E-BOOK

How to fight ransomware attacks and build cyber resilience

The IT Office companion guide

NetApp

Contents

Introduction

It’s no longer a question of if you will be targeted by a ransomware attack. It’s a matter of when.

Ransomware attacks are rising—and effective protection can seem elusive. Damages from ransomware attacks are anticipated to top $30 billion globally by 2023.[1]

Not only do you need rapid response and recovery if an attack is successful. The more you can detect attacks in real time and protect against damages in the first place, the less downtime you will experience. And that’s critical because downtime comprises the majority of the cost of ransomware attacks.

The reality is that many businesses are not adequately prepared for an attack. Today, around 77% of businesses rely on backup software for data recovery.[2] With backups experiencing a 37% failure rate and 34% restore failure rates, relying on backups alone can be a risky proposition.[3]

New ways of building cyber resilience have emerged that offer businesses a choice. Instead of relying on manual searches or bolted-on security solutions, you can implement unified multicloud services that can detect threats before they strike, provide real-time visibility into what’s happening on your network with user analytics and storage anomaly monitoring, and prevent damage before it occurs.

Here’s an in-depth look at what happens when ransomware strikes—through the lens of our new series, **The IT Office**—and how to protect, detect, and recover from an attack.

77% of businesses rely on backup software for data recovery.

1 The IIAP, Ransomware attacks on the rise in 2022.
2 Gartner Peer Insights, Cyber Resilience survey.
3 Veeam, Data Protection Report, 2021

An inside look at a ransomware attack in progress

About The IT Office
The IT Office is a short, funny, fiction-that-could-be-reality video series that offers a firsthand look at an office thrown into chaos when a ransomware attack strikes—and a practical guide to how you can take different steps along the way. View the series here.

Need a recap? Read on and then discover what you can learn from the team's experience.

The company
Third Bank of Lackawanna Scranton (known affectionately as "3BoLS" by employees) is a regional bank with 13 branch locations throughout Eastern Pennsylvania. It has recently been acquired by Principled Principles Investment Group (PPIG).

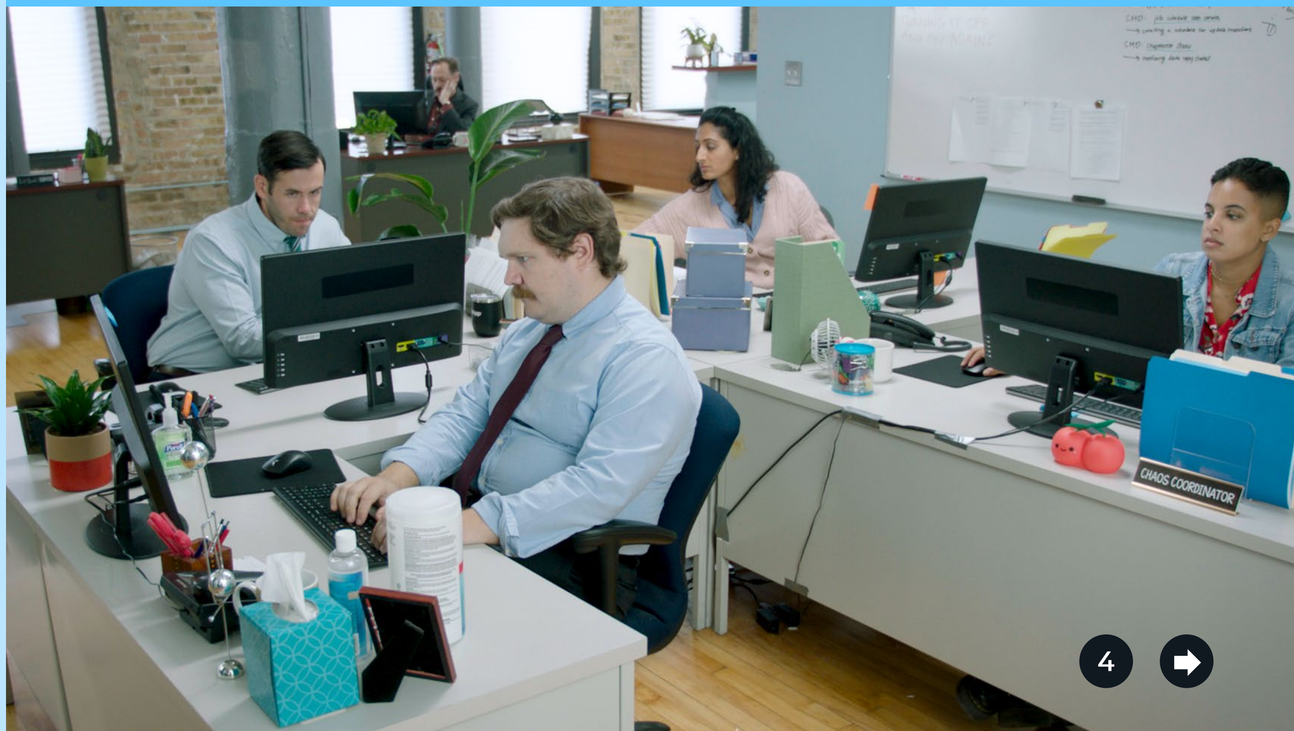
The story
During a recent malware attack on the parent company, only the Third Bank IT team managed to avoid any damage. However, the reality is that an intern was updating the VPN software and accidentally took out the network connection between Third Bank and PPIG during the time the malware struck. It was totally by accident—and to some degree, incompetence—that Third Bank avoided the attack.

