Cyber resilience: Protect your data from the inside out
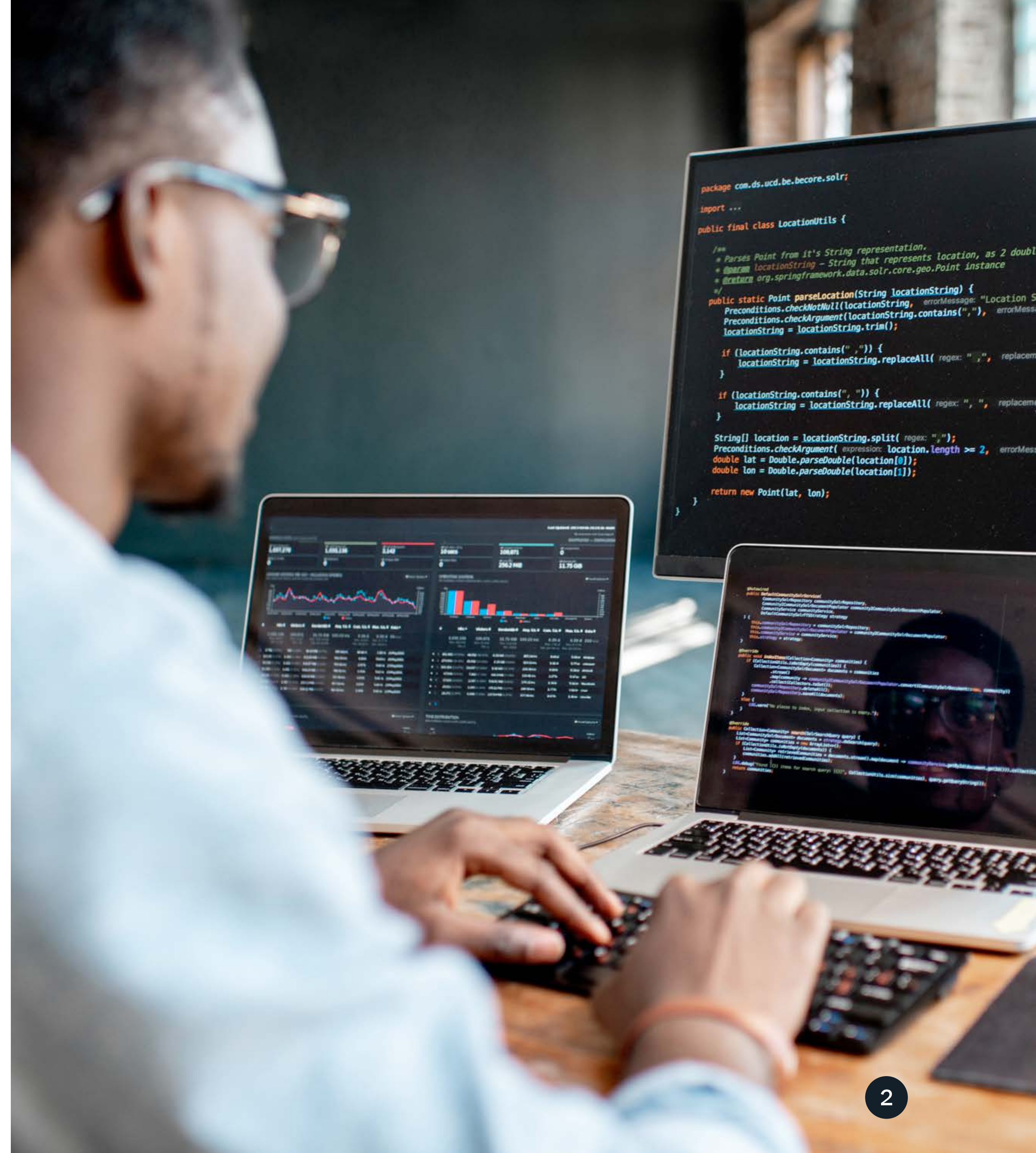
■ NetApp

Overview

Journey to the center of the IT organization

It's time for your weekly grocery run. You grab your disposable shopping bags, get your keys, and then pop a massive silver pill, your Driver Resilience Pill, into your mouth before heading out the door.

Now you can drive safely, knowing that your body has the superhuman ability to withstand potential risks on the way to the store.

If we could take magical resilience tonics, build our houses with bricks that eject intruders, or buy jewelry that flies out of a thief's hands, we'd hardly bother with seatbelts, locks, or alarm systems.

