arcserve®

Ensuring Data Resilience and Cyber Resilience With Unified Data Protection and Immutable Storage

Table of Contents

ChatGPT and Data Resilience: AI Adds to Business Cybersecurity Risks

ChatGPT is the fastest-growing app in history, reaching 100 million active users in just two months. For comparison, it took TikTok nine months to build that big of an audience. This powerful, open-source tool does whatever you ask it to, from writing school essays to drafting legal agreements to solving complex math problems. It also has the potential to revolutionize the way businesses operate.

With ChatGPT, you can generate reports quickly and handle customer service requests efficiently. The software can even write code for your next product offering, conduct a market analysis, and help build your company website.

While ChatGPT offers many business benefits, it also raises some urgent security questions. That's because ChatGPT makes it possible for cybercriminals with no coding experience to create and deploy malicious software. That opens the door for anyone with bad intentions to quickly develop and then unleash malware that wreaks havoc on companies.

Security firm Check Point Research reported that, within weeks of ChatGPT's release, individuals in cybercrime forums, including those with limited coding skills, used the tool to create software and emails for espionage, ransomware attacks, and malicious spamming. Check Points says it's still too early to tell if ChatGPT will become the go-to tool among dark web dwellers, but cybercriminals have already shown strong interest in ChatGPT and are already using it to develop malicious code.

In one example cited by Check Point, a malware creator revealed in a cybercriminal forum that they were using ChatGPT to replicate well-known malware strains and techniques. As evidence, the individual shared the code for a Python-based information stealer that they developed using ChatGPT. The stealer searches, copies, and transfers 12 common file types from a compromised system, including Microsoft Office documents, PDFs, and images.

ChatGPT Increases Your Exposure to Attacks

Bad actors can use ChatGPT and other AI writing tools to increase the effectiveness of phishing scams. Traditional phishing messages are often easily recognizable because they are written in clumsy English. But ChatGPT can fix this. Mashable tested ChatGPT's ability in this area by asking it to edit a phishing email. Not only did it quickly improve and refine the language, but it also went a step further and blackmailed the hypothetical recipient without being prompted to do so.

While OpenAI says it has strict policies and technical measures to protect user data and privacy, the truth is that these may not be enough. ChatGPT scrapes data from the web—potentially data from your own company—which brings security risks. For instance, data scraping can result in sensitive information, such as trade secrets and financial data, being exposed to competitors. Your reputation can also be damaged if the scraped information is inaccurate. Moreover, when data is scraped, it can open your systems to vulnerabilities that malicious actors can exploit.

Given that the attack surface has dramatically expanded with the advent of ChatGPT, what impact does this have on your security posture? Before, small and mid-sized businesses may have felt secure, thinking they weren't worth the bother of an attack. But, because ChatGPT is making it easier to create malicious code at scale, everyone's exposure to cybercrime has significantly increased.

ChatGPT demonstrates that while the number of security tools available to protect you may be increasing, these tools may not be able to keep pace with emerging AI technologies that could increase your vulnerability to security threats. Given the spiraling impacts of cybercrime, your business needs to be aware of the potential risks posed by ChatGPT and other advanced AI systems—and take steps to minimize those risks.

Data Protection in the Age of ChatGPT

Your first step is to understand just how vulnerable you are. Penetration testing, also known as pen testing, can help protect your data by simulating a real-world attack on your company's systems, networks, or applications.

This exercise aims to identify security vulnerabilities that malicious actors could exploit. By exposing your weaknesses in a controlled environment, pen testing lets you find and fix those weaknesses, improve your security posture, and reduce the risk of a successful data breach or other cyberattack. In the age of ChatGPT, penetration testing can play a crucial role in helping you safeguard your data and ensure its confidentiality, integrity, and availability.

You also need to double down on your data resilience strategy. That includes having a solid data protection and disaster recovery plan in place. Your data resilience strategy defines how you will protect critical data and systems and restore normal operations as quickly and efficiently as possible if a data breach occurs.

