

MainTegrity CSF with NetWatch Combats Billion Dollar Data Breaches

MainTegrity CSF 3.2 with NetWatch gives mainframe teams visibility into data movement—detecting potential exfiltration before it becomes a costly breach.

CALGARY, ALBERTA, CANADA, January 23, 2026 /EINPresswire.com/ --

MainTegrity Inc., the leader in ransomware protection for IBM mainframes, today announces a significant advancement to prevent data breaches - the most costly attack on IBM z/OS mainframes.



MainTegrity CSF NetWatch secures mainframe environments from data exfiltration

In recent attacks, data exfiltration (data breach) has resulted in billions of dollars in consequential damages. But now MainTegrity CSF V3.2 gives clients the power to stop data theft in flight.

The Invisible Threat

For decades, mainframe security has focused on access control.

How is it then that cyber criminals stole 190 million healthcare records, received ransom payments of over \$20 million and took basic medical services away from 100 million Americans? No amount of backup will bring back stolen data, it is gone forever. By the time most organizations discover a breach, weeks or months of data leakage have already occurred.

For decades the mainframe has stood guard on data security. With new AI-powered tools and network access, attackers are now able to breach even mainframes.

In an IT industry first, NetWatch from MainTegrity can detect unusual data transfers, report malicious network behavior, and stop data exfiltration before significant damage occurs.

A Capability the Industry Has Demanded

Major financial institutions, including organizations that process trillions in daily transactions, have been requesting this capability for years. The growing sophistication of insider threats and compromised partner networks has made network-level monitoring not just important—but essential.

"This changes everything," says Al Saurette, CEO of MainTegrity. "We're not just detecting threats anymore—we're stopping data from leaving the building. Threats are identified and resolutions implemented so fast that cyber criminals will be stunned."

Protecting What Matters Most

Mainframes power 87% of credit card transactions and process 29 billion ATM transactions daily (Source: IBM). They hold the crown jewels: financial records, healthcare data, social security numbers, authentication credentials. CSF 3.2 ensures this data stays protected—even when trusted insiders or compromised partner nodes become the threat.

About MainTegrity

MainTegrity Inc. is dedicated to safeguarding the critical IT infrastructure that powers the world's most essential services. As the leader in ransomware protection for IBM mainframes, MainTegrity delivers advanced solutions that protect, detect, respond, and recover—ensuring operational continuity for financial institutions, healthcare organizations, government agencies, and enterprises worldwide. With CSF 3.2, MainTegrity continues to innovate at the intersection of proven mainframe reliability and modern threat intelligence. For more information visit maintegrity.com.

Press Contact

Al Saurette, CEO
PR@MainTegrity.com
(720) 245-2246

Allen Saurette
MainTegrity Inc.
+1 720-245-2246
[email us here](#)
Visit us on social media:

[LinkedIn](#)
[YouTube](#)
[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/885381953>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.