ANALYST BRIEF

Sponsored by: VMware

A cyber-resilient private cloud environment combines infrastructure hardening and advanced threat prevention as well as cyber-recovery across all layers of the infrastructure to minimize the impact of cyberattacks.

Cornerstones to Enabling a Cyber-Resilient Private Cloud Environment

June 2024

Written by: Johnny Yu, Research Manager, Infrastructure Software Platforms, Worldwide Infrastructure Research, and Phil Goodwin, Research Vice President, Infrastructure Software Platforms, Worldwide Infrastructure Research

Introduction

As high-profile ransomware attacks increasingly make headlines, companies have been struggling to find the best solution to protect their data. Many organizations begin by evaluating their disaster recovery (DR) tools and methods, which are designed to restore systems and data to a functional state after a large-scale outage. While DR functionality is foundational to cyber-recovery and is indispensable as an organizational capability, DR alone is not enough. Cyber-recovery poses unique challenges that most IT teams don't have the tools to address. Attacks have become increasingly sophisticated, and true cyber-recovery requires going beyond traditional backup and DR measures. It requires recovery point validation tools to identify and contain ransomware strains across snapshots, an isolated "clean room," and network isolation of VMs at restore to prevent lateral movement, none of which are part of DR. Instead of DR alone, organizations should be looking at cyber-recovery and all the additional capabilities required to enable it in a confident, secure way.

AT A GLANCE

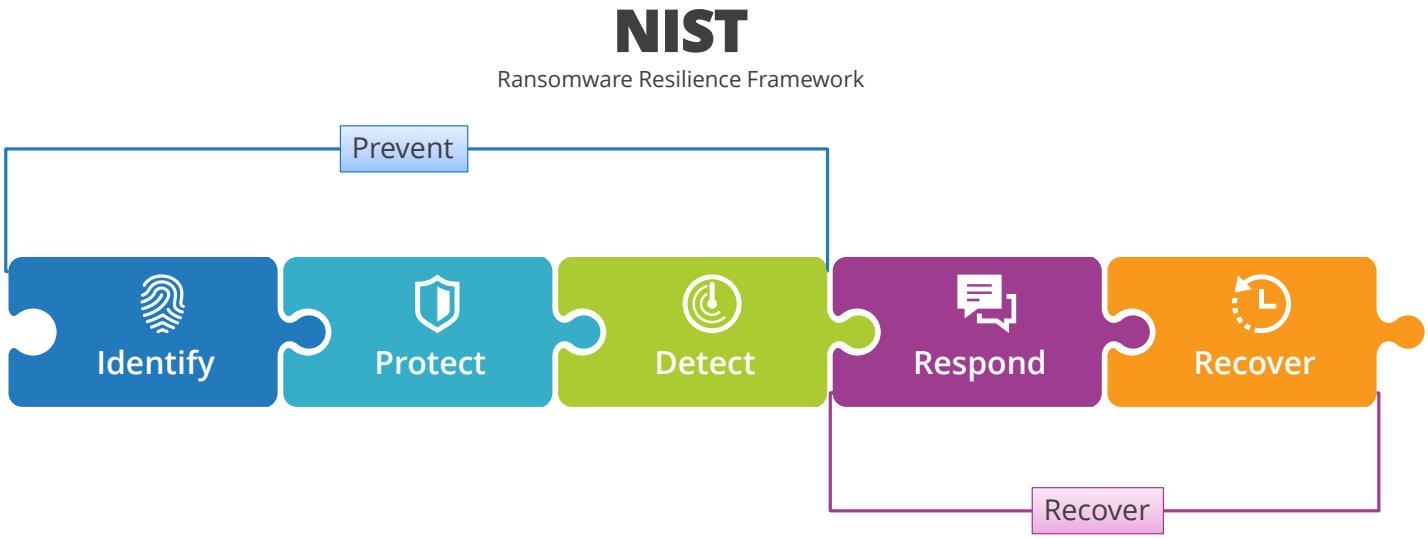
KEY TAKEAWAYS

- Cyber-resilience can be broken down into prevention and recovery components, and both are necessary for a strong cyberattack defense strategy.
- Prevention involves infrastructure hardening, strong distributed lateral security, and early intrusion detection and network segmentation.
- Recovery requires behavioral analysis and next-gen antivirus to detect fileless and file-based attacks, a deep history of snapshot copies, and isolated recovery environments.