Your disaster recovery plan provides a roadmap for responding to cybersecurity threats, including detailed instructions for securing your systems, backing up data, and communicating with stakeholders during and after an incident. By putting a disaster recovery plan in place, you can minimize the impact of cybersecurity threats and reduce the risk of data loss, helping to ensure your organization's ongoing success and survival.

Another way of stopping ChatGPT-enabled bad guys is through immutable data storage. Immutable backups are converted to a write-once-read-many-times format that can't be deleted or altered. There isn't any way to reverse the immutability, which ensures that all your backups are secure, accessible, and recoverable. Even if attackers gain full access to your network, they still can't do anything to the immutable copies of your data.

Understand Your Options

While ChatGPT offers benefits to businesses, it also poses significant security risks. You must be aware of these risks and take steps to minimize them. You should invest in solid cybersecurity measures and stay informed about the latest security trends. By putting the proper protection in place, you can realize the many benefits of ChatGPT while defending yourself against those who use the tool for malicious purposes.

Get help navigating data protection in the age of ChatGPT by talking to an expert Arcserve technology partner. To learn more about Arcserve products, check out our free trial offers.

Cyber Resilience: Report Shows Rise in Proactive Measures Amid Increasing Ransomware Attacks

The Business Continuity Institute (BCI), a global network of business continuity and resilience professionals, just released its BCI Cyber Resilience Report 2023. The report digs into the disruptive effects of cyberattacks on organizations, the cyber resilience actions these organizations are taking, and the role of senior executives in developing cyber resilience strategies.

The bad news is that 74 percent of respondents saw an increase in cyberattacks over the previous 12 months. The (somewhat) good news is that the impact of those attacks was "small to medium."

BCI says that these reduced impacts result from respondents adopting a proactive approach to cyber resilience. That's also reflected in the survey results, with more organizations now reporting an increase in the use of technical measures and organizational policies that reduce the impacts of cyber incidents.

Here are some of the other key results of the survey:

Social Engineering Drives Ransomware Attacks

The report found that employees falling for social engineering techniques were the cause of most attacks, with nearly three-quarters of respondents saying their organization suffered a cyber incident due to phishing or spear phishing. The primary causes? Employees opening malicious links, opening infected downloads, or visiting malicious sites. Ransomware continues to be the most frequent and disruptive threat.

And the result? Financial losses resulting from cyber incidents were upwards of €10,000 for more than 40 percent of respondents. And nearly one in three respondents said their organization had suffered more than five cyber incidents in the previous 12 months.

Cybersecurity, IT, and Executive Teams: Leading Cyber Resilience Strategies

Clearly, the need for proactive cyber resilience strategies is sinking in, as 65 percent of respondents reported that high levels of top management were committed to cyber resilience. And nearly 87 percent have business continuity arrangements to deal with cyber incidents, while 66 percent execute regular backups to ensure cyber resilience.

The report points out that data silos that separate business continuity and cybersecurity remain an “omnipresent issue,” highlighting the need for more integration between technical teams. Notably, there was nearly unanimous respondent agreement that these closer relationships need to be created through solid leadership in cyber strategy by top management.

Culture Makes All the Difference

A cyber-aware organizational culture is a foundation for building cyber resilience. Respondents said that employee training, validation and testing, and having internal policies in place are critical. And they are dedicating efforts and resources to make cyber awareness an essential aspect of the organization’s culture. The survey found a significant increase in training and exercises over the prior year.

Many organizations have dedicated teams or structures to comply with regulations and align with industry standards relating to cybersecurity and business continuity.

Validate Your Defenses

BCI says that validation is vital to cyber resilience, with the data showing that most organizations conduct cyber exercises and penetration tests incorporating learnings from prior incidents and simulations. Outsourcing these services is increasingly popular.

Business Continuity and Cyber Resilience

One of the survey’s findings is that business continuity efforts support cyber resilience. The primary reasons given for that support include faster recovery (81 percent of respondents), mitigation of financial losses (51 percent), and the availability of expert resources to deal with incidents at 50 percent. BCI concludes that this metric suggests that the business continuity profession has adjusted to evolving challenges by taking a more dynamic approach.