However, PPIG is not aware of the true cause and believes that Third Bank's superior security practices saved the day. As a result, the IT team—with manager Spence at the helm—has been tasked with creating a one-pager detailing best practices. But instead, he's brought in a documentary crew to make a video to create dynamic content. And in the process, he's set up a scenario where the crew winds up shooting a behind-the-scenes look at an office in crisis after a ransomware attack is unleashed.

Get into the action of what goes wrong when teams rely on traditional security solutions to combat ransomware—and in this practical guide, explore how NetApp® solutions can change the game.

Watch The IT Office on-demand

Haven't seen it yet? Check out the full series here.



Staying one step ahead of threats

Episode 1 recap: The birthday surprise

Spence, director of IT, announces that the team has received a Very Important Project. Third Bank was the only division to successfully avoid a ransomware attack last month. Now, they've been asked by their parent company, PPIG, to create a best practices one-pager on data management and security. And Spence has a visionary idea: hire a documentary video crew to make a video instead.

Just as the crew is introduced, Spence receives a birthday e-card from his colleague Cam and clicks on the link. Before you learn what the birthday card says, chaos ensues. The help desk begins blowing up with new support tickets for locked user files. The database administrator, Karen, can't get into her applications. No one knows exactly what's happened, but a question looms: Is Third Bank of Lackawanna under attack—and just how big is the problem?

Key takeaways:

- Don't leave detecting ransomware to chance. Instead, quickly identify an attack before it happens with virus and malware detection that's built into your storage.
- Automatically block files with known malicious extensions, that could unleash ransomware on your network.
- Avoid the long goose chase trying to identify threats. With storage and user behavior anomaly detection, get automatic notifications when alarming behaviors occur—and clear insights into which data is impacted.

Eliminate your security blind spots

In hybrid multicloud environments, blind spots are everywhere. Stopping the domino effect of ransomware attacks once they're in motion requires more than bolted-on solutions.

NetApp cyber-resilience solutions include built-in ransomware detection that adds layers of protection to keep your data safe. Prevention is the best cure for threats like ransomware. Put automated systems in place that identify suspicious activity before it becomes a major threat.

In other words, you need solutions that enable you to monitor user behavior across hybrid multicloud environments for suspicious activity and detect anomalies in storage behavior. Don't rely on a few individuals to manually spot and combat ransomware or other threats, while juggling day-to-day IT management tasks.

NetApp BlueXP™ is a unified control plane that lets you manage your data estate across hybrid multicloud environments. BlueXP includes an observability service that can detect user account abnormalities that might indicate a ransomware attack. It can help identify the source of the attack and automatically block the compromised user account to prevent further damage.

When abnormal user behavior is detected, a Snapshot™ backup copy is immediately and automatically created, in case it's needed as a recovery point to help restore your data rapidly.

Your primary volume may be susceptible to encryption, but your Snapshot copies are immutable. When combined with BlueXP backup and recovery services, you get a secure and effective data protection strategy.

