IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Cybersecurity

Six Essential 'Cyber Stack' Ingredients

Eric Herzog

Eric Herzog
Chief Marketing Officer
Infinidat

Biography

Eric Herzog is the Chief Marketing Officer at Infinidat (https://www.infinidat.com). Prior to joining Infinidat, Herzog was Chief Marketing Office and Vice President of Global Storage Channels at IBM Storage Solutions.

His executive leadership experience also includes: CMO and Senior VP of Alliances for all-flash storage provider Violin Memory, and Senior Vice President of Product Management and Product Marketing for EMC's Enterprise & Mid-range Systems Division.

Eric blogs at https://www.infinidat.com/en/blog

Keywords Cyber attacks, Cybersecurity, Security Operations Centre (SOC), Cyber resilient storage, Enterprise data
Paper type Opinion

Abstract

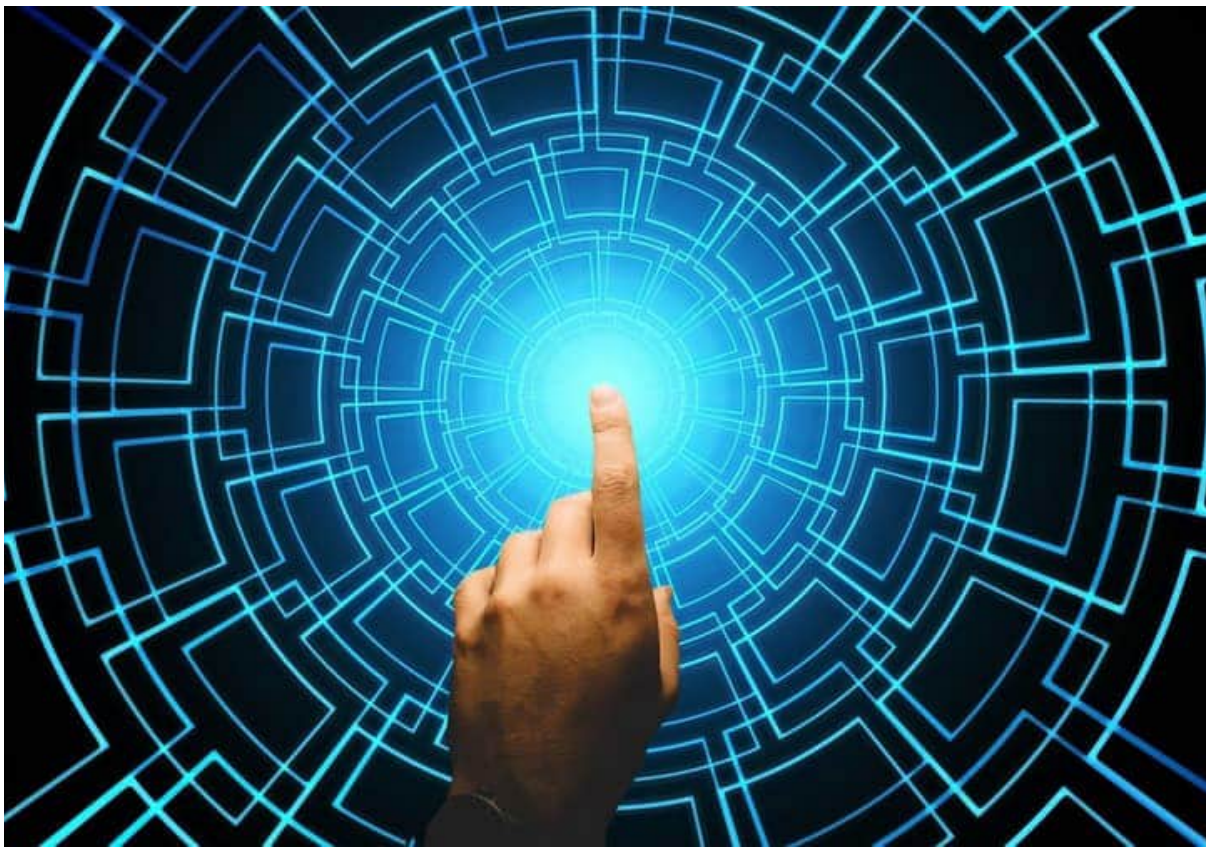
Every single second of the day there's a cyberattack taking place multiple times somewhere in the world. A well-known brand or public sector organisation is almost always in the news and facing serious disruption because of a cyber incident. So far this year we've had retailers, hotels, hospitals, airports, schools, and manufacturers such as in the automotive sector – all forced to shut down their operations to minimize the effects of a cyberattack. In this article, the author discusses the six essential ingredients of cyber resilient enterprise storage needed to have in your Cyber Stack and why.

Introduction

The heightened risk and frequency of cyberattacks means that finding solutions to deliver proactive, next-generation data protection, by employing sophisticated AI enhanced technology and deep content analysis, is imperative. This what we call your 'Cyber Stack'. It comprises all the essential capabilities needed by today's enterprises if they want to ensure their storage systems are truly cyber resilient. Cyber resilient storage, that proactively protects data to withstand an attack and that offers the ability to rapidly detect a breach and then restore operations to normal functioning, is critical.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**



1. Ability to map the attack's impact and progress

Understanding how an attack unfolds is fundamental to being able to control it. Using tools like Security Operations Centre (SOC) systems or dedicated storage cybersecurity software (SIEM or SOAR), enterprises can track suspicious activity as it moves through the network, servers and, crucially, storage. This visibility acts as an early warning system provided storage scanning is also included.

2. Identification of known ransomware varieties and outcomes

By leveraging AI-based detection technologies such as regular updates and global intelligence feeds, it's possible to ensure rapid recognition of any ransomware and malware that is already known to the cyber security community. By keeping cyber risk databases current, detection levels continuously improve and the storage system is able to adapt to thwart new cyberattack types.