A new approach to cybersecurity

These magical protections might not exist in the real world, but they're starting to emerge in the virtual one. They're converging with existing protective gear. For the past few decades, the IT world has used the "seatbelts and alarm systems" approach to cybersecurity, because that's what was available.

Today, there's a smarter approach: *cyber resilience*.

Cyber resilience combines data protection with data security, so organizations can 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.

3

Why does this matter?

Cybersecurity measures that take a castle-and-moat approach aren't keeping pace with ever-evolving criminal tactics. Today:

Most security strategies revolve around stopping the enemy at the gate by fortifying the perimeter.

Companies aren't defending just one gate. They're responsible for hundreds, thanks to the proliferation of endpoints, bring-your-own-device policies, and the rise of remote work.

It's now easier than ever for criminals to compromise organizations that are already too overwhelmed to thoroughly monitor complex network environments.

And many organizations forget that the goal isn't to prevent intrusions. The main goal is to protect what's most valuable: **your data**.

Cyber resilience *noun*

cy·ber re·sil·ience

The capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber-resources[1]

Does your cyber-resilience strategy start with what matters most?

With threats everywhere you look, where do you start?

You start by making your security and protection data-centric. And you make it a key part of your cyber-resilience plan. In the modern threat landscape:

✓ **With a 62% increase in ransomware worldwide**[2] and a 3.4% increase in ransomware families,[3] attackers are becoming increasingly good at holding data hostage.

✓ **About one-third of organizations end up paying** to get their encrypted data back after experiencing a ransomware attack.[4]

✓ **The average cost to deal with a ransomware attack in 2021 was US$1.85 million**, up from US$768,106 in 2020.[5]

✓ **Double-extortion ransomware attacks are on the rise**, which means that organizations are at risk not just of losing their data, but of having it released to the public.[6]

The stakes are higher than ever, and ransomware attacks have become a when-not-if reality of modern computing.

But do you have to live in fear of the next ransomware attack? No. You can underline unfear ransomware and **activate cyber resilience** by taking a data-centric approach to cybersecurity.

This approach involves starting as close to the data as possible, rather than at the perimeter.
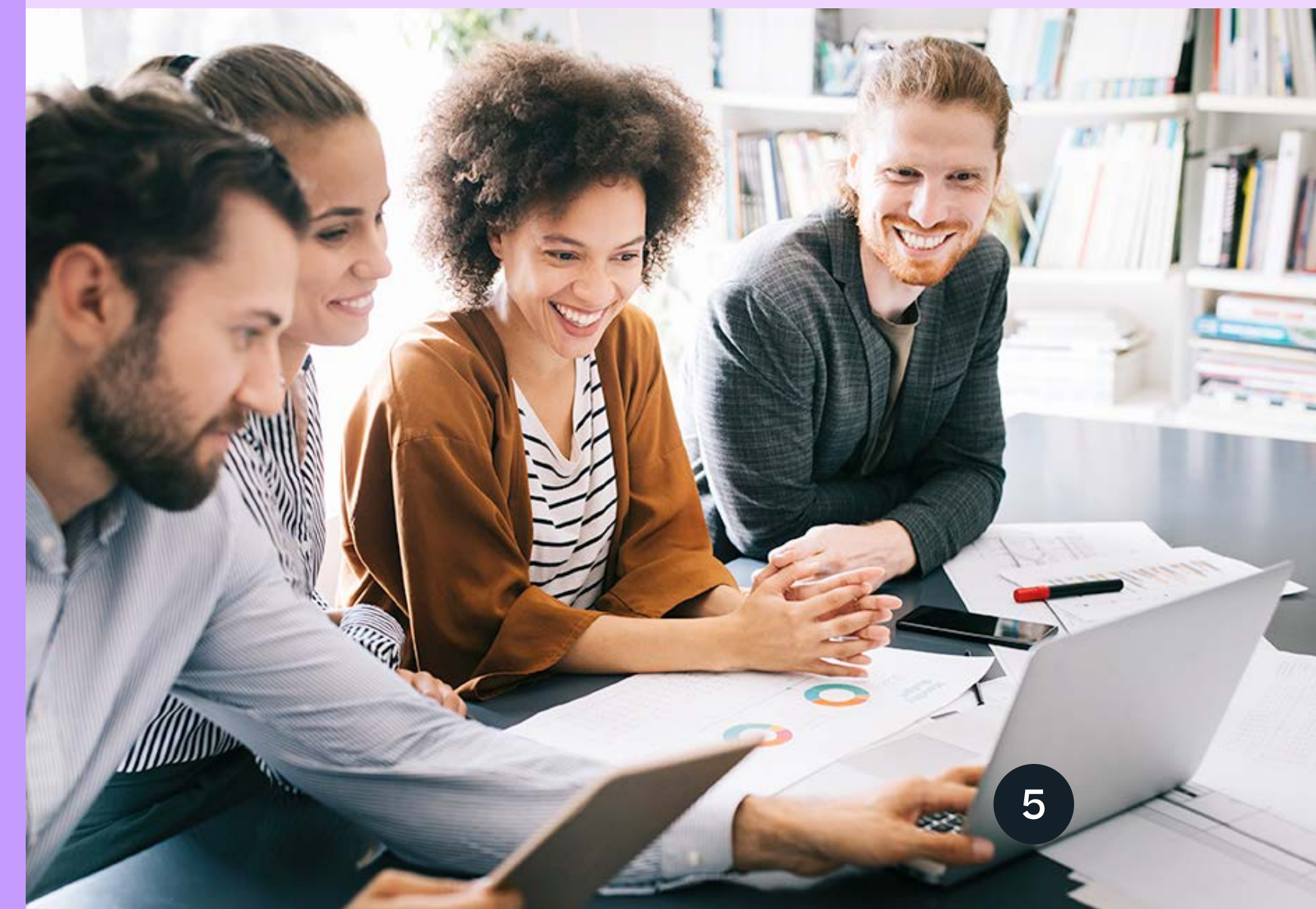
5