Prevention is the best cure for threats like ransomware.

Know what to do in a crisis

Episode 2 recap: Coulda, shoulda, woulda

Instead of offering a triumphant review of the bank's data protection policies for the video crew, the IT department scrambles to respond to the ransomware attack. The servers and applications are shut down, which means the malware can't be detected, key workloads can't be run, and alternate ways of contacting stakeholders (such as texting) aren't possible because their contact information is stuck in offline databases.

Storage administrator Cam and security administrator Aidan work together to bring servers and devices back online, and then manually run scripts to determine what's been impacted. They also run security updates. But even these heroic efforts leave an incomplete picture. Because Cam and Aidan can't easily tell what data is there, it's impossible to see what's deleted.

Blu, the application owner, opens applications to see if they are compromised and sees damage happening in real time. Just as these issues are discovered, a ransom request pops up and Spence has been called to a meeting with his boss, Gabriela, the CISO from the parent company.

Key takeaways:

- User behavior analytics can help you immediately uncover the source of an insider threat to isolate and remediate it.
- Multi-administrator verification can prevent a single rogue or compromised admin account from creating havoc with your data.
- Automated threat detection uses built-in machine learning (ML) to detect and respond to ransomware and other cyberthreats.

Respond to ransomware attacks

Responding effectively to a ransomware attack requires that every member of your team knows what they need to do during the emergency—and has the tools they need to do it.

Autonomous ransomware protection:

Rapidly discover and remediate cyberthreats by using ML technology. Built into NetApp ONTAP® software, this technology monitors the file system for anomalies, which can indicate slow-moving encryption.

File-extension blocking:

Use built-in anti-malware extension blocking to prevent known malware from propagating on NAS file shares.

Protect your data with more safeguards:

Prevent insider threats to your data by requiring multiple approvals for critical administrative tasks—an industry-first native approach from NetApp. Rogue administrators or compromised credentials can put your data at serious risk. NetApp ONTAP can prevent a single administrator account from causing damage by requiring more than one administrator account to approve key tasks, such as deleting Snapshot copies using the new multi-administrator verification feature.

Automated backups:

Responding quickly in the face of a ransomware attack requires having access to the latest version of your uncompromised information. BlueXP delivers seamless and cost-effective backup and recovery services for protecting and archiving your cloud and on-premises ONTAP data. No added delays waiting for physical tapes to arrive.

Identify your data for effective remediation

Episode 3 recap: Gloom and Zoom

Spence's boss, Gabriela, calls a Zoom meeting to discuss the best response to the attack. The ransomware attack has compromised the entire Third Bank enterprise. And now PPIG leadership wants answers. Spence meets with CISO Gabriela and PPIG cloud architect Diana. They have two key questions: What's the source of the threat, and what's the remediation plan?

During the call, they identify the source of the attack: Spence's email. It's discovered when Jack, the CIO, clicks on the forwarded link himself. Yikes! Cloud architect Diana is deployed to Third Bank to address the issue with an eye toward a solution that also supports the PPIG cloud-first mandate. And the team discusses bringing in outside help. The team calls in a NetApp consultant.