Immutable Backups and Cyber Resilience

The survey also found that respondents used several tools to ensure cyber resilience. These include regular backups of critical data (66 percent), regular updates of software and applications (64 percent), endpoint protections like next-gen firewalls or endpoint detection and response (EDR) (56 percent), and disaster recovery programs (53 percent).

This is where the report makes what we think is its most critical point: “Backups are a useful technique to defend against malware, but vulnerabilities remain. The backup itself could also have become compromised by malware, which leaves the organization without lines of defense.” BCI adds, “an increasing number of cyber security and IT teams are shifting to immutable backups to help mitigate the threat.”

Make Data Resilience and Cyber Resilience Your Priority

The BCI survey shows that organizations are making progress as they work toward becoming more resilient. But implementing an effective data resilience and cyber resilience strategy is complex and can be overwhelming for internal teams.

By working with an Arcserve technology partner, you gain access to the expertise and experience necessary to navigate your options and put solutions in place that solidify your ability to prevent cyberattacks and recover quickly if you become a victim.

Find an expert Arcserve technology partner here. Check out our demos to learn more about Arcserve’s immutable storage solutions.

DCIG: The Role of Cloud Consoles and Unified Data Protection in Sustainable Innovation

Enterprises are reaching a point where they recognize that they must not only find and deploy the latest and greatest technologies. More and more IT leaders are also asking for better options for managing all of the features and technologies they already use, according to leading technology analyst firm DCIG's Jerome Wendt.

Wendt explains that introducing innovative features and technologies is still most vendors' mission. But many vendors are pushing to sustain this innovation by employing cloud consoles.

Point Solutions Drive Innovation

Organizations of every size run into challenges that require a new product feature or technology. Point solutions are usually the way those challenges are initially overcome. Wendt also sees new point solutions from startups as a problem for existing technology providers. That's because technology providers that have already achieved a solid market position may not prioritize new features or technologies. They may also make updates that don't really solve the problem or, worse, don't even address the issue.

Point Solutions Create Problems, Too

Startups developing point solutions that solve problems can cut organizations' costs or even create new industries, writes Wendt. But every time a point solution is added, it brings its own issues. Managing multiple point solutions adds its own costs and overhead, like software licenses. And some point solutions may need specialized knowledge that makes them difficult to deploy at scale.

Centralized, Unified Data Protection

Wendt notes the recent release of Arcserve Unified Data Protection (UDP) 9.0, which includes Arcserve Cloud Console, centralizes data management and offers advanced recovery features. Cloud Console is a unified, web-based management interface that provides a seamless user experience for protecting organizations. It increases IT productivity and eliminates business continuity strategy gaps in a single solution.

Cloud Console is hosted and maintained in an Arcserve cloud data center, so it doesn't require manual deployment, installation, or extended time spent on configuration. Users log in and use the interface to perform tasks that help lock down their backups. Users can:

- Create and define backup policies
- Configure infrastructure, source groups, and user access controls
- Manage account resources and users
- Monitor and analyze all backup and recovery jobs

Arcserve UDP 9.0: Tighter Security, More Robust Backup and Recovery

Strengthened security is another enhancement Arcserve has added to UPD 9.0. That includes multi-factor authentication (MFA) for access to Cloud Console.

Other new Arcserve UDP 9.0 features Wendt points out include the ability to perform full or granular recovery of Oracle Pluggable Databases (PDBs). It also has more robust backup and recovery for Microsoft SQL, with UDP now generating an alert and marking backups as unusable for restores if a consistency check fails.

Cloud Consoles Integral to Innovation

Wendt closes his post by writing that "centralized management, now often delivered in the form of a cloud console, must accompany today's innovations. The cloud consoles ensure organizations can sustainably administer this innovation no matter where they deploy it in their environment."