Chart your course to greater cyber resilience

If you're going to travel to the center of your IT organization to protect your data, a little work is in order. Fortunately, others have already ventured forth and left some helpful guideposts:

🔍 **Identify**   🛡 **Protect**   ◎ **Detect**

🔧 **Respond**   🕐 **Recover**

Even with these markers to help out, building a comprehensive cyber-resilience plan is still challenging and expensive. Your team has to juggle limited resources, fill in skills gaps, incorporate regulatory requirements, and jockey for attention with other priorities.[7] Cyber resilience can become exhausting—and forgotten—fast.

Here's how to work your way through each step.

62%

With a **62% increase in ransomware worldwide**[2] and a **3.4% increase in ransomware families**,[3] attackers are becoming increasingly good at holding data hostage.

Identify:
Take stock of your environment

Identify what needs protection and rank each item by importance.
Questions to consider include:

Q

Do you know where your data resides and what data types exist in your environment?

For each type of data, is it sensitive and who has access permissions?

Which systems are essential to maintaining business operations?

What role does each technology play in your business operations, and how could it potentially be exploited by a malicious actor?

Are information flows documented?

How are roles and responsibilities related to cybersecurity activities assigned?

What's your plan for threat identification and risk management?[7]

What are your current data protection and security solutions?

In other words, you'll need to assess your current data protection and security. You'll also need to classify different types of data, determine where the types are located, and evaluate their permissions.

Challenges associated with the Identify stage
The Identify stage is time consuming. IT leaders already have a tremendous number of day-to-day infrastructure and data management tasks on their plates. Just inventorying an entire IT infrastructure, especially without automation tools, can consume a significant amount of time.

If this inventory exercise isn't conducted with a specific plan or standardized classification protocols, it can create an even more confusing set of data that teams have trouble deciphering and operationalizing.

Protect:
Put your defenses in place

In the Protect stage, you build your walls.

Encrypt your data, conduct regular backups, ensure access control, implement perimeter defenses, update vulnerable operating systems and applications, and train users about cybersecurity best practices.[7]

This stage involves blocking malicious users, quarantining potentially bad data, preventing additional data from being written to a disk, creating granular immutable copies that thwart infection, and preventing data deletion with indelible backups.

Challenges associated with the Protect stage
The Protect stage reveals some of the latest changes in the approach to cybersecurity. Although organizations have been using firewalls and network intrusion tools for decades to protect their IT environments, the new reality of massive amounts of data has complicated these strategies. IT teams must answer challenging questions like:

How can you encrypt large amounts of data that's being generated faster than it can be inventoried?

How can you ensure access control without severely compromising the user experience (potentially leading to lower productivity levels or unsafe workarounds)?

How can you be certain you've covered everything, given the number of blind spots you've uncovered?