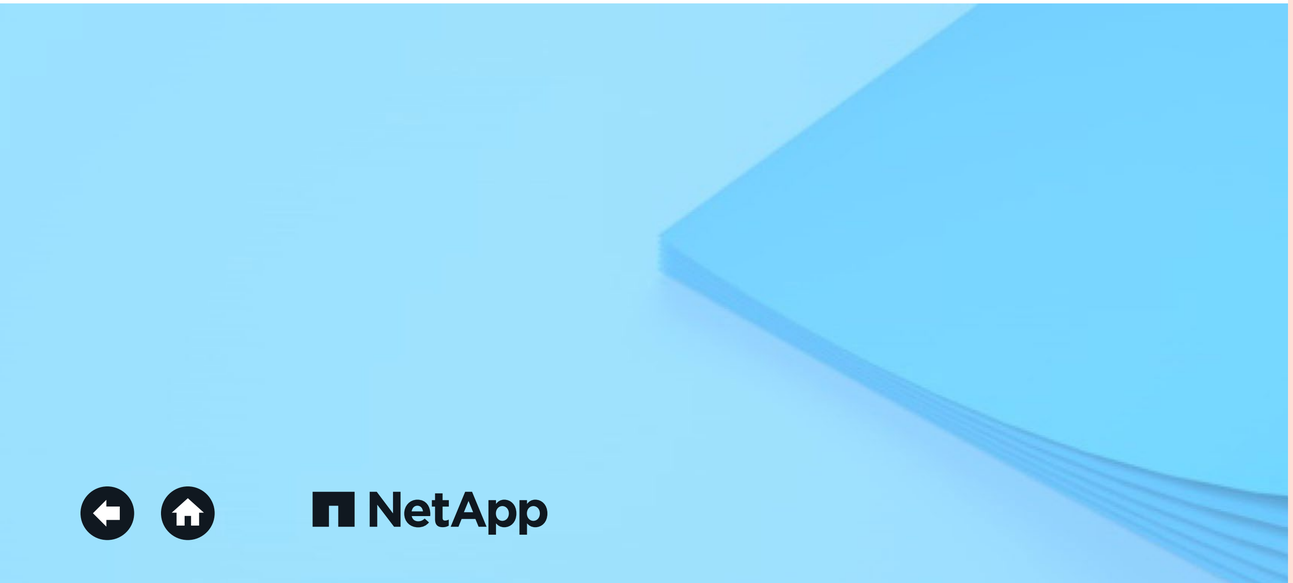
Key takeaways:

- User behavior analytics can help you immediately uncover the source of an insider threat to isolate and remediate it.
- Multi-administrator verification can prevent a single rogue or compromised admin account from creating havoc with your data.
- Automated threat detection uses built-in ML to detect and respond to ransomware and other cyberthreats.

Gain visibility with infrastructure monitoring

Understanding what data has been impacted during a ransomware attack begins with answering the questions of what data you have and where it resides. This may include:

- What applications and systems are essential to maintaining your business operations?
- Do you have an inventory of your hardware and software and where it resides?
- Where is all your data stored? How is it protected? What are the access permissions?
- Are information flows documented?
- What roles and responsibilities do each member of your team have for monitoring and remediation?



Know what data you have: Answering these questions manually takes a significant amount of time, and if your team isn't following the right protocol, important insights can be missed. NetApp can help. BlueXP data governance services scan your corporate on-premises and cloud data sources to map and classify data and to identify private information and who has access permissions. Powered by artificial intelligence (AI), it's fast, cost-effective, and accurate. Quickly and seamlessly discover what data you have, and create a roadmap to add the right layers of security management to it.

With infrastructure visibility, uncover impact and focus recovery: BlueXP observability services give you complete visibility into your infrastructure and applications so you can monitor, troubleshoot, and optimize all your resources and applications across your entire technology stack, whether it's on-premises or in the cloud.

With BlueXP governance and observability services, you can apply intelligent file forensics to identify what data was impacted and by whom to focus your data recovery and reduce downtime. Logs can be exported to leading security information and event management (SIEM) software for further analysis.

Secure data with integrated backups: Your IT team then has a roadmap for how to best manage restoring data in minutes using BlueXP backup and recovery services. And your entire team can rest easy knowing their data is fully protected. NetApp SnapLock® Compliance and NetApp StorageGRID® S3 Object Lock create a logical, operational air gap to prevent data deletion and offer native write-once, read-many (WORM) capabilities to prevent data deletion.

Zero Trust: Verify, never trust

Episode 4 recap: Zero Trust

Everyone is exhausted from pulling an all-nighter fighting the ransomware attack. Cam brings in Will “Do” Doucette, a friendly consultant who works exclusively with NetApp solutions. Aidan challenges him about getting security from “a data storage company.” Will introduces the concept of Zero Trust architecture—the concept of “verify, never trust.” The team is dubious, but the proposal offers a strategy forward.

Key takeaways:

- Verify, never trust: Zero Trust architecture is based on building a data-centric protection and security solution from the inside out.
- Advanced user access management and permission optimization can help mitigate the damage done by ransomware, compromised credentials, and other threats.

Build a shield around your most important data

Manage user access with permission controls: With advanced access management and permissions controls, set tight access to different classes or types of data. Use policy-based guidelines to limit access to potentially sensitive data, further restricting a ransomware attack's ability to destabilize your environment.

