E-BOOK

Cyber resilience: Real stories of data loss and how to protect your company

n NetApp | Google Cloud

Contents

Introduction

In today's IT world, we often replace the word "landscape" with "threatscape."

If you're an information technology professional, you know that you and your company are facing digital danger at every turn. Whether it's a result of malicious intent or employee error, a breach can cost thousands or even millions of dollars to correct. It can damage brand and reputation, alienate customers, and sometimes even take a company down.

At the same time, IT budgets are shrinking and skilled resources are in short supply. The demands on IT professionals have never been greater. This is not a problem that any one person or company can tackle on their own.

At NetApp, we spend a lot of our time thinking about data—how to protect it, secure it, and make it always available for our customers, without worry. To do this, we partner with the most powerful technology giants in the world. One of those giants is Google Cloud.

This e-book features three true stories of customers who suffered serious breaches that impacted their lives and the lives of their customers. We've disguised the companies to protect the innocent, but you'll recognize the scenarios. They're playing out every day around the world—they might even be playing out in your company this very minute.

In this e-book, we identify the greatest threats to your business and how to look out for them. We share how

NetApp and Google Cloud reduce the risk of threats turning into breaches. We've also linked to a self-assessment questionnaire to help you better understand the current status of your cyber-resilience operation and how you can improve it.

If you are looking for greater protection and a partner that has multiple strategies and tools to help, look no further than NetApp. Now, with NetApp BlueXP™, we're delivering a unified control plane, an intuitive interface, and powerful automation to simplify your operations—across Google Cloud and on premises—to further reduce your risk.

The NetApp Cyber Resilience Team

Three cries for help

Holly Hudson*, CEO of a midsize manufacturing plant that supplies parts to the auto industry, had already navigated a tough year due to supply chain issues and chip shortages. When she arrived at work on Monday morning, she was shocked to see the image of a skull and crossbones on her laptop screen.

"Your system has been hacked and you need to pay $50,000 to unlock your data." Holly's managed service provider (MSP) was unable to help. Holly made the payment and fired her MSP the same week.

* Name changed

Vijay Patel* had spent more than ten years climbing the IT ladder at his organization.

Beginning as an intern right out of university, his career had grown along with his company's good fortunes. Poised for promotion to Director of IT just as his organization was ready to cross into $1B in revenue, his latest project had been to consolidate their business continuity plans and negotiate SLAs with all business units.

A massive outage at the company's primary data center would test IT's ability to recover; but with a government request-for-proposal deadline looming, the 24-hour recovery time objective might as well have been two months. The bid team was not able to access the systems that housed their bid response in time to meet the government deadline. As a result, their submission lacked crucial information and they didn't even make the first cut in the tender process for a project they had been slated to win. The new Director of IT was hired from outside the company.
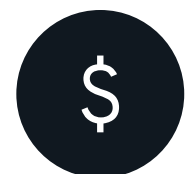
* Name changed

∩ NetApp

The first hint that something was wrong appeared in the forecast reports.

Amy Pho*, controller at a large telecom supplier, noticed that the sales forecast and close rates were widening. It didn't make sense. For years, the company had been on a steady growth curve, and new 5G technologies meant their proprietary solutions were in more demand than ever. They had great customers and an even greater reputation.

Digging further, Amy learned they were losing most of their deals to a competitor. Although the competing organization was fairly young, its technology—which looked suspiciously like the telecom supplier's own—was very sophisticated. A forensics security team was formed to investigate. The results were worse than anyone expected. An intruder, masked as the company's CEO and using her credentials, had been in their network for more than two years, downloading sensitive engineering documents that were not encrypted or secured. Millions of dollars in research and advanced technology had been leaked through poor security practices. Within 12 months, Amy's company was forced into Chapter 11.

* Name changed

The rise of cyber resilience

Organizations are under tremendous pressure to protect their data and applications from cyberthreats. Consider the following:

Cyberattacks are getting easier and cheaper for criminals, but more dangerous and expensive for businesses.

According to a survey by Sophos, over the past year **72%** of organizations in 31 countries saw an increase in the volume, complexity, or impact of cyberattacks.

According to *Cybercrime Magazine,* a ransomware attack happens **every 11 seconds** worldwide.

Recovering from a ransomware attack costs **$1.4 million** on average (Sophos study).

The average victim loses **39%** of their data (Sophos study).

The average time to recover from an attack is **one month** (Sophos study).

This threatscape has given rise to a practice called cyber resilience.