3. Mapping an attack timeline and data changes with precision

Technology such as the SIEM and SOAR installed in the data centre, when combined with storage scanning tools, enable cybersecurity teams to pinpoint exactly if, when and how data was modified. This precision supports both a secure forensic investigation and a timely response to damage limitation during ongoing cyberattacks.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

4. Maintaining a full audit trail for compliance and examination purposes

Comprehensive cyber security solutions must log every event across servers, storage, and snapshots. By maintaining an unbroken audit trail, it becomes possible to drill down to the individual asset level and observe what was affected during a cyber incident. This level of granularity is crucial for both regulatory compliance requirements and when performing a root cause analysis.

5. Dashboard reporting showing key event information

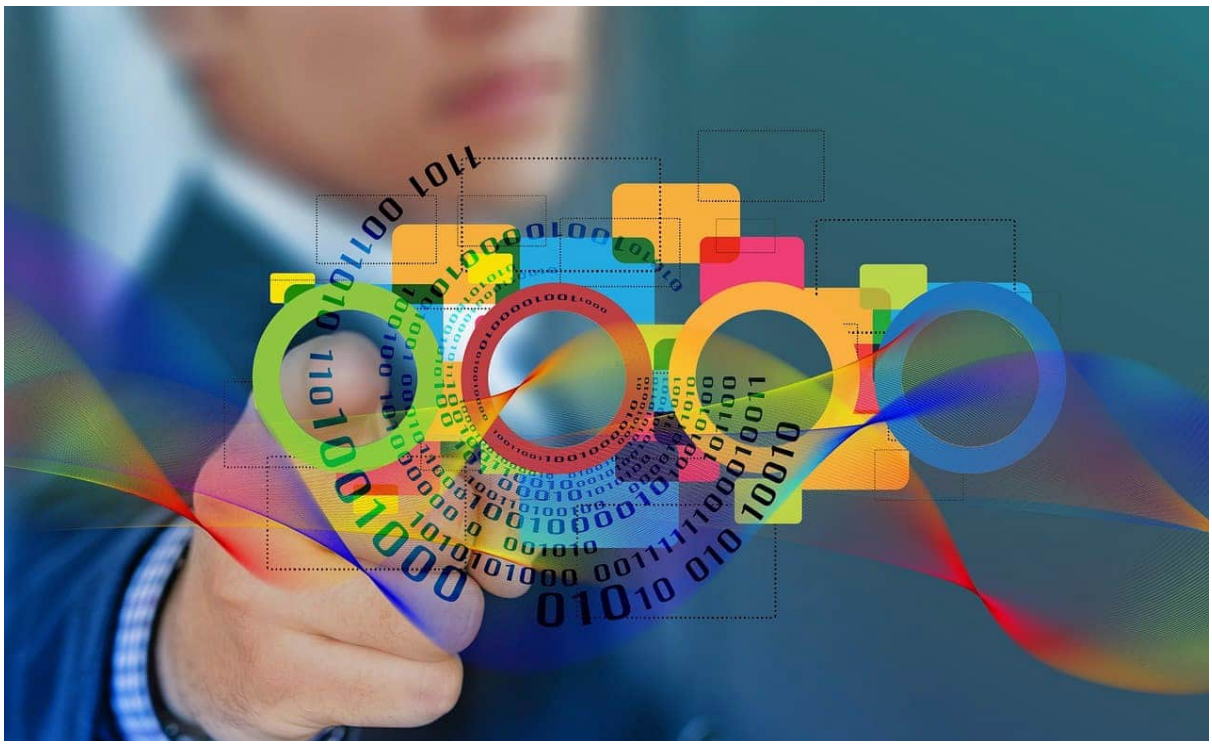
Dashboards provide clear, actionable views into key event details. They can verify the time, type and scope of each attack, plus provide more detailed information about immutable snapshots taken that contain uncompromised data. A best practice approach is to adopt automated policies and fully integrate enterprise storage with other cybersecurity tools. This helps to ensure quick, visible action is possible, with policy adaptation as and when needed.

6. Sourcing the latest clean versions of damaged data for rapid recovery

Rapid recovery after a cyberattack depends on secure forensic fencing and the ability to scan immutable data snapshots until a clean (uninfected) backup copy can be found. Scanning can either be automated or completed manually and checked by application teams. Whatever the approach taken, it should always prioritise the most recent data, unless a compromise is detected, in which case earlier snapshot versions must be reviewed.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**



In conclusion: nothing beats proactive, early detection

These six ingredients are vitally important to mitigate the effects of a cyber incident, but nothing can replace the importance of early detection of an impending attack. This is always more important than detection once an attack is underway. In spite of this, many enterprise storage companies persist in offering reactive ransomware/ cyberattack detection capabilities based on "Anomaly Detection" technology. These approaches are far less effective than proactive threat detection – because once the attack has taken place, it is most likely too late. The data compromised has probably already been written to storage and may even have been captured as snapshots – and once compromised data has been backed up, it becomes a very lengthy process to identify clean recovery points.

Best practice advice is always to invest in proactive detection of your data to ensure that in the event of an attack, you're well equipped to recover quickly, with comprehensive forensic reporting. You can then perform a deep content analysis to accurately determine "known good" copies of data and restore them quickly. These capabilities are one of the most important elements of a "total storage cyber resilience solution" that's designed to deliver a "cyber-focused and recovery-first strategy" – next-generation data protection. Experience has shown that enterprises with a well-defined Cyber Stack, proactive detection, and well tested response plans always recover quickly. In contrast, the ones lacking these essential ingredients will struggle to recover and inevitably, some never do.