Gain the tools needed to implement Zero Trust: With Zero Trust architecture, the idea is to verify, never trust. Each attempt to access data is considered suspicious until it's verified. Embrace a Zero Trust approach to security with controls such as multifactor authentication, role-based access, comprehensive logging, and auditing to protect against attacks.

Limit the risk from compromised credentials: Often, a ransomware attack occurs when a user clicks on a compromised link and provides their user credentials. Those credentials can often be used to access a wider range of the network. Prevent damage from compromised administrator accounts by using native ONTAP multi-administrator verification. This feature requires more than one administrator to authorize critical storage actions such as the deletion of volumes and Snapshot copies, or even admin account creation.

Monitor for anomalies based on permissions and policies: Detect anomalies in real time to identify compromised user accounts or possible rogue behavior. Combined with the NetApp FPolicy component of ONTAP, BlueXP ransomware protection services enable you to automatically create data recovery points and even block further account storage access to prevent data theft.

Take the pain out of cloud-first

Episode 5 recap: The NetApp advantage

Aidan is sufficiently impressed with Will to invite him to review his recovery plan. Diana arrives and is irked when Spence insists on calling her “Lady Di.” Will and Diana turn out to be old friends and former colleagues– making Spence realize he needs to get on the “Will Do” train quickly or he’s likely to be run over.

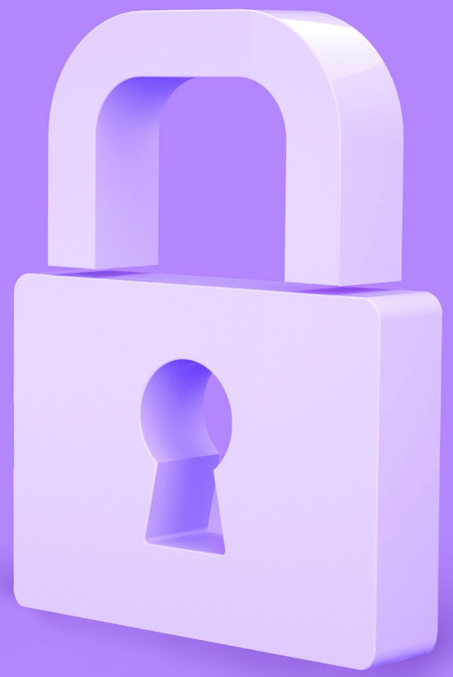
Will discusses how NetApp can help with seamless cloud migrations, reduce cloud storage costs with proactive tiering, and deliver cloud services. At the end, it’s confirmed that Gabriela and Jack are coming out to Third Bank so that Will can pitch NetApp solutions—not just for Third Bank, but for the entire PPIG enterprise portfolio in support of their cloud-first mandate.

Key takeaways:

- Don’t let a good crisis go to waste. A ransomware attack may be the wake-up call you need to really consider cloud migrations. With the right tools, taking your data to the cloud securely doesn’t have to be difficult or expensive.
- Reduce production storage costs with storage tiering. Automatically move cold data blocks to low-cost object storage, on-premises or in the cloud.
- NetApp data services support customers on any major cloud, including AWS, Microsoft Azure, and Google Cloud.

Security starts with your data

When disaster strikes, it may be time to rethink your approach to data protection and data security. A ransomware attack may cause you to seriously consider investing in the security, cost-effectiveness, and flexibility the cloud can offer. NetApp has the only enterprise-grade storage services embedded natively in the world's public clouds, and a unified control plane that makes it easier than ever to store, manage, and protect your data across a hybrid multicloud environment.



Migrating to the cloud can be seamless: NetApp Cloud Volumes ONTAP, the leading enterprise-grade storage management solution, delivers secure, proven storage management services integrated with AWS, Azure, and Google Cloud. Cloud Volumes ONTAP capacity can scale into the petabytes, and it supports various use cases such as file services, databases, DevOps, or any other enterprise workload, with industry-leading features including high availability, data protection, storage efficiencies, Kubernetes integration, and more.

And BlueXP includes integrated replication and sync services to make migration easy, efficient, and secure.

