arcserve®

Building a Ransomware-Proof Organization: Data Protection, Immutability, Air Gapping, and Zero Trust

Table of Contents

Data Protection and Management: 4 Trends You Need to Know About

By Ivan Pittaluga, CTO, Arcserve

In today's hyper-connected digital economy, protecting your data from damage, destruction, or a cyberattack is more critical than ever. The very survival of your business may depend on it. But managing and protecting your business data isn't easy. You need to be aware of ever-evolving privacy regulations and security threats that could come at you from anywhere in the world. With that in mind, four trends are shaping how companies approach data protection and management as we move through 2022.

1. Attack Surfaces Continue to Increase as Hybrid Workplaces Evolve

To get a sense of your potential vulnerabilities, consider that your attack surface includes every possible way an attacker can get into your company's devices and networks. Once inside, they can lock up or exfiltrate your data. That's why it's essential to keep your attack surface to a minimum. But the challenge is that your attack surface is probably growing as more people work remotely and others choose a hybrid where they spend time both in the office and at home. And everyone is using multiple devices.

That creates more entry points for cybercriminals to carry out cyberattacks. Even worse, the attack surface constantly changes because of its many disparate fragments and not a single surface. Add to that the increasing complexity that comes with controlling endpoints, as retrieving company equipment can be more complicated when employees leave organizations today.

The bottom line? Breaches are an inevitability. So, everyone needs to do a better job of recognizing breaches so they can extricate themselves as quickly as possible. With more exposed attack surfaces, your

security and recovery strategies need to be more thorough, providing protection not just for your on-premises data, but also your data in the cloud, at the edge, and everywhere in between.

2. Data Management Is More Complex Due to Data Sovereignty Requirements

As companies go global and become more interconnected, the rules around data privacy have become more complicated. A company in Germany may use a US-based company like Amazon or Google to store and send data. Where does that German company's data legally reside, and by what rules is it governed?

The answers to these questions are not straightforward. Global IT, legal, and HR experts continue to passionately discuss how to interpret our constantly evolving data processing reality. That's why 86 percent of IT decision-makers say their organizations have been impacted by changing compliance requirements surrounding data privacy, according to a global survey conducted by Dimensional Research.

Companies no longer have a single data lake that IT can focus on protecting at their corporate headquarters. These days, much of their data, probably like yours, resides in the cloud. That translates to a globally distributed data infrastructure. And a global footprint demands tracking data sovereignty issues in different jurisdictions. Expert help in meeting these requirements is usually necessary, and cloud providers need to work more closely with their customers to manage sovereignty and comply with varying rules.

Now, the onus is on both businesses and cloud providers to address compliance and data sovereignty issues by understanding the petabytes of data that are being stored and the regulations surrounding every aspect of that data. That demands getting smart about your data content and putting sound policies in place around that content.

3. Data Protection Is Part of the Global Supply Chain Issue

Supply-chain issues are causing significant disruptions to the global economy, with everything from cars and refrigerators to semiconductors and toys in short supply. These issues don't look like they will go away any time soon. And a

survey of CFOs compiled by Duke University's Fuqua School of Business and the Federal Reserve Banks of Richmond and Atlanta confirms that expectation, with a majority saying they don't expect these issues to be fixed until the second half of this year or later.

Logistics issues and digital risks are everywhere. Cyberattacks are on the rise—like the one that struck Colonial Pipeline last year, bringing down the largest fuel pipeline in the United States and temporarily causing fuel shortages along the East Coast while costing the company a substantial ransom. That means the supply chain must remain one of your top priorities. You need to have data protections in place that ensure your company's supply chain keeps moving with data available 24/7 and instantly recoverable.

4. Data Protection Officers are a Strategic Advantage

The data protection officer (DPO) is an enterprise security leadership role that, under certain conditions, is required by the General Data Protection Regulation (GDPR). And according to recent GDPR stats, the demand for DPOs has risen by more than 700 percent over the last five years. DPOs are responsible for providing expert knowledge of data protection laws and practices while overseeing their company's data protection strategy and ensuring compliance with GDPR requirements.