Cyber resilience is a combination of traditional IT security technologies and tools coupled with data protection. Strong governance, policies, and procedures are integral to the success of this approach.
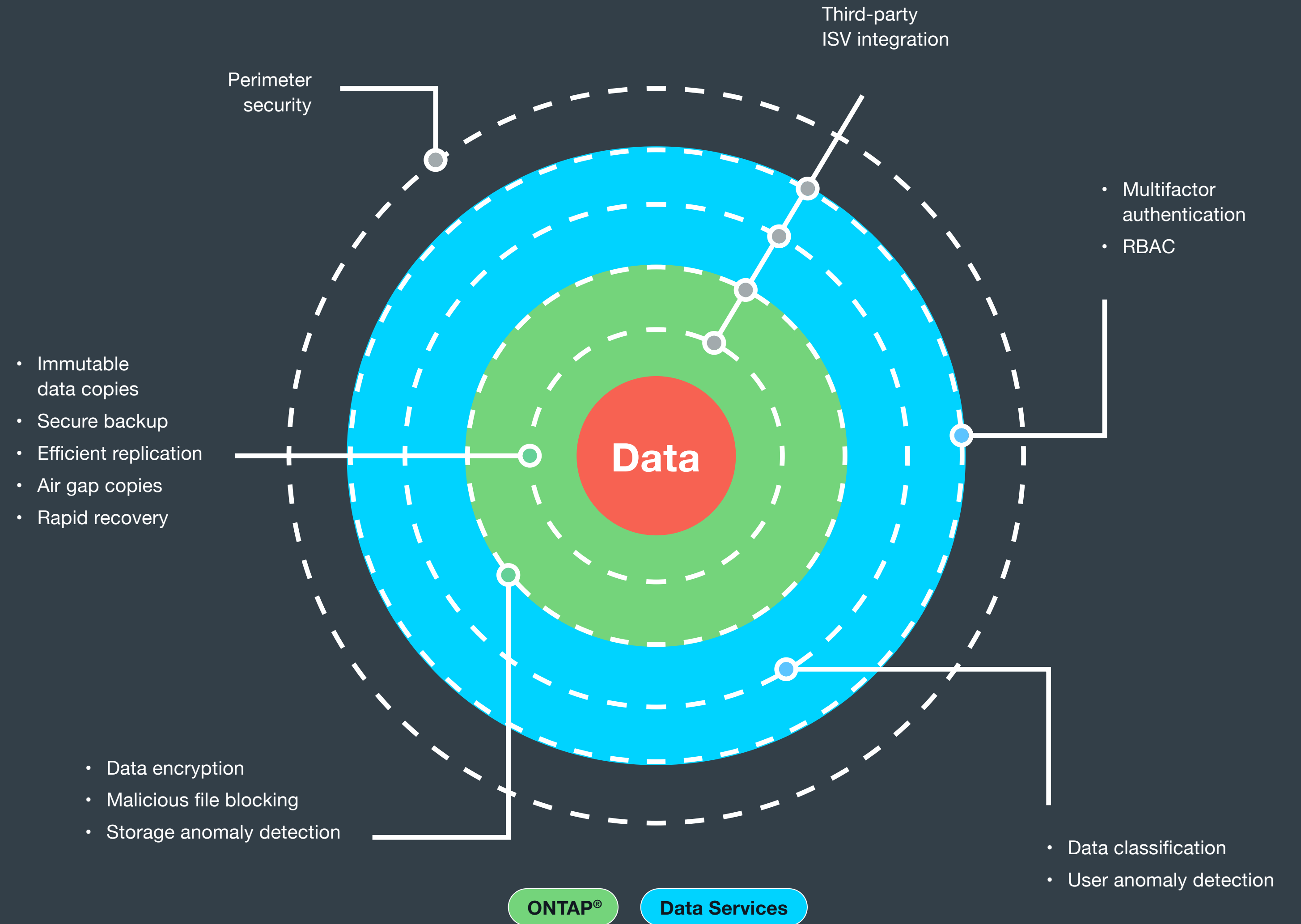
When done well, a cyber-resilience strategy can prevent stories like Vijay's and Holly's from ever materializing, by reducing reliance on a set of point solutions that don't integrate with or support one another. Even if your perimeter is breached, an employee unwittingly leaves a virtual door open, or an intruder takes malicious action, with the right methods and tools, your data will be protected. You will have implemented an intentional strategy that includes an overarching and connected data protection plan, designed for this new world.

It's important to prevent intrusions by insulating your data from those who shouldn't have access—using firewalls, encryption, the principle of least privilege, and write-once, read-many (WORM) file locking. But your main goal is to protect what's **behind** that firewall: your data. It's a new mindset. Instead of starting from the outside (at the perimeter or microperimeters) and working in, cyber resilience begins behind the walls. It starts at the level of your data.

■ NetApp

Building a Zero Trust cyber resilience landscape

NetApp approaches cyber resilience with your data at the center. Criminals are targeting your data. They want to steal it, expose it, or prevent you from using it. Having the right solutions is crucial to ensuring that your data is protected so you can detect threats and recover quickly from attacks.