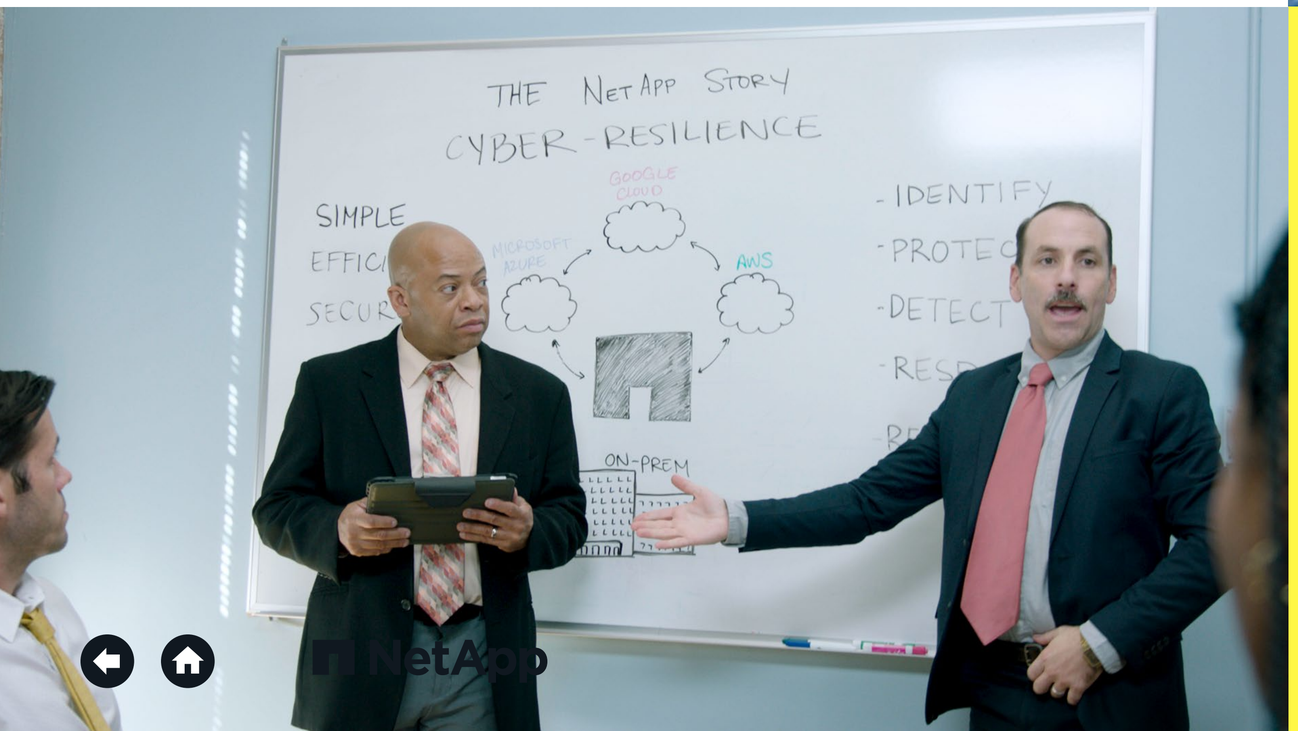
Managed cloud migration services can help: If you need more hands-on help with any stage of the process or with the entire initiative, NetApp Data Migration Services for Cloud help customers to determine the best cloud transition strategy and tailor and execute large-scale data migration plans to meet changing business needs.

Storage tiering controls cloud costs: Don't let rising cloud costs put the brakes on your migration plans. BlueXP includes a data tiering service that extends ONTAP-based storage by leveraging low-cost object storage of your choice. Without compromising on manageability and performance, BlueXP tiering services efficiently manage your storage pool by automatically placing your data at the right tier at the right time. With ONTAP, data in flight and at rest is fully encrypted, preventing any unwanted data access.

Cyber resilience is the new paradigm

Episode 6 recap: The pitch

Gabriela and Jack join Spence and his team in the conference room to hear Will make the pitch for NetApp solutions. Will introduces the concept of cyber resilience and how the right solutions can support data security, protection, and incident remediation across the entire hybrid multicloud ecosystem. By the end of the pitch, the team is sold.