The role of the DPO is continuing to grow in importance as responsibilities extend beyond traditional IT to encompass a holistic view of data, security, and education. The DPO can even open new opportunities across your organization, with our hybrid workplace, where the DPO is a strategic enabler for business success, being just one example.

Data protection isn't going to get any easier. As your company stores more data across on-premises, cloud, hybrid, and third-party systems—and as data regulations multiply—you need to stay on top of the ever-evolving data landscape or face potentially harrowing consequences.

Learn more about Arcserve data protection solutions.

Data Storage: An Integral Part of Every CISO's IT Security Strategy

By Florian Malecki, Executive Vice President, Marketing, Arcserve

Ransomware is on every IT pro's mind these days. In a recent survey conducted by Dimensional Research, 96 percent of IT decision-makers reported worrying about ransomware. Just one in five of those respondents said they are very confident they could recover from a ransomware attack. Another study by Sophos supports these concerns: 37 percent of respondents—all IT decision-makers—said they were hit by ransomware the previous year, and 54 percent said the cybercriminals succeeded in encrypting their data.

As ransomware attacks become increasingly sophisticated, CISOs have ramped up their protection and attack prevention solutions, including firewalls, identity and access management, and password hygiene. But data storage is still a challenge.

Your Last Line of Defense: Data Backup and Storage Solutions

If your company falls victim to a cyberattack, every second your systems are down is costly and painful. Over 60 percent of Uptime Institute's 2021 Global Data Center Survey respondents reported losing more than $100,000 to downtime. Of that, 60 percent lost over $1 million. While the prevention measures noted above are essential for security, CISOs also need data protection if they are going to meet their primary requirements: data security and availability. Achieving that goal depends on a sound backup and storage solution.

Data backup and storage solutions are the foundation of business operations. That makes them a prime target for hackers. And that should also make them your top priority as you develop your data security policies. An effective backup and immutable storage solution protects your data if you suffer an attack—or any other business disaster. Think of data backup and storage as your last line of defense, ensuring data security and availability no matter what.

Why Immutable Storage Matters

Strengthening your data resilience takes a holistic approach to data security. A crucial element of that approach is immutable data storage. While you can never stop cyberattacks, you can neutralize their effects by ensuring business continuity.

The most important step you can take to protect your company against ransomware is to back up your files regularly to an immutable storage solution. An immutable snapshot is a copy of your data that ransomware—or any user—can't modify or delete. The most sophisticated snapshots let you encrypt both your files and your recovery points. That means you can quickly recover data written to these immutable storage solutions, whether the cause of the disaster is data corruption, accidental deletion, a ransomware attack, or a data breach.

These data backup and storage solutions also let your users independently recover their data simply by looking through their files on Windows Explorer or Finder on a Mac. They don't have to recover data using the previous day's backup. They simply find and select the data they want to restore. You'll find these features—and more—are offered by Arcserve OneXafe. OneXafe also gives you inline deduplication and compression, reducing your data footprint and storage costs.

Keep Data Storage at the Top of Your Priority List

While ensuring your team is on top of evolving security risks is your top priority, CISOs also need to stay aware of their data storage because data is critical to success. But many data security policies are limited to basic guidelines that don't cut it in the real world, where attacks continue to increase in volume. Hackers are getting rich thanks to unprotected businesses. You need to stay vigilant because it's most likely "when" and not "if" you will be attacked.

Change Your Approach

If you aren't sure your company is ready for any data disaster that comes your way, it's time for a new data protection approach. Find an expert Arcserve technology partner to help you get there. Or contact us for more details about Arcserve's extensive portfolio of data protection solutions.

Tape Air Gapping Cybersecurity: Key Ransomware Defense Solution

Arcserve has introduced an enhanced version of its widely adopted tape air gapping solution, Arcserve Backup 19. Arcserve Backup 19 tape backup software improves performance, security, and reliability over prior releases. With Arcserve Backup 19 air gapping technology, you get a last line of defense against ransomware by physically disconnecting your digital assets from network connections.

