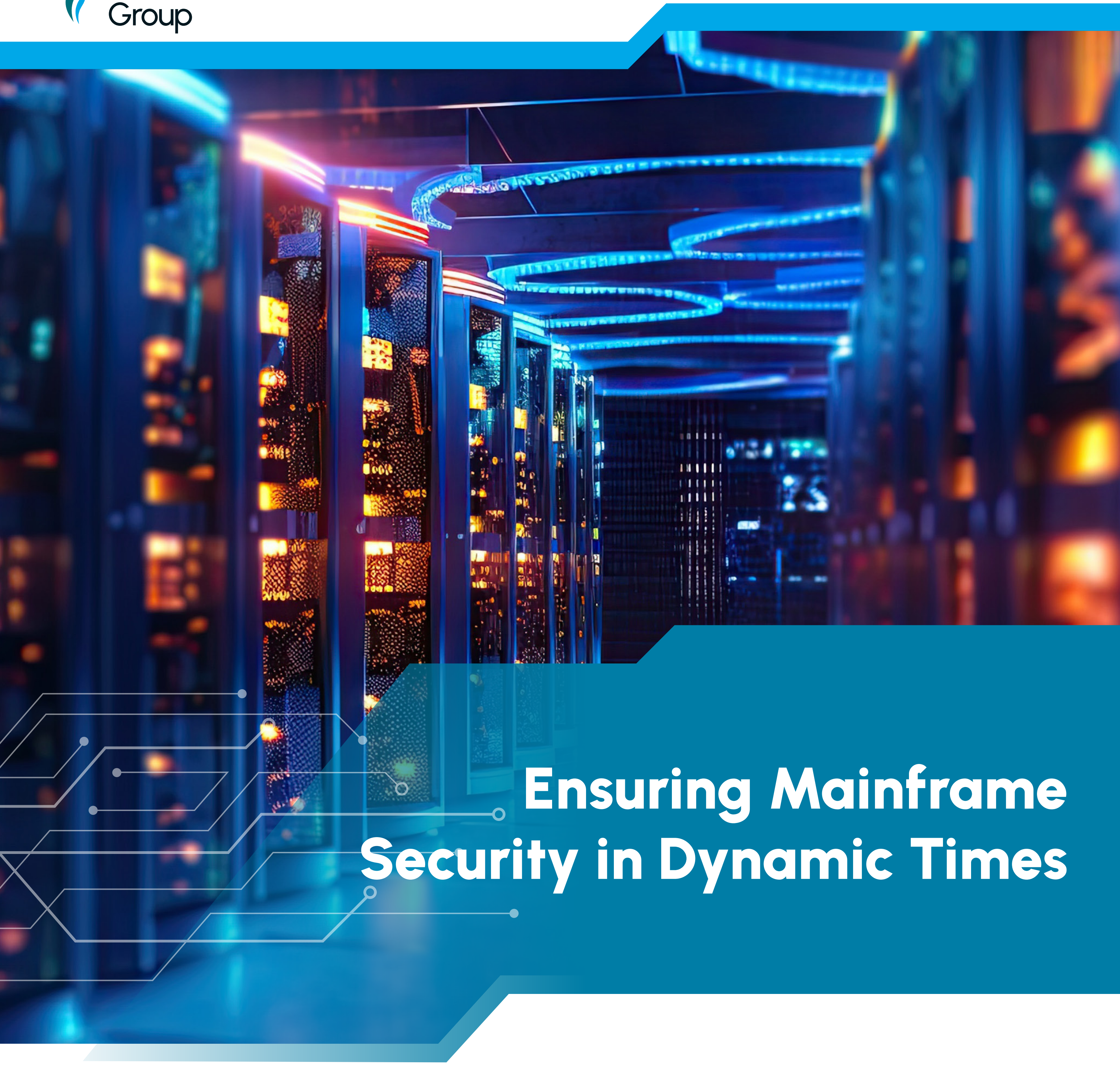


Ensuring Mainframe Security in Dynamic Times

AUTHOR

Steven Dickens
Vice President and Practice Lead | The Futurum Group

Todd R. Weiss
Senior Analyst | The Futurum Group

IN PARTNERSHIP WITH

MAINTEGRITY

NOVEMBER 2023

Executive Summary

In the rapidly evolving digital landscape, enterprises face an increasingly complex array of cyber threats ranging from nefarious actors looking to profit from their actions to nation states looking to gain global competitive advantage.

Cyber-attacks – specifically ransomware attacks – are becoming pervasive and sophisticated, resulting in much consternation within the ranks of C-suite leaders tasked with maintaining the integrity of their businesses.