What regular testing are you conducting of your data protection technologies to ensure that in the event of a threat, you can successfully recover your data?

Detect:
Stay one step ahead

Prevention is the best cure. Put systems in place that identify suspicious activity before it becomes an existential threat, including:

• Updated detection processes

• Regularly monitored logs so that anomalous activity can be detected and addressed

• A thorough understanding of regular data flows, so that you can spot unusual activity that might signal data theft

• The ability to not just detect, but also gauge the impact (or "blast radius") of a breach[7]

In other words, you need to monitor user behavior for suspicious activity and detect anomalies in data behavior.

Challenges associated with the Detect stage

Manage alert overwhelm: Possibly the greatest challenge of the Detect stage is the amount of noise that organizations must filter out. Cybersecurity teams and security operations centers (SOCs) are overwhelmed with threat alerts, which they often have to work through manually.

Automate threat triage: They need a way to automatically investigate and eliminate false and low-priority alarms, so they can dedicate their attention to the trickier alerts.

Increase detection speed: Cybersecurity teams also need a way to detect these threats faster, so they can respond before serious damage is done. In particular, they need immediate notice of unauthorized access with compromised credentials before a bad actor can encrypt a significant amount of data.

Respond:
Know what to do in a crisis

Threats evolve alongside security measures. As a result, it's important to continually put your plans to the test in three steps:

1

All team members must know their responsibilities, including general cybersecurity best practices and their specific roles in an emergency.

2

Update plans as threats evolve and as lessons are learned in the aftermath of attacks.

3

Share all plan updates with other stakeholders, both internal and external, so that there's a cohesive response if an attack occurs.[7]

Challenges associated with the Respond stage
Acing the Respond step requires an overview of your systems, so you can evaluate where your data is, monitor what kind of activity is happening within your environment, and update your plans accordingly.

Again, this is a time-intensive activity for organizations that are already overwhelmed with day-to-day infrastructure and data management needs.

And the truth is that any effective response needs to be faster than the time it takes for individuals to manually execute a plan, no matter how well prepared. Cybersecurity teams need automated tools that follow predetermined steps—such as taking a data snapshot—as soon as the system detects suspicious activity.

Recover:
Get back to normal in no time

If a cyberattack interrupts business operations, you need to be able to get back up and running quickly. It's imperative to know:

- What information will need to be shared?

- Who will need access to this information?

- How will you ensure that these stakeholders get the information they need in a timely manner?

- How will you communicate the breach to the public, informing people whose information might have been compromised?

- What steps need to be taken to communicate with regulatory bodies?

In the Recover stage, you'll want to reduce downtime by restoring data quickly, bringing uncompromised applications back online, and applying intelligent forensics to identify the source of the threat.

Challenges associated with the Recover stage
In the aftermath of an attack, it can take valuable time to identify what's been compromised and how much. But you'll need to get this information quickly if you're going to manage both the internal response and the external optics.[7]

These five parts of a cyber-resilience plan—Identify, Protect, Detect, Respond, and Recover—are supported by the NetApp® cyber-resilience solution. But many organizations are invested in a patchwork of cybersecurity tools that can make the thought of shifting to another provider overwhelming.

With NetApp, you don't have to be overwhelmed by this shift. You can introduce a ransomware solution that serves as either a full-scale solution or a complement to your existing investments.

Build a modern approach to cyber resilience from the inside out

Let's take a closer look at building a modern approach to cyber resilience for your business, including the solutions that can address the common challenges highlighted above. NetApp cyber-resilience solutions approach these challenges from the inside out, with security and protection solutions designed around your data.

NetApp's portfolio of solutions includes powerful, robust data management, intelligent data and user monitoring, and professional services to help organizations at any stage of their preparation and management.

When your data becomes your primary focus, it's easier to tackle your cyber resilience needs. Your first step is understanding your current state by working through the following questions.

Prevention is the best cure. Put systems in place that identify suspicious activity before it becomes an existential threat, including:

- Where is my data located? In the cloud? On premises? At the edge? In multiple geographies?

- What kind of data do I have?

- What kinds of permissions does my data have?

- How can I quickly identify and block malicious activity?

- How can I ensure that all my data is safe while I determine the blast radius of an attack?

- How can I bring my data and applications back online, in minutes, if an attack occurs?

- How can I investigate the source of a threat so that I have enough information to prevent future similar attempts?