As we wrote in a recent post, tape backup is experiencing a renaissance in the digital era because it may be a wise choice when weighing all of your backup options. And the Enterprise Storage Forum recently made a strong case for the resurgence of tape backup solutions. Now, Arcserve Backup 19 gives you even more reasons to give tape another look.

With these enhancements, the Arcserve Backup 19 solution has been migrated to an updated development platform that improves performance and reliability. Security has also been strengthened with Federal Information Processing Standards (FIPS)-compliant secure communication updates and crypto libraries for customers who require military-grade encryption.

Arcserve Backup 19 now certifies and adds broad support for the most popular platforms deployed in customer environments, including compatibility with:

- Windows Server 2022
- Windows Server 2022 Hyper-V
- SharePoint Server 2019
- Oracle Database 19c on IBM AIX, Solaris, and HP-UX
- AlmaLinux 8.x

- Rocky Linux 8.x
- Free BSD 13.x
- macOS Catalina (version 10.15.x)
- Debian 11.x
- Red Hat Enterprise Linux 8.x for IBM Z® (Mainframe)
- Default Arcserve Backup Database (ASDB) upgraded from Microsoft® SQL Server® 2014 Service Pack 2 (SP2) Express to Microsoft SQL Server 2019 Express

Arcserve has been the market leader in tape-based data protection for decades. With over sixty certified vendors, the company offers the broadest and deepest support for tape-based media.

"Tape air gapping is emerging as the most important 'last line of defense' from ransomware attacks." Said Florian Malecki, executive vice president of marketing at Arcserve. "While most vendors don't handle tape due to its complexity, Arcserve has been leading the market with this technology for decades. This gives us the unique ability to provide customers a complete 3-2-1-1 ransomware defense and recovery solution including on-prem, immutable storage, cloud services, and tape backup."

Learn more about Arcserve tape backup software solutions, or find an expert Arcserve technology partner to provide you with expert guidance as you improve your data protection, backup, and disaster recovery capabilities.

How a Zero Trust Cybersecurity Approach Can Protect Your Data and Ensure Data Recovery

Gartner defines zero-trust network access as a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. Tech Target puts it more simply, stating that the zero-trust cybersecurity model assumes that no user that is allowed onto your network should be trusted by default because they could be compromised.

A zero-trust approach requires identity and device authentication throughout your network—not just at the perimeter. Think of zero trust as locked doors at every access point, demanding the right key and authorization for anyone to gain entry.

That's incredibly important, considering that 85 percent of all breaches involve the human element. All it takes is one person in your organization clicking on a malicious link or downloading an infected PDF to immediately put your network and your data at risk from malware and ransomware. With social engineering schemes becoming ever more sophisticated, a recent Tech Target article says some attacks are so well crafted that they even fool security researchers.

Zero Trust: Bolstering Your Frontline Defenses

As part of its efforts to fortify the US against cyberattacks, the National Security Agency (NSA) recommends that organizations embrace a zero-trust security model. The NSA defines the model as "a coordinated cybersecurity and system management strategy based on an acknowledgment that threats exist both inside and outside traditional network boundaries."

When you move to a zero-trust model, you continuously limit access by anyone only to what is needed. And zero trust includes monitoring for unusual or malicious activities, granular risk-based access controls (RBAC), and automated, coordinated system security throughout your infrastructure. You should also put an added focus on protecting critical data in real-time.

Going back to the human element, a successful zero-trust security model requires that everyone within your organization, from the top down, understands and commits to zero-trust principles.

Foundational Concepts of Zero Trust

The NSA has published high-level guidelines that should serve as the basis for your decisions as you move to a zero-trust model, including:

- Never trust; always verify
- All users, devices, apps, workloads, and data are treated as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
- Assume a breach has occurred
- IT teams need to start with the assumption that they have already been breached and operate and defend accordingly. Every attempt at access by every user, data flow, device, and request should be denied by default. All configuration changes, resource accesses, and network traffic should be monitored, logged, and inspected for malicious activity.
- Verify everyone
- Use a consistent, secure approach with multiple dynamic and static attributes to increase confidence that access to resources is limited based on contextual factors.