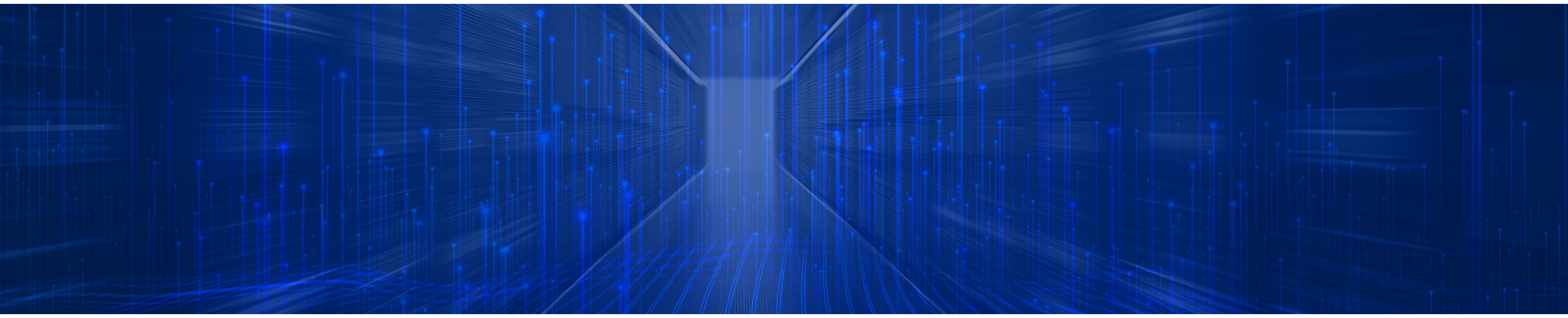
Cyber-attacks not only jeopardize data integrity and business continuity, but they also carry significant financial and reputational repercussions. Existing defensive measures, ranging from traditional firewalls to advanced AI-driven approaches, have shown limitations in preempting the multifaceted tactics employed by adversaries. To safeguard their digital assets and ensure operational resilience, enterprises must adopt a holistic cybersecurity strategy, one that integrates robust preventive measures, real-time monitoring, and contingency planning in the face of inevitable breaches.

The challenge becomes greater when dealing with mainframes, which are often the home of an organization's most sensitive data. While mainframes have long held the position as the most secure server environments available, this does not mean that bad actors cannot exploit mainframes. According to a **recent survey by IBM**, the average cost of a data breach reached an all-time high in 2023 of $4.45 million. More worrying, the IBM report goes on to say "Only one-third of companies discovered the data breach through their own security teams, highlighting a need for better threat detection. Sixty-seven percent of breaches were reported by a benign third party or by the attackers themselves."

Introduction

Supply chain security has gained more focus in the wake of the 2019 SolarWinds attack. A combination of robust perimeter controls and role-based access control with tools such as RACF, ACF2, and Top Secret have long been a security focus in many mainframe deployments, but this legacy viewpoint has arguably reached the end of the road. We see a need for enhanced security measures that go beyond traditional approaches and extend further into the architecture of the data..

The concept of file integrity has become paramount yet implementing effective measures while ensuring smooth continuous integration/continuous deployment (CI/CD) pipelines in a DevSecOps environment presents an intricate task. Additionally, the threat of ransomware looms large, with malicious actors increasingly targeting these systems to encrypt mission-critical data, thereby amplifying both the risk and the potential impact. Addressing these challenges necessitates a multifaceted approach that combines robust encryption, real-time monitoring, and proactive defense mechanisms, all while maintaining operational agility.



Solution Overview

File integrity monitoring has been available on open systems such as Linux and Windows for years but has been missing from the mainframe platform. MainTegrity's File Integrity Monitoring+ (FIM+) now brings this capability to mainframes, complementing existing mainframe tools. Because most attacks on business data require unauthorized changes to programs and parameters, by detecting malicious changes to system software, applications, job control language (JCL), and other components, FIM+ mitigates attempts to attack or steal sensitive data on zOS mainframes.

In the cybersecurity domain, the latest FIM+ version introduces a range of advanced features worthy of consideration by the most security conscious of mainframe customers. The MainTegrity FIM+ suite of solutions takes a holistic, but fine-grained approach to managing the integrity of data by taking snapshots of system and application components and creating a hashkey for each. It then stores keys in an encrypted data set on zOS (FIM Vault), which becomes the whitelist. FIM+ continues to learn about approved changes, keeping the whitelist current. It is then able to identify anything not on the list as a problem. It creates new hashkeys on a regular schedule and compares them to those in the Vault. If they match, everything is in its trusted state. If they don't match, FIM+ sends a real-time alert to the response team. Customers can then utilize the FIM+ advanced forensics, and automated recovery steps to restore integrity. FIM+ also provides support for immutable backups from all storage vendors.