Key takeaways:

- It’s time to move beyond thinking about data security or data protection as separate ideas and embrace a new paradigm: cyber resilience.
- The NetApp portfolio of cyber-resilience solutions supports the full cycle, from protecting against attacks and detecting threats to getting data and applications back online quickly.
- Protection and security are built in, rather than bolted on, to deliver a solution around your most important asset: your data.

Cyber resilience: The best defense against ransomware

Facing a ransomware attack quickly shows that effectively defending against threats requires a new approach. Enter cyber resilience.

Cyber resilience combines data protection with data security, so organizations can prevent or quickly bounce back from a cyberattack. Even if an intruder breaches the perimeter or an insider takes malicious action, the data is covered, because it has protection that's built in rather than bolted on as an afterthought.

NetApp looks at the problem of cyber resilience from the inside out. We combine data protection with data security, so you can detect threats before they impact your data and get you back online quickly. Our solutions begin by building a shield around your most important asset: your data.

For true cyber resilience you need an architecture that delivers simple data management. The National Institute for Standards and Technology (NIST) proposes a five-part framework for cyber resilience.[4] Organizations need to easily identify and protect data, detect and respond to all threats, and recover quickly, with minimal data loss or exposure. And any solution needs to be easy to manage at scale, both on-premises and in the cloud. NetApp solutions help you do that in five easy steps.

4 NIST, Cybersecurity Framework.

1 **Identify: Take stock of your environment**
Start by identifying and prioritizing what needs protecting. You need to discover where your data is stored, whether it's sensitive or regulated, who has access, what role it plays in business operations, and what hackers could do with access to it.

2 **Protect: Put your defenses in place**
Next you can take proactive steps to protect your data. Start by securing your data with powerful authentication technology and in flight and at rest encryption, to conducting regular backups that allow restores in seconds to minutes using immutable and indelible data copies. Block known malicious files before being written to disk and then prevent rogue actors by requiring more than one admin to perform critical tasks.

3 **Detect: Stay one step ahead**
Put systems in place that leverage modern AI and ML technologies to help identify suspicious activity before it becomes a real threat. Track user behavior analytics as well as storage and file system anomalies to uncover the source of an attack in real time.

4 **Respond: Take steps to minimize damage**
If a threat is detected, automatically block malicious user accounts and create immutable recovery points to minimize further damage and help prevent data theft.

5 **Recover: Get back to normal in no time**
See how easy it can be to minimize data loss with granular recovery points, restore data quickly with recovery time objectives in seconds to minutes, use intelligent forensics to help identify the source of the threat, and gauge its impact.

The right technology solutions give you the confidence to know you've built cyber resilience that prevents a ransomware attack from happening again, helps you quickly detect threats, and gives you a clear path for responding and recovering if it does.

Third Bank achieves full cyber resilience with NetApp

Episode 7 recap: Told you so

NetApp services are installed, and everyone in the office has positive things to say about how NetApp cyber-resilience solutions have simplified their lives. Spence is determined to come out of this incident in the best possible light for the video crew, who are on-site for the last day of shooting.

As Spence pontificates in his office, Cam sends him a fake phishing email. Spence clicks on it—and it's all caught on camera.

Lessons from Third Bank:

NetApp helps organizations build enduring cyber resilience, and the IT team at Third Bank is capturing the benefits.

BlueXP makes it possible to monitor your hybrid multicloud infrastructure through a single control plane that includes data protection, governance, and observability services.

BlueXP also includes a ransomware protection service, which provides a clear path to protecting data, detecting threats, and recovering quickly when attacks occur.

Get everything you need to understand, manage, and close the pathways to ransomware attacks and other cyberthreats—while empowering your entire team to focus on their specific roles and responsibilities for ensuring long-term cyber resilience.

Conclusion

With NetApp, you can build cyber resilience across your entire hybrid multicloud environment and have the tools to fight ransomware attacks and other cyberthreats from the moment they're detected. Our data protection and data security solutions are built in—not bolted on—to help you minimize data loss and downtime, proactively detect potential threats, and quickly recover data, applications, and workloads in minutes if a cyberthreat strikes.

Start your journey to cyber resilience today. Schedule a one-on-one meeting with a NetApp cyber resilience specialist.

Learn more at https://www.netapp.com/cyber-resilience/.

About NetApp
In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services, and applications to the right people—anytime, anywhere.

NetApp

+1 877 263 8277