cloudfortress

Companies Need to Rethink Their Security Strategies Following CrowdStrike's Recent Failure

The belief that CISOs should adopt tools just because Fortune 500 companies use them is flawed. Here's why:

CIOs and CISOs should prioritize micro-segmentation with robust quality assurance controls. Controlling changes to production environments is crucial; relying on security software for automatic updates in live production systems is too risky. This is an unacceptable practice in Operations Technology (OT) used for managing critical infrastructure such as nuclear, hydro-electric power plants, and substations. Avoiding reliance on single baskets like public clouds and systems inherently interdependent on public cloud APIs is key.

The solution lies in Cloud Fortress' Secure Micro Cloud Platform, unaffected by recent events. Featuring Ironclad® technology, originally designed for industrial control systems and operational at Avangrid and other utilities. Starting at $10M USD, it offers a secure hyperconverged platform scalable up to 5MW in Latham, NY, expanding to Equinix Atlanta, GA, and looking for investors to expand active-active infrastructure into a 50MW NET ZERO CARBON IMMERSION COOLED DATA CENTER.

We should all know by now that there is a shortage of data center infrastructure readily available in the U.S. to meet demand because of limitations in our electric "not-so-smart grid" infrastructure. The outages on Azure and AWS will become more frequent over the next few years and more catastrophic as supply cannot meet the demand for Artificial Intelligence computing and Azure/AWS struggle with capacity management. What is the alternative? Ironclad®. It enables the rapid deployment of 500 KVA secure micro cloud active-active data centers for immediate operational redundancy, scalable to 5,000 KVA within eighteen months. 100% customer owned! Companies can begin migrating critical systems and applications immediately as the infrastructure expands concurrently and seamlessly; proportionate to CAPEX availability.

Furthermore, our multi-tenant hosting platform, secured by SEC20.001-U.S. Provisional Patent Application No. 62/818,390, provides inherent cybersecurity at no extra cost. Ironclad® ensures mission-critical applications run securely, tailored to U.S. and Canada operations. We manage YOUR infrastructure, allowing you to focus on your business.

Our Private Cloud Air-Gap Reference Architecture prohibits automatic updates, allowing only firewall changes at preset intervals. Software updates undergo rigorous testing before reaching production via Air Gap Data Diodes. Companies cannot effectively operate systems and defend their assets by interconnecting their infrastructure with public cloud service providers and using vendors that run their applications on the same third-party infrastructure.

Partnering with Checkpoint® and Trend Micro, we offer a defense-in-depth architecture with fifteen isolation zones on-premises via perpetual software licenses to avoid interconnect to uncertified APIs. Endpoint protection and Trend Micro's Layer-2 Security Appliances safeguard against malware and reinforce system integrity.

Visit Cloud Fortress for more information.

Paulo Silva CEO, MLS, CISSP, CISA
Cloud Fortress, LLC

Ironclad®
Next-Generation On-Premise MicroCloud Platform.
EXADATA
AUTONOMOUS DATABASE
Ironclad®
Next-Generation On-Premise MicroCloud Platform.