White Paper

Increase Data Resilience and Improve Ransomware Defense by Integrating Data Protection and Security

Sponsored by: Arcserve

Phil Goodwin
August 2021

IDC OPINION

Ransomware – a word that entered the lexicon only a few years ago – has become one of the top business concerns. Numerous IDC surveys have shown ransomware to be an issue for both business and IT executives, as the fallout of a successful attack can be profound for the organization. Our research has found that the consequences of ransomware attacks include direct loss of revenue and permanent loss of customers, employee productivity, IP, and data, not to mention lasting damage to corporate reputations. Moreover, downtime, whether from ransomware or any other cause, can cost organizations from tens of thousands of dollars per hour up to millions of dollars per hour depending upon the industry, lost applications, and other factors.

Ransomware attackers are not selective about the industry, organizational size, or geography; they will attack any vulnerable target, SMB, or enterprise. IDC's research shows that more than 90% of those organizations surveyed acknowledge having been attacked by malware. And we find it likely that many of the remaining 10% are simply unaware of having been attacked or did not want to admit it. Particularly vulnerable industries include financial services, healthcare, and education, but manufacturing, transportation, utilities, and other industries report attacks on par with other organizations. No organizational leader should believe they are invulnerable or "under the radar" of bad actors. Attacks are inevitable, and robust preparation and response is an organizational imperative.

The inherently increasing complexity of the IT environment contributes to the challenge of implementing comprehensive cyberprotection and cyber-recovery. Application deployments are growing rapidly at the cloud and edge. In turn, data is scattered across core, cloud, and edge resulting in more potential attack points for organizations to defend. It is also well known that the trend toward work from anywhere results in a significant increase in malware and ransomware attacks.

IT organizations are further challenged by the ever-evolving sophistication of ransomware attacks. Data-related attacks involve four primary methodologies: data encryption, data deletion, data corruption (scrambling), and data exfiltration. Each requires a different defense strategy and technological solution. Bad actors have learned to first attack the backup data sets, especially NAS systems that house backup data sets. If they can make data recovery all but impossible, the organization's odds of being forced to pay the ransom go up significantly. The possibility of an insider attack must also be factored in, as insiders may have intimate knowledge of the IT infrastructure,

defensive capabilities, and credentials to access systems. Thus management and system controls must be included in any solution.

Data protection, recovery, and security have traditionally been treated as separate IT security efforts. However, with the threat of ransomware, organizations are looking for solutions that seamlessly integrate all three into a coordinated solution. Vendors are beginning to respond with cyber-recovery systems and platforms to deliver the robust response needed to ensure ransomware recovery and minimize harm to the organization.

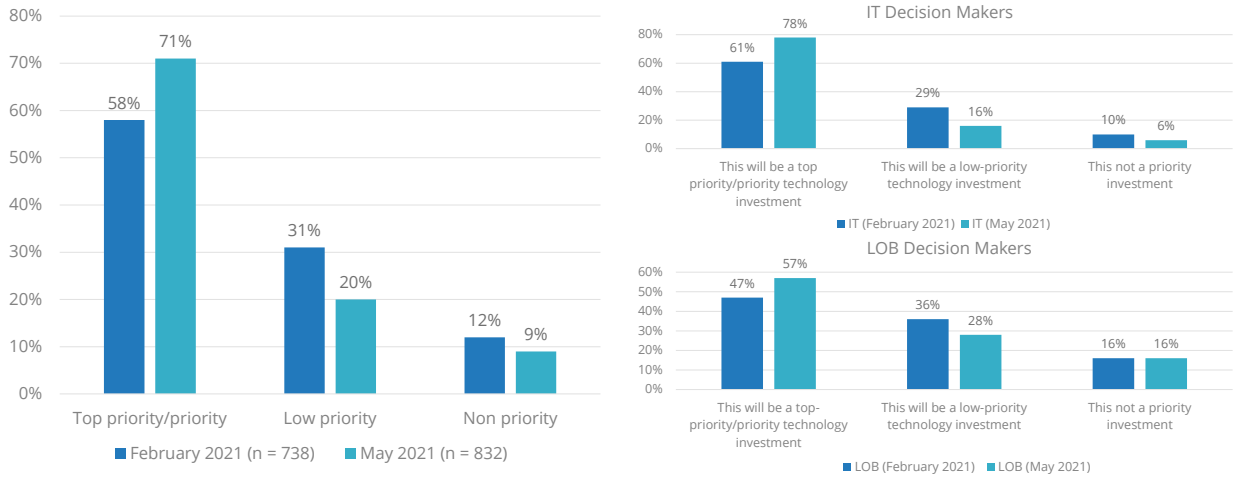
SITUATION OVERVIEW

Business and IT leaders alike understand the urgency of cyber-recovery and digital resilience. A recent IDC study found that digital resilience as a top priority rose sharply in the short time between February and May 2021. In this survey, 61% of IT leaders responding in February indicated digital resilience would be the top investment priority over the next two years. By May, this response increased by 17 percentage points to 78%. Among line-of-business (LOB) leaders, responses to this same issue increased from 47% to 57% in the same time frame. Only 9% of IT leaders and 16% of LOB leaders indicated that investing in digital resilience would be a low priority over the next two years (see Figure 1).