Cyber-resilience is an organization's capacity to prevent, withstand, and quickly recover from cyberattacks while maintaining functionality and data integrity with minimal loss. The U.S. National Institute of Standards and Technology (NIST) has established a framework that describes the components of cyber-resilience (see Figure 1). Organizations can leverage this framework to develop comprehensive strategies to prevent, detect, respond to, and recover from ransomware attacks effectively.

FIGURE 1: ***Data Resilience and the NIST Framework***

Interleaving data security with data protection.



Source: IDC, 2024

The NIST framework can be largely divided into prevention and recovery components, or five pillars, that help guide what individual pieces of a strong ransomware defense should look like. Preventative measures such as infrastructure hardening, endpoint protection, and network security are designed to contain and eliminate an attack before it spreads. Cyber-recovery measures, unlike traditional DR, are designed to enable intelligent selection of recovery point candidates, their subsequent validation through security integrations in an isolated recovery environment, and workload isolation to prevent lateral movement and thus reinfection of the production site. Too often, prevention and recovery are viewed as separate tasks. To enable a true cyber-resilient private cloud environment, the framework must be viewed holistically and enable collaboration between the ITOps team (responsible for recovery) and the SecOps team (responsible for security and prevention).

Prevention

Prevention is about blocking intrusion attempts and mitigating the impact of successful intrusions, and it starts at the infrastructure level. Environments must be hardened against intrusion with capabilities such as centralized security management across all workloads, automated patch management, and network segmentation to prevent lateral movement and limit an attack's blast radius. Done correctly, prevention lowers the burden on further steps of the cyber-resilience process and enables detection and containment of the threats before they can cause widespread damage.

A crucial component of prevention, and one of the five NIST pillars, is detection. Once inside a target's environment, cybercriminals will try to remain undetected for as long as possible, up to weeks or months, to infiltrate core systems and identify critical data they can encrypt and hold ransom. The longer the dwell time, the greater the damage they can inflict and the higher the ransom demand.

By using both signature- and behavior-based detection capabilities across endpoints and networks, a cyber-resilient private cloud environment can be equipped to root out and stop infiltration attempts. When combined, capabilities such as network traffic analysis, distributed firewalls, IDS/IPS, multifactor authentication, and network segmentation can help detect and stop criminal intrusion, limiting lateral movement and reducing the blast radius of the attack.

Recovery Components

Recovery is the last line of defense once threats have infiltrated an organization's environment and ransomware has blocked access to systems and data. The foundation of successful cyber-recovery requires specific capabilities to help IT teams identify recovery point candidates, safely validate them within the bounds of an isolated clean room, and run these operations at scale without risking infection of the production environment. A common misconception is that immutable, air-gapped backups are all that's needed to enable confident cyber-recovery, but given how attacks have evolved over time and their destructive nature, this no longer holds true.

Recovery point selection is a major difference between traditional DR and cyber-recovery. In a non-malicious outage such as power outage or hardware failure, the latest backup copy is sufficient for recovery. However, in a cyber-recovery scenario, the possibility of malware having already infiltrated the backups means the latest copy may be infected. Therefore, a true cyber-recovery solution must allow for aided recovery point selection and be able to assist administrators in finding that last clean backup within the hundreds or thousands of available restore points.

Recovery points must also be validated to ensure they are malware free before restoring them back to production. This is a necessary step that leverages security capabilities such as endpoint detection and response tools, antivirus software, behavioral analysis, and other means to detect malware in the backups. Given the increasing prevalence of fileless cyberattacks, which are undetectable through traditional file scanning methods, restore point validation needs to be done by powering on the workload in a clean, quarantined environment and analyzing how the data within that workload behaves over time. This validation must take place in an isolated recovery environment with network isolation across VMs to prevent the infection from spreading laterally.

Finally, cyber-recovery must be able to restore quickly at scale. A cyber-recovery solution must be able to orchestrate the recovery of multiple workloads and products effectively with minimal downtime.

Benefits

A cyber-resilient private cloud environment must integrate these prevention and recovery measures to yield several benefits:

- **Early intrusion detection:** Threats are discovered before they have time to propagate. The proactive intrusion detection and response minimizes the blast radius of the attack and helps reduce or avoid system disruptions.
- **Stopping the spread:** Strong distributed lateral security and continuous monitoring of east-west traffic across applications in the production environment can stop attacks from spreading and causing widespread damage. Controlled network isolation of workloads during recovery point validation will also stop lateral movement and contain the attack if a compromised workload is powered on.