Our cyber-resilience solution begins with data protection, detection, and recovery at the storage layer. We specialize in storing, accessing, protecting, and moving data. Protection and security are not afterthoughts; they are built into the DNA of every solution we deliver with Google Cloud.

Perimeter security

Third-party ISV integration

- Multifactor authentication
- RBAC

Data

- Immutable data copies
- Secure backup
- Efficient replication
- Air gap copies
- Rapid recovery

- Data encryption
- Malicious file blocking
- Storage anomaly detection

- Data classification
- User anomaly detection

ONTAP®   Data Services

NetApp ONTAP data management software managed via NetApp BlueXP™ offers additional features and capabilities that protect your data where it's stored, such as:

- NetApp Snapshot™ copies to provide rapid and granular data recovery, preventing encryption by malware

- Cross-region replication for backup and disaster recovery

- Cloud WORM storage, powered by the SnapLock® feature of ONTAP, which provides indelible copies that can be used for secure data retention and as a logical air gap

- In-flight and at-rest data encryption

- Policy identifiers to limit user access to data and prevent malicious files from being written to disk

- Layered additional intelligent data services that add even more protection, by scanning through all your file and object data stores to identify sensitive data, where it is located, and who has permission to access it

One important capability in Cloud Volumes ONTAP for Google Cloud enables you to make sure that file shares are being accessed only via NFS and SMB on the network to which they are attached. By default, such networks are isolated in Google Cloud and cannot be easily accessed from the outside. On top of network isolation, NetApp's export policies and Kerberos authentication can be used to restrict access to the network.

We also take advantage of Google Cloud projects to compartmentalize workloads and limit the "blast radius" of security breaches. Managing services on a per-project level instead of as on one, big, central data lake also limits the scale of data leaks, deletions, or loss, while backup and replication mechanisms provide additional protection.

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

Director of IT, Transportation Company

Protect your data.
Protect your business.

A data-centric approach to address the challenges of cyberthreats and availability

The right tools for the job
NetApp BlueXP and ONTAP cyber-resilience capabilities deliver leading data protection and security.

Protect	Detect	Recover
Eliminate the threat of ransomware attacks and unplanned data loss	Quickly identify threats before they impact operations	Rapidly restore data and accelerate application uptime
Thwart ransomware attacks and prevent unplanned data loss: • Block malicious files • Establish rapid, granular recovery points • Efficiently replicate data for backup and disaster recovery • Create a logical air gap and flexible secure data retention • Identify and correct security exposures on your storage systems • Learn normal user file-access behavior • Categorize and locate sensitive data • Identify file access permissions	Quickly identify threats before they become a problem: • Trigger alerts based on storage behavior • Detect data and storage anomalies • Gain visibility into unusual user directory performance metrics • Identify change in user file-access patterns • Detect attempted mass file deletions	Restore data rapidly and accelerate application uptime: • Recover data in minutes, locally or remotely • Apply file-level forensics • Initiate NetApp® Snapshot™ recovery point • Block malicious user accounts • Provide forensic data to identify which files to restore

Financial services firm moving from on-premises data center to the cloud

This client is a midsize firm in the financial services sector that provides data management and analysis of data to deliver real-time, high-value business insights to their customers across mortgages, properties, and other assets for consumer and business lending. Because its core business is ingesting, manipulating, analyzing, and reporting on data, it was crucial for them to find a cyber-resilience solution that offered the least amount of risk and the highest level of security.

Google Cloud for performance

Although this customer had never worked with NetApp before, it recognized that its existing storage and data management provider did not have the levels of security needed to move to the cloud. It also required consistently high performance. The client decided to use Google Cloud to house its enterprise applications. Google recommended NetApp® Cloud Volumes ONTAP.

NetApp all the way

NetApp Cloud Volumes ONTAP addressed this customer's strict requirements for rapid disaster recovery, compliance, and governance. With NetApp and Google Cloud, the company built a highly available failover business continuity architecture using features such as cross-region replication to build redundancy. It gained ransomware threat management and the highest level of security. Additionally, NetApp delivered architecture, training, and knowledge transfer throughout the project, leaving nothing to chance.

NetApp

"When we moved to Google Cloud with NetApp, we did not experience any performance degradation from our on-premises data center. We are able to test our business continuity quarterly and have had no loss of data. Our confidence that our business is completely protected with NetApp on Google Cloud is a ten out of ten."

Senior Director of IT, Financial Services Company

Take the readiness assessment

How resilient are you?
Every organization is on a cyber-resilience journey, and almost every enterprise has at least one gap area. To understand where you are today and what some of your gaps might be, take our self-assessment. It also provides you with recommendations and suggestions for next steps.

Take the readiness assessment →

Want to learn more?

Schedule a 1:1 consultation with a NetApp specialist →

Read our e-book: Protect your data with NetApp and Google Cloud →

Read more about NetApp Snapshot technology →

See the NetApp Google Cloud cyber-resilience overview →

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