FIGURE 1

Digital Resilience Investment as a Priority

Q. Which statement best describes your organization's view on the priority of digital infrastructure resiliency investments over the next two years, as it relates to ensuring the long-term resilience and success of the business?



Source: IDC's *Future of Enterprise Resiliency and Spending Survey,* February and May, 2021

The need for this increase in investment is not just ransomware but the increase of data growth and complexity of the environment. Our research has found that the average data growth rate expected for enterprises is 43% per year over the next two years. Much of this growth is in the cloud and at the edge. The application portfolio of organizations is also expanding, with new data types (i.e., NoSQL)

and traditional structured/unstructured data. Deployment platforms also expand as organizations subscribe to diverse SaaS applications and are now rolling containerized applications into production.

Given this expanding complexity and IT landscape, organizations are finding traditional backup tools alone are not enough to address sophisticated, evolving threats. Solutions must factor in numerous potential scenarios and respond to those threats with a system of coordinated capabilities that address the contingencies yet make deployment and management simple. Piecemeal do-it-yourself (DIY) solutions require considerable labor to integrate, test, and maintain; they simply won't have the agility and flexibility needed to keep up with the rapidly evolving threats. Integrated commercial solutions also often include a recovery orchestrator to automate many processes that would otherwise be manual and apply that automation across the enterprise. With the consequences and cost of downtime being so severe, a recovery orchestrator that can shave hours or even days off a recovery becomes invaluable.

Although the focus of most organizations is on cyberprotection, IT leaders must take a broader perspective and view resilience holistically. Resilience considers cyberattacks and all potential disruptors, including human error, system failure, datacenter outages, and so on up through natural disasters. Even though many of these more significant events are highly unlikely, as the previously mentioned research shows, a cyberattack is a certainty and the need for recovery a strong possibility. Thus organizations are investing in disaster recovery (DR) systems that can address any event that impacts the broader organization on a large scale.

Our research shows that more than 90% of organizations operate in a hybrid cloud and/or multicloud environment. This means that organizations have data spread across multiple private and public cloud locations and seek comprehensive data protection solutions. Some organizations may attempt to continue managing data protection themselves. Still, many are using or strongly considering cloud service providers and managed service providers capable of keeping systems updated technologically and simplifying in-house IT operations. Many providers also offer value-added services, such as threat analysis, runbook development, policy development, training, testing, and technical services. Many cloud-based providers offer solutions for both on-premises and cloud environments from a single management point of view.

FUTURE OUTLOOK

IT leaders no longer consider data security and data protection as separate tasks and actively seek integrated solutions. Multicloud data management platforms are emerging to address the breadth of data protection, cyber-recovery, and disaster recovery scenarios faced by today's organizations. These platforms often extend beyond data protection and recovery and might include data capture, movement, and governance across the core, cloud, and edge. The central component of these platforms is a policy engine that can ensure the consistent treatment of data regardless of the repository while reducing the labor needed to manage the data. These solutions should have the extensibility to integrate with other solutions — such as intrusion detection — and scale to match the size and growth of the organization. Key capabilities should include:

- **Encryption.** Encryption of data at rest, in flight, and in backup sets helps prevent data exfiltration and theft, whether the threat is internal or external.
- **Immutable backup data copy.** Keeping immutable data copies (which should also be encrypted) ensures that data cannot be corrupted, changed, or deleted by anyone except those using special processes, whether internal or external. This ensures data survival in the

event of an attack. IT buyers should be confident that a workaround to immutability is unavailable, such as system clock or policy changes.

- **Air gapped backup data copy.** The principle of an air gap is to prevent physical access to the backup copy so that it is not compromised by a bad actor. IT organizations should be sure that the control path and data path are separately managed to reduce the possibility of compromise significantly. Many organizations are increasing their use of tape, whereby tapes are removed from the tape library (either onsite or offsite) to provide this physical separation.
- **Integrated solutions.** Hardware, software, and cloud capabilities should be seamlessly integrated to deliver a layered approach to data protection and cyberprotection to give organizations the greatest chance to recover fully, completely, and quickly from any successful cyberattack.
- **Multifactor authentication (MFA).** Many breaches are enabled through stolen credentials (often from successful phishing). Implementing solutions with MFA can help prevent breaches even if credentials are compromised.