Although integrity monitoring is effective against ransomware attacks the MainTegrity approach also addresses the pressing issue of malicious encryption attacks, a favored form of ransomware attack. By continuously monitoring and promptly responding to any suspicious use of encryption services, FIM+ offers a proactive approach compared to traditional detection methods. After identifying encryption in the first seconds, FIM+ checks against its whitelist to immediately decide if it is a malicious or desired encryption. If the encryption is unrecognized, FIM+ will suspend the encryption event and send a real-time alert to the security staff, who can resume the process or take corrective action. This is critical as it stops the damage occurring almost immediately in the first few seconds. This soon to be patented process effectively eliminates the human reaction time required using conventional tools.

Additionally, these capabilities play a pivotal role in attack vectors that include mass deletes, mass updates, or overwrites.

Based on our initial analysis, the MainTegrity software is thoughtfully designed to streamline administrative processes, incorporating mechanisms to gather pertinent information, utilize approved lists to minimize false alarms, and adapt to the specific usage patterns of each environment. In the ever-evolving landscape of cybersecurity, this solution emerges as a solution that offers robust and proactive defense against a wide array of threats and is therefore worthy of consideration.

FIM+ Functionality

MainTegrity FIM+ is a comprehensive security solution designed to monitor and protect mainframe environments but also to provide modern generation investigative and recovery capabilities. As such it can provide customers with an end-to-end multi-vendor resiliency process that allows prevention and reaction in a fraction of the time otherwise required.

Additionally, FIM+ employs continuous dataset monitoring to scrutinize active data files and libraries for irregular activities, even if they are not part of routine validation scans. The system incorporates behavioral analytics to detect abnormal access patterns, such as unusually high access rates, which may signify the reconnaissance phase of a cyber-attack. Automated alerts and corrective actions are triggered if any monitored activity exceeds customer-defined thresholds, thereby providing a multi-layered, real-time defense against a range of cybersecurity threats.

Specifically, FIM+ functionality includes:

- Intercepts malicious encryptions and mass deletes in seconds
- Halts malicious processes immediately to mitigate damage
- Detects tampering with backups and support immutable backup recovery
- Provides user behavioral analytics (insider attacks)
- Monitors sensitive datasets such as VSAM, PDS/E, and Seq USS
- Sends real-time alerts but avoids support fatigue by reducing false positives
- Keeps approved access lists updated in an automated manner
- Links other security tools from Vertali, IBM, BMC, Splunk, ServiceNOW into a single process
- Provides a change assurance process to security CI/CD pipelines