- How can I build protection directly within or around my data so that it can "self-protect" quickly—while we're identifying and addressing a threat? How can I monitor user behavior for suspicious activity across my global network?

By answering all of these questions, you'll create the skeleton for a data-centric cyber-resilience plan that can help your organization prepare for ransomware attacks.

If there are more "Unknown" responses than you're comfortable with, NetApp offers professional services that not only gives you answers but also provides the tools you need to execute your new ransomware protection and recovery plan.

A cyber-resilience plan in action with NetApp

NetApp offers a portfolio of solutions designed to address the needs of IT and security teams to better protect and secure data. Built on a foundation of ONTAP® storage software, we layer data services to enhance visibility, detect threats, and automate response and recovery.

Read on to find out how NetApp, plus a cyber-resilience plan based on answers to the questions just given, can help your team during an actual ransomware attack.

"We recently experienced a ransomware event, and when we saw what Cloud Insights ransomware detection provides, we were sold."

Director of IT, Transportation Company

Identify

Your team needs to know what kind of data you have, whether it is sensitive, and where that data is located in order to better plan what and how you will protect it. NetApp Cloud Data Sense, a software-as-a-service (SaaS) solution, uses artificial intelligence (AI) algorithms for data discovery, mapping, and classification to deliver this information.

Meanwhile, NetApp Cloud Insights, which provides visibility into the hybrid cloud infrastructure, enables your team to monitor and secure your entire environment. And it's a good thing, too, because your defenses are about to be put to the test.

Protect

One morning, your New York–based IT team comes into work and learns that someone in the London office has clicked an unfriendly email link.

Even though no one was around to physically monitor this attack, NetApp FPolicy®, part of NetApp ONTAP data management software, used its Zero-Trust data protection to block known malicious file extensions.

Nevertheless, your hackers persist. They use a compromised user account to infect files through a zero-day malware exploit. More malware taps into several compromised user accounts to encrypt data—slowly, in the hope of avoiding detection.
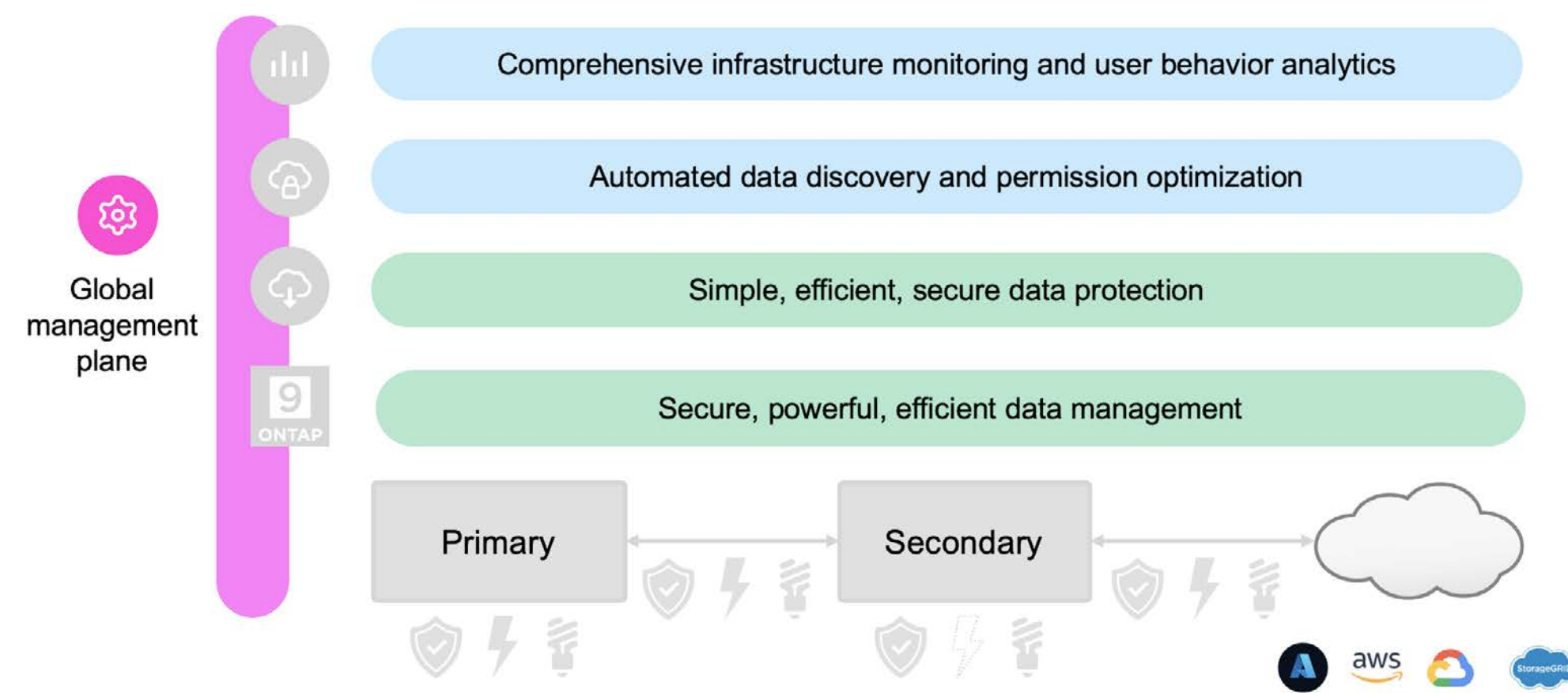
Detect and Respond