- **Faster recovery:** The more contained an attack is, the less damage there is. Automating the different stages in cyber-recovery (selection, validation, restore) will yield faster recovery times and help preserve the integrity of the data being protected.
- **Protecting the backup:** IDC research shows that cybercriminals attack the backup first in about half of all attacks, with half of those attacks being successful. If the backup can be compromised, then the odds of being forced to pay the ransom increase greatly. True immutable, air-gapped backup copies are key to stopping these efforts. But as we've established, they're not enough as a standalone capability to enable secure cyber-recovery.
- **Avoiding paying ransom:** Paying the ransom provides no guarantees. An IDC survey taken in December 2023 found that in one out of four instances, paying the ransom resulted in incomplete decryption. The only true way to ensure cyber-resiliency is to have purpose-built prevention and recovery mechanisms in place.
- **Better than DIY:** The integration of all the capabilities needed to enable confident cyberprevention and cyber-recovery is a nontrivial task, and organizations struggle as they have to stitch together multiple disparate products from different vendors. This has a direct impact on IT costs and resource allocation, and it leaves gaps that further expose victims to increased damage. IDC found that only about 30% of companies were able to recover successfully from ransomware attacks on DIY efforts alone. For this reason, organizations should prioritize private cloud infrastructure deployments that integrate most of or all these prevention and restore capabilities.

Considerations

Cyberattacks evolve rapidly, and no one can predict all the vectors or methods of attacks. Ransomware is lucrative, leading to increasingly sophisticated attacks as criminals grow bolder and craftier. Therefore, it's unreasonable to expect that any product or technology will be able to completely defend organizations from all cyberattacks.

Similarly, no amount of preparation can fully prevent intrusion. Even the best defense can be penetrated, either by criminals being persistent or dedicated enough or by lapses in diligence and judgment by employees. This is why both prevention and recovery are necessary for a complete cyber-resilient solution.

Operating under the assumption that intrusion is inevitable, the best defense therefore consists of multiple layers. Multiple authentication checkpoints, multifactor authentication, and role-based access controls aren't silver bullets for solving cyberintrusion on their own, but when combined, they make infiltration as challenging as possible for criminals.

Trends

- **Data protection vendors are "shifting left."** Data protection products are increasingly incorporating the ability to detect anomalous behavior and help pinpoint when an intrusion took place. There is a push for data protection to get involved in earlier stages of ransomware attacks rather than coming into play only during remediation and recovery.
- **Cyber-resilience isn't just an IT matter.** IT organizations are fostering more cooperation and integration between the ITOps and SecOps teams, and similarly, there is a trend of data protection products integrating and sharing information with data security products. Business unit stakeholders and executives are increasingly brought in on

cyberpreparedness planning as organizations recognize the responsibility of cyber-resilience needs to extend beyond IT.

Conclusion

Ransomware is an ever-looming, ever-changing threat, and organizations must adopt cyber-resilience to combat it. A cyber-resilience approach covers gaps in traditional data protection and DR, incorporating measures to prevent, detect, and eliminate intrusions; mitigate the damage from successful infiltrations; and rapidly recover systems and data at a large scale. IDC believes organizations that can build cyber-resilient environments stand the best chance at minimizing the impact of ransomware and will be well equipped to keep their most critical data safe from cybercriminals.

Ransomware is an ever-looming, ever-changing threat, and organizations must adopt cyber-resilience to combat it.

About the Analysts

***Johnny Yu,** Research Manager, Infrastructure Software Platforms, Worldwide Infrastructure Research*

Johnny Yu is a research manager within IDC's Infrastructure Software Platforms research group. He covers storage controller software; data replication, protection, and archiving; storage device management; and container data management, with a focus on how businesses optimize costs and secure their storage environments as their infrastructure expands beyond their datacenters.

***Phil Goodwin,** Research Vice President, Infrastructure Software Platforms, Worldwide Infrastructure Research*

Phil Goodwin is research vice president within IDC's Worldwide Infrastructure Research organization and global research lead for the Infrastructure Software Platforms practice. He leads a team of analysts that provide detailed insights into and analyses on evolving infrastructure software trends.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com