Building a Zero Trust Solution

The NSA also shares some core concepts that should form the basis of your zero-trust strategy, including:

- Set clear objectives: Your zero-trust architecture needs to meet your organization's specific requirements, including identifying your critical data, assets, applications, and services.
- Start inside: Your first step is to protect the components of your architecture listed above. Your next step is to secure all access to these components.
- Decide privileges: Create security policies and apply them consistently across your environments—local area networks (LANs), wide-area networks (WANs), endpoints, perimeters, users, and devices.

- Gain visibility: Put a solution in place that gives you complete visibility into all activity throughout your network architecture to enable analytics that detect suspicious activity and let you inspect and log all activity before taking action.

Zero Trust Includes Your Backup Solution

With hackers targeting backups with much greater frequency so they can prevent your organization from recovering from an attack, protecting your backups is more critical than ever. We designed Arcserve UDP to support zero-trust security strategies and minimize exposure of essential data backups to external threats.

Arcserve UDP and Zero Trust

Arcserve UDP prevents unwanted access by including extended default and customizable configuration. The solution's features also ensure that only authorized users can access your data backups and your data protection infrastructure. Arcserve UDP can enable access to local users or can be integrated with your organization's Active Directory deployment to simplify user management.

UDP also leverages zero-trust principles throughout the platform to protect your backups, including:

- Only admins can use Arcserve UDP Agents and the recovery point server (RPS) by default, with strict authentication required for every access.
- Advanced RBAC functionality lets you assign one of the pre-defined admin, backup, restore, or monitor roles to users. Or you can choose to define a new role with a set of permissions that controls access to more than three dozen individual features.
- In Linux environments, Arcserve UDP components can operate under non-root user IDs and use the SuperUser DO (Sudo) command when administrative privileges are required.

Beyond Zero Trust: Isolating Your Backup Infrastructure

Arcserve UDP is, for the most part, self-sufficient, designed to operate in isolated environments. This approach adds further support to your zero-trust strategy by monitoring and minimizing access to your backup data so you can recover in the event of a disaster, including:

- Exceptionally few primarily non-standard TCP ports must be open for secure communication between Arcserve UDP's components, and all other operations are performed locally on the protected systems and RPS.
- A web-based interface operates over HTTPS and doesn't require opening potentially unsecured ports such as remote desktop protocol (RDP).
- The only automated external internet queries are periodic checks for updates. If the environment is secure and completely isolated, the check can be disabled to prevent outbound connection attempt alerts from firewall solutions.
- Arcserve recommends that Arcserve UDP servers should not be integrated with larger Active Directories to minimize the potential attack surface of the data protection infrastructure.

Arcserve also recommends limiting direct connections between networks to required ports when backups are replicated to remote sites or the cloud—TCP/8014 to replicate data and TCP/8015 for centralized management. This minimizes exposure of secondary backup copies of your data if your primary site is attacked by hackers or locked up by ransomware.

Monitoring for Maximum Security

With advanced monitoring functionality, Arcserve UDP lets your backup admins react quickly to investigate any aspect of backup infrastructure operations—including security—by offering:

- Ad-hoc, as needed and emailed, scheduled reports regarding your Arcserve UDP deployment.
- Automated email alerts for most backup operations so you can quickly address any issues.
- Comprehensive job logs that include all necessary information required to investigate backup and infrastructure anomalies. Arcserve UDP also alerts backup admins when an issue arises without logging in to the management console.

Make the Move to Zero Trust

Arcserve is a strong supporter of the zero-trust model. To find out how you can put a zero-trust strategy in place, choose one of our expert technology partners or contact us for more product details.

Need Answers?

Arcserve is always here—standing by and ready to help.

arcserve®

+1 844 639-6792

arcserve.com