Spotting and combating all of this activity would be difficult for a few individuals to do, especially if they're juggling other responsibilities in a different time zone. But the IT team has NetApp Cloud Insights to monitor networked file shares and spot user anomalies. Even if the team doesn't notice the attack, Cloud Insights does and instantly creates a NetApp Snapshot™ copy to protect the data.

Your primary volume may be susceptible to encryption, but your Snapshot copies are immutable and when combined with NetApp Cloud Backup deliver a secure and effective data protection strategy.

Cloud Insights can identify the source of the attack and automatically block the compromised user account to prevent further damage and help prevent data exfiltration.

What about the malware that's slowly moving through your file storage? No problem. An alert is sent thanks to the built-in autonomous ransomware protection in ONTAP, which uses machine learning to monitor workload activity and data entropy. This alert also triggers an automatic Snapshot copy, providing several recovery points.

Phishing scams and email attachments aren't the only threats. Compromised administration credentials, or even worse a rogue administrator, 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.

Global management plane

Comprehensive infrastructure monitoring and user behavior analytics

Automated data discovery and permission optimization

Simple, efficient, secure data protection

Secure, powerful, efficient data management

Primary — Secondary

Restore

With Cloud Data Sense and Cloud Insights, you can apply intelligent file forensics to identify what data was impacted and by whom to focus your data recovery and reduce downtime.

Your IT team can then proceed to restore data rapidly, terabytes in minutes, by using NetApp tools. Logs can be exported to leading security information and event management (SIEM) software for further analysis.