To learn more about Arcserve UDP 9.0 and Arcserve Cloud Console, check out our 30-day free trial offer or request a demo.

Read the complete DCIG article here.

Review: Arcserve UDP and Arcserve OneXafe Deliver Comprehensive Data Protection

A recent review of Arcserve Unified Data Protection (UDP) by LANline caught our eye. Per its website, “LANline’s independent editorial staff stands for high-quality and technological competence, offering IT pros vendor-neutral, objective reporting on all topics relevant to network, IT, and data center infrastructure.” We always appreciate an independent look at our products so we can continue to improve them.

While the review tested UDP 8.1, Arcserve recently released UDP 9.0, further enhancing the solution’s data resilience and security capabilities, among other updates. Here’s an overview of LANline’s assessment.

Setup: Arcserve UDP Plus OneXafe

LANline tested an Arcserve OneXafe 4512 immutable storage appliance along with Arcserve UDP software, which includes Sophos Intercept X Advanced for Server. UDP was installed on a physical Dell server running Windows 2022 for the test. The review notes that the setup was finished in a few minutes, and on first login to the UDP console, a wizard guides you through the basic configuration.

LANline created a new repository for primary backups, then commissioned the OneXafe appliance, noting that it “is typically configured as a secondary backup target to which UDP replicates the primary backup data.”

The reviewers point out that OneXafe encrypts data with AES-256, and a directory share with required permissions was established using the UDP console. Once that was done, Sophos Intercept X Advanced was installed on the UDP backup server and configured via the UDP cloud-based console.

LANline set up a daily scan of the UDP server, with Intercept X providing endpoint protection via malware and threat detection that relies on a deep-learning neural network to prevent malicious intrusions and stop ransomware.

Backup and Restore Capabilities

LANline set up two backup tests to assess the backup and restore capabilities of the Arcserve solution. The first job was an agentless backup of virtual machines (VMs) running on a VMware vSphere 7 ESXi cluster and using a hypervisor-type data protection plan. The second backed up three Windows VMs running on a VMware workstation.

The review notes that once these VMs were added as new nodes in the UDP console, the software automatically installed the UDP agent on the machines.

To replicate the primary backups to the OneXafe appliance, LANline created a directory share in the OneXafe console. They then set up the OneXafe share as an additional data store in the UDP console.

Once finished, LANline could add a replication job to the two backup tests. Arcserve UDP automatically transfers backup data to the OneXafe immutable storage appliance once the primary backup is completed. When the setup was finished, LANline tested the two backup plans and found that they successfully backed up all the VMs.

LANline tested UDP’s recovery capabilities in conjunction with OneXafe by deleting a Windows VM in vCenter and the associated backup data from the UDP (primary) repository. With the UDP console indicating that the VM could no longer be found, LANline highlighted the VM and opened the restore menu. The reviewers point out that the system administrator can choose whether the restore should be pulled from the primary or secondary repository.

After selecting the OneXafe secondary datastore, all available recovery points for the missing VM were shown on the console. The reviewers chose a backup from the previous evening and started the recovery process. UDP recreated the VM in vCenter and successfully restored all of the data.

In a second test, LANline encrypted the file disk in the primary backup for one VM, then deleted the VM from vCenter. Once again, the reviewers started the restore process via the UDP console. But the restore process failed because the virtual disk file they had previously encrypted could not be restored. LANline then turned to the backup stored on the OneXafe appliance, successfully restoring this second backup.

The Verdict: Your Last Line of Defense

LANline concludes that the combination of Arcserve UDP, OneXafe appliances, and Sophos Intercept X Advanced delivers a solution that protects companies from ransomware on multiple levels, with OneXafe’s immutable snapshots providing a last line of defense against attacks.

To learn more about Arcserve UDP and Arcserve OneXafe, request a demo. If you’re ready to see what Arcserve UDP can do for your business, take advantage of our free trial offer.

Read the complete review (in German) here.

Need Answers?

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

arcserve®

+1 844 639-6792
arcserve.com