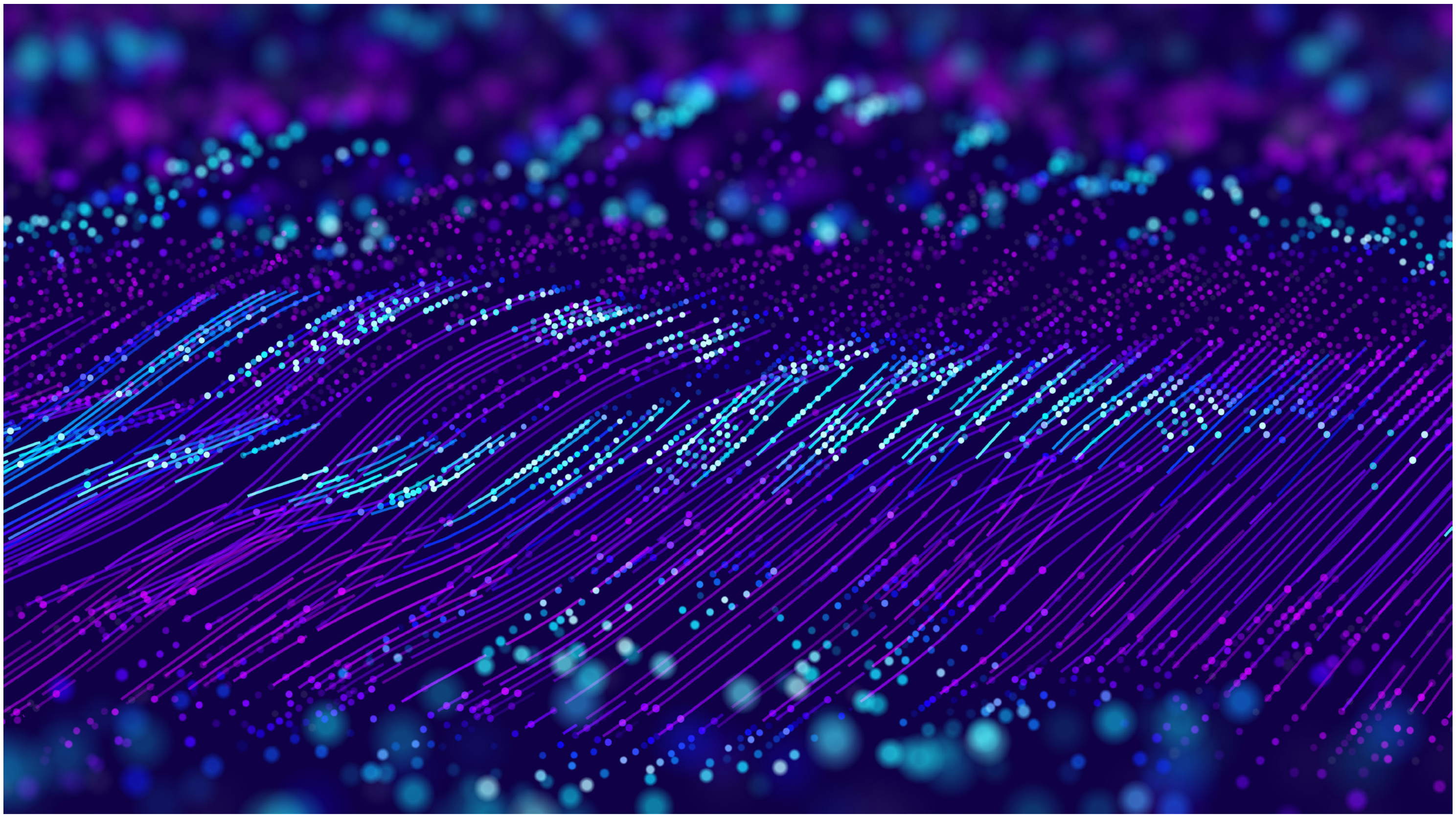
Lessons Learned and Recommendations for Driving Mainframe Security

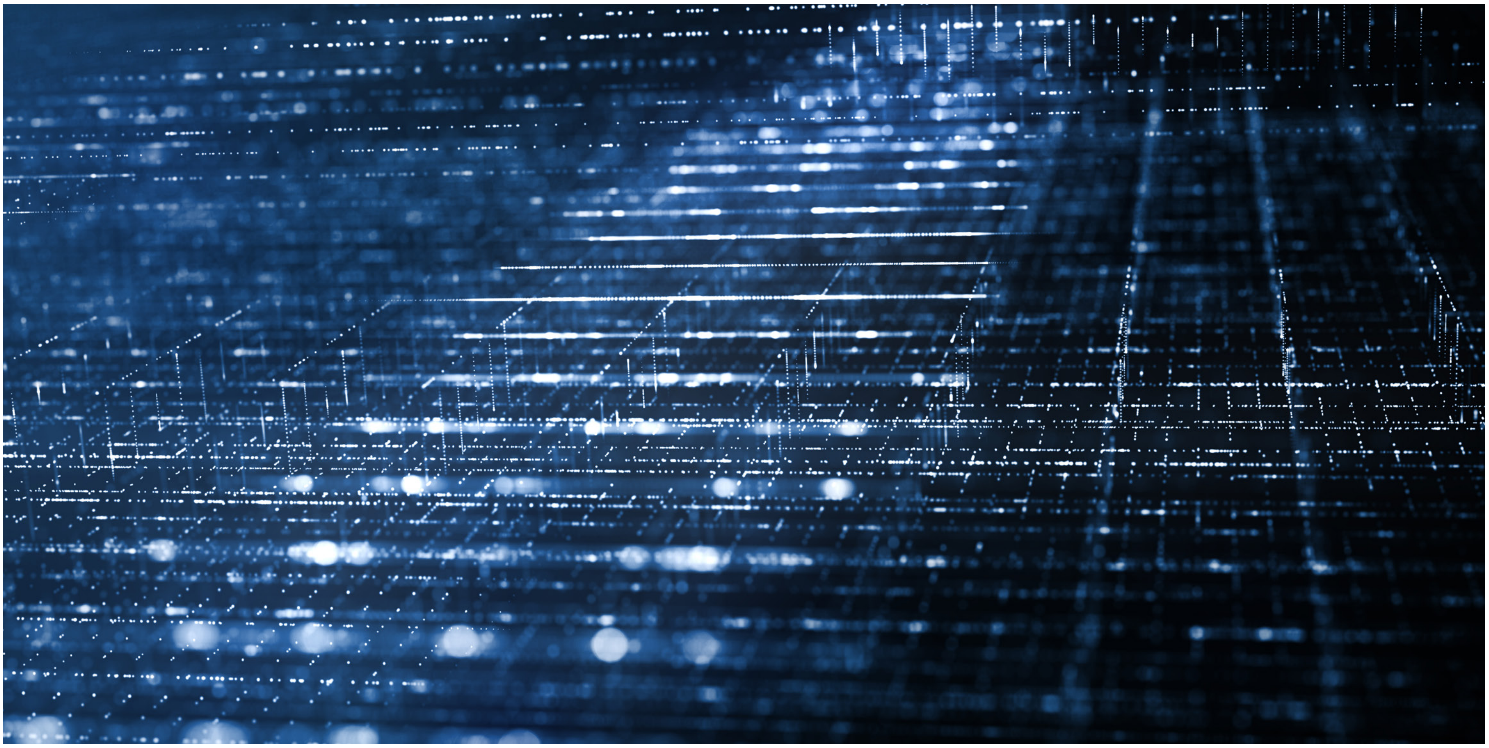
Three major areas of concern for security systems of record are file level integrity, CI/CD security, and the ability to detect encryption. They each require a distinct set of tools and processes.