And despite the high drama of the moment, the entire team can rest easy knowing that the recovery of the data was never in question because NetApp SnapLock® software uses secure WORM file locking to prevent data deletion.
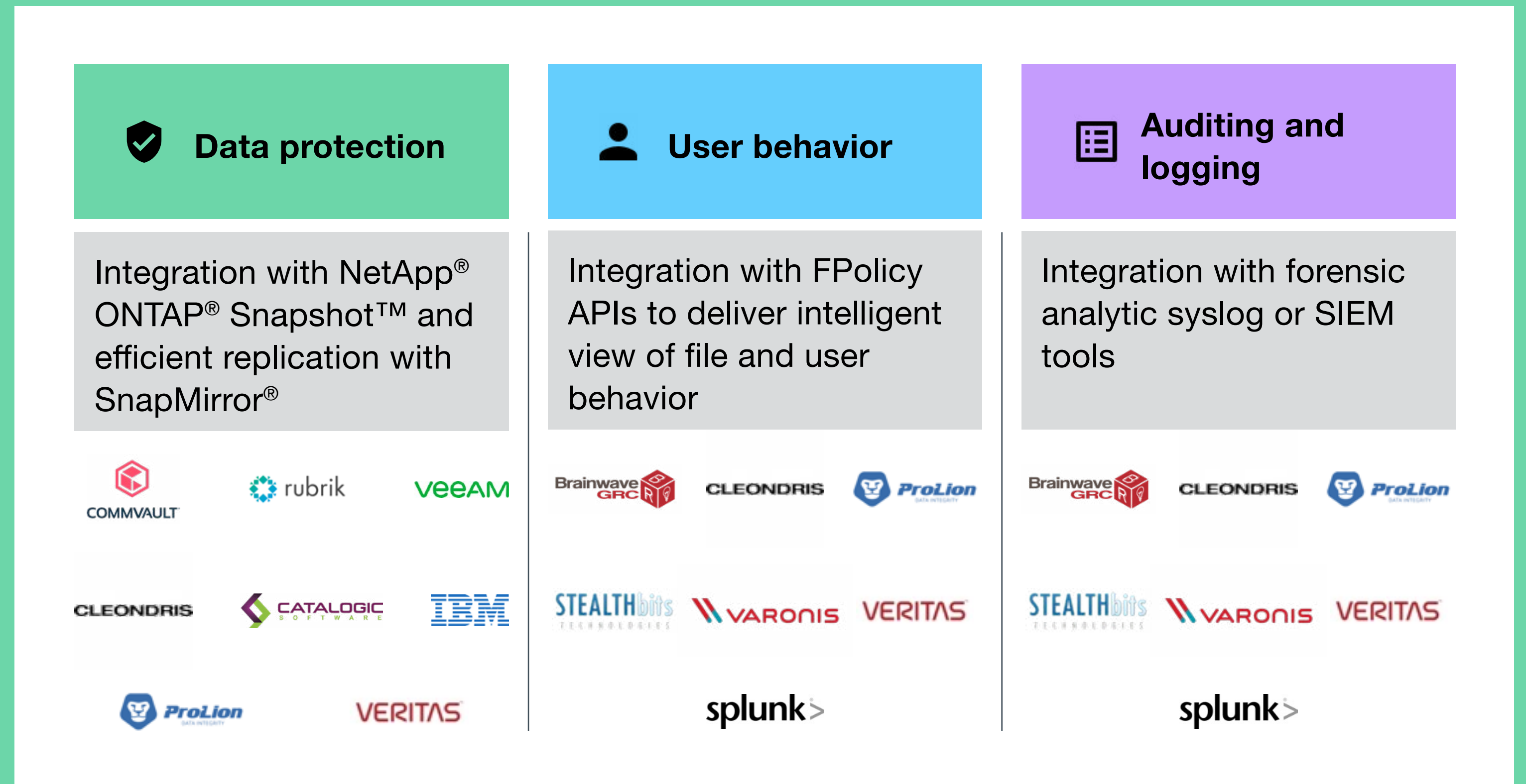
A data-centric cyber-resilience plan no matter where data resides

Does the previous scenario still apply if your IT team manages data on premises? In the cloud? In a hybrid environment? At the edge? Absolutely.

Because cyber resilience is data-centric by design, your data is always fully secure, resilient, and available no matter where it resides—on premises, at a remote location, or in the cloud. The NetApp cyber-resilience solution spans the hybrid cloud and integrates with every major public cloud.

Make the most of your existing investment

The data-centric NetApp cyber-resilience solution can assist with all five stages of the plan we've outlined here. But your organization might have already made investments into cybersecurity tools. The NetApp ONTAP software features can integrate with existing cybersecurity investments, so you can close gaps instead of starting completely from scratch.

🛡 Data protection	👤 User behavior	▤ Auditing and logging
Integration with NetApp® ONTAP® Snapshot™ and efficient replication with SnapMirror®	Integration with FPolicy APIs to deliver intelligent view of file and user behavior	Integration with forensic analytic syslog or SIEM tools
COMMVAULT rubrik veeAM	Brainwave GRC CLEONDRIS ProLion	Brainwave GRC CLEONDRIS ProLion
CLEONDRIS CATALOGIC SOFTWARE IBM	STEALTHbits VARONIS VERITAS	STEALTHbits VARONIS VERITAS
ProLion VERITAS	splunk>	splunk>

Your cyber-resilience plan is just a few clicks away

We can't eliminate criminals, but we can activate your organization's cyber-resilience with the right tools.

→ Learn more about how NetApp can help put your data-centric cyber-resilience plan into action. **netapp.com/cyber-resilience/**