Considering Arcserve

In early 2021, Arcserve and StorageCraft merged into a single company. The merger brought together Arcserve's long history and capabilities of data protection software with StorageCraft's unique object-based storage platform and data management capabilities. Along with Arcserve's partnership with cybersecurity leader Sophos, the company can offer a fully integrated solution of data protection and management software, object storage platform, and appliance-based data cyberprotection. The combined solution also brings together Arcserve's strong history serving the data protection needs of medium to large enterprises with StorageCraft's focus on the needs of small and medium organizations to offer a combined breadth of scale across nearly all enterprises. Moreover, the companies show synergy in channel partner organizations, with Arcserve more rooted in value-added resellers (VARs) and StorageCraft with managed service providers (SPs) and cloud service providers. Thus existing partners for both companies will have new capabilities to offer.

Arcserve's product line includes:

- **Arcserve Unified Data Protection (UDP).** As Arcserve's flagship product, Unified Data Protection offers backup and recovery across workload platforms, both virtual and physical, to cover common backup scenarios and disaster recovery and cyber-recovery with recovery orchestration. The product support extends to hybrid cloud support with cloud tiering of data from on premises to the cloud. Arcserve UDP includes deduplication to reduce storage costs and boost ROI. UDP also supports M365 backup and immutable cloud storage on AWS.
- **Arcserve Business Continuity Cloud.** Arcserve Business Continuity Cloud is a cloud-based solution that offers integrated business continuity and DR for hybrid cloud environments of almost any platform, including current x86 workloads plus legacy Unix (HP/UX, AIX), whether on premises, in the cloud, or both.
- **Arcserve Cloud UDP secured by Sophos.** Arcserve UDP secured by Sophos is an appliance-based, fully integrated data protection and data security system, including cloud backup. Sophos Intercept X Advanced is cybersecurity that uses deep learning neural networks to detect known and unknown malware while relying on signatures. CryptoGuard and WipeGuard use behavior analytics to detect and remove the ransomware and boot-level attacks, even if they are previously unknown.
- **ShadowXafe and OneXafe Solo.** ShadowXafe is a complete backup and recovery solution based on a converged scale-out object-based storage platform, offering data backup and

recovery for cloud and on-premises virtual infrastructure environments. It uses context-sensitive policy administration to simplify management and backup tasks. It is tightly integrated with StorageCraft Cloud Services to offer one-click disaster recovery-as-a-service (DRaaS) functionality. OneXafe Solo is designed for simple environments and offers a plug-and-play appliance-based backup solution.

- **StorageCraft Cloud Backup.** StorageCraft Cloud Backup protects M365 and G-Suite applications to quickly and easily restore files, whether accidentally or maliciously deleted.
- **OneXafe.** OneXafe is an object-based scale-out storage system that provides a single integrated hardware/software stack for data protection. The product connects to StorageCraft Cloud Services for business continuity and, using StorageCraft OneSystem, can be managed via browser from any location.
- **ShadowProtect.** ShadowProtect is an integrated image-based backup to simplify DR and speed data restoration. It uses VirtualBoot technology to instantly boot a backup image on a virtual machine and is designed for on-premises, cloud, and hybrid environments.
- **StorageCraft Cloud Service.** StorageCraft Cloud Services is a disaster recovery-as-a-service solution to ensure complete recovery of systems in the cloud. For organizations that do not need a complete DRaaS solution, options are available for recovery as a service or data replication to the cloud.

This combination of technologies, which provide encryption, immutable copies (on premises and in the cloud), authentication, and air gap, makes Arcserve solutions capable of giving organizations the best possible chance of recovering data regardless of event, including ransomware. The integrated hardware, software, and intrusion protection give the company a unique solution positioning in the data protection market.

CHALLENGES/OPPORTUNITIES

Challenges

The data protection market is highly competitive and rapidly evolving, as new customer requirements drive technology development and innovation. Moreover, new data types and application deployment models are being introduced that change data protection requirements and strategies. Needs are constantly evolving and technology developing.

This scenario makes keeping products current a challenge for all data protection vendors, including Arcserve. Data protection vendors must carefully target specific markets as none can be all things to all customers. Arcserve will have the added challenge of integrating products from StorageCraft while keeping up with technological advances. Furthermore, while having a single, fully integrated stack has many advantages, it also means that there are more technology areas where the company must keep pace.

Opportunities

The combination of Arcserve and StorageCraft positions the new entity to address the data protection, security, and data use needs of organizations from SMBs to large-scale enterprises. Since its spin-off from CA Technologies, Arcserve has focused on innovating with its core data protection software platform, best represented by the recent announcement of UDP 8.0 as its flagship solution. StorageCraft's scale-out, immutable