File Level Integrity: A file has integrity if you can assure that it has not been corrupted and cannot be accessed or modified by unauthorized sources. Determining file integrity requires looking at a file to determine if it has been altered after its creation, curation, archiving, or other event. Unauthorized changes are signs of potential cyber-attacks on the file. File integrity monitoring tools may use checksums to compare two versions of a dataset, and hashing to create and then compare cryptographic keys to show if a file has been altered.

CI/CD Security: The SolarWinds breach underlined how high-value CI/CD pipelines are to hackers, as malicious or vulnerable code could be injected into an application. Securing a CI/CD pipeline requires establishing controls for committing code into the central repository, the ability to analyze committed code quickly, running security tests, and continuously monitoring an application after deployment.

Encryption Detection and Monitoring: Ransomware attacks encrypt important files on storage systems and demand a ransom to decrypt the files. Any effective defensive against ransomware and other malicious attacks include the ability to recognize encryption – and whether it is malicious or not – is crucial.





Conclusion and Looking Ahead

By now, it should be clear now that "doing nothing" represents a significant risk for any organization. Effective cybersecurity requires evaluating and deploying solutions that address serious threats.

In an ever-evolving digital landscape, enterprises grapple with a diverse range of cyber threats. Ransomware attacks have surged in complexity and impact, posing significant challenges for C-suite leaders entrusted with safeguarding their organizations and their most sensitive data.

These threats not only endanger data integrity but also inflict severe financial and reputational damage. Traditional defense mechanisms often fall short against the evolving tactics of adversaries. To fortify their defenses and ensure resilience, enterprises must adopt a holistic cybersecurity strategy that integrates robust preventive measures, real-time monitoring, and agile response strategies.

As we focus on the critical realm of mainframes, traditionally perceived as secure, complacency has created vulnerabilities. Recent data breach costs are a stark reminder of this, highlighting the need for improved threat detection.

The post-SolarWinds landscape underscores the importance of securing systems of record. Beyond conventional approaches, the focus now extends to data architecture itself. File integrity has become paramount, especially within DevSecOps environments. The looming threat of ransomware demands multifaceted approaches, including encryption, real-time monitoring, and proactive defenses.

In the face of these challenges, organizations must act decisively. MainTegrity's File Integrity Monitoring+ suite offers comprehensive solutions that promise robust protection and are therefore worthy of active consideration. As the cybersecurity landscape evolves, proactive strategies will be the key to resilience and success.

Important Information About this Report

CONTRIBUTORS

Steven Dickens
Vice President and Practice Lead | The Futurum Group

Dave Raffo
Senior Analyst | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

This document, including any supporting materials, is owned by The Futurum Group. This publication may not be reproduced, distributed, or shared in any form without the prior written permission of The Futurum Group.

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

ABOUT MAINTEGRITY

Based in Canada, supporting clients globally, **MainTegrity Inc**. is a world-class mainframe cyber security company. We provide next-generation threat detection, advanced file integrity monitoring, automated forensics and recovery solutions. Combining thought leadership with advanced software, we have been innovating in mainframe security for over 30 years.

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

CONTACT INFORMATION

The Futurum Group LLC I futurumgroup.com I (833) 722-5337