Click the links below to see the latest NetApp cyber-resilience solutions, blogs, and videos
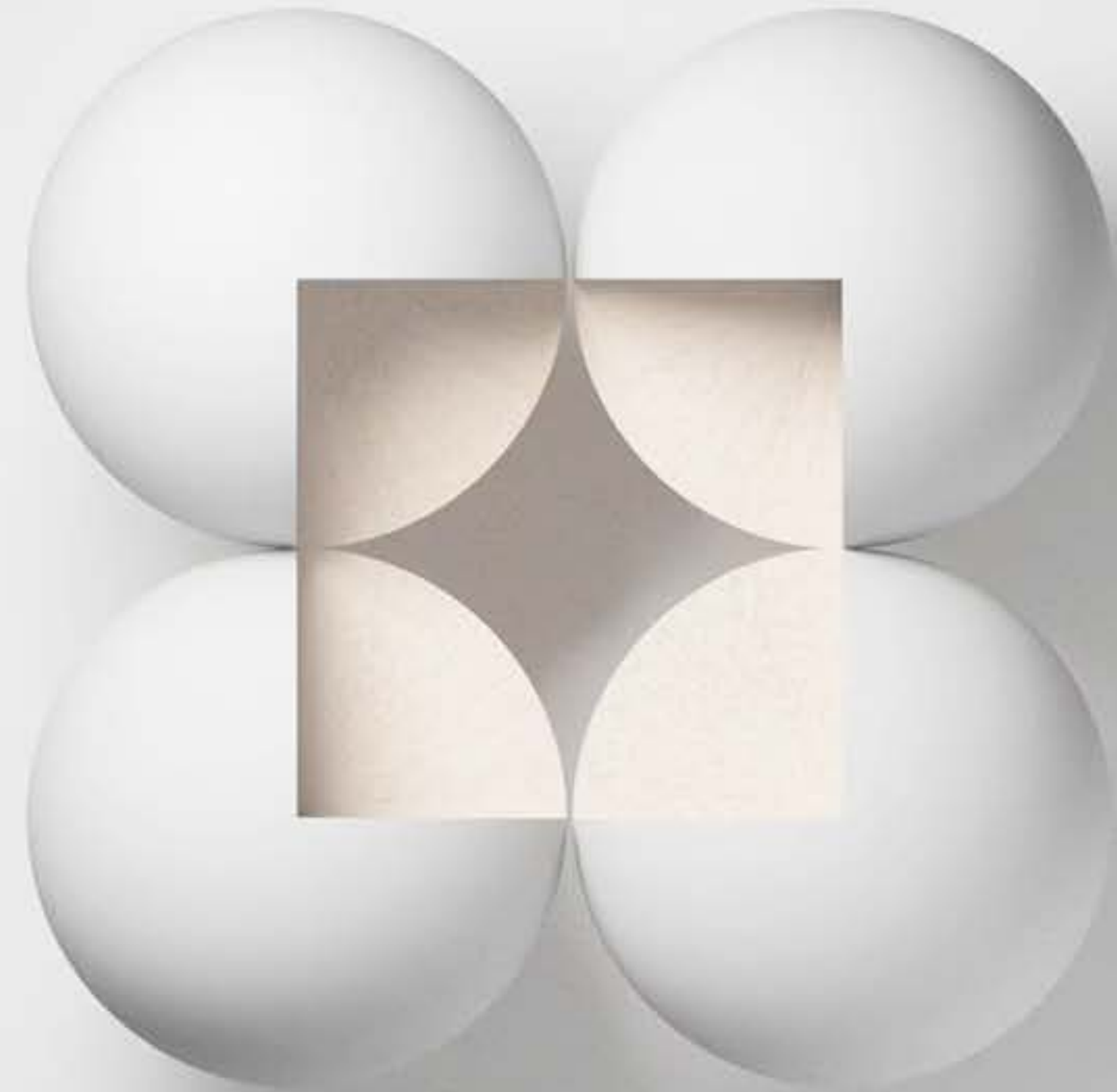
🛡 [NetApp cyber-resilience solutions](#)

🔒 [NetApp data protection solutions](#)

🔓 [NetApp ransomware solutions](#)

📶 [NetApp cyber-resilience blogs](#)

▶ [NetApp.tv cyber-resilience videos](#)

1. National Institute for Standards and Technology, "Developing Cyber-Resilient Systems," December 2021.
2. PBS NewsHour, "Why ransomware attacks are on the rise—and what can be done to stop them," July 8, 2021.
3. Business Wire, "Ransomware Index Spotlight Report Reveals Steady Increase in Sophistication and Volume of New Ransomware Vulnerabilities and Families in Q3 2021," November 9, 2021.
4. Statista, "Methods of organizations compromised by ransomware to get their encrypted data back as of February 2021," 2021.
5. Sophos News, "The State of Ransomware 2021," April 27, 2021.
6. Deloitte, "Double extortion incidents," October 2020.
7. Infosec, "NIST CSF: Implementing NIST CSF," February 19, 2020.

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

📺 🐦 in f ▶   +1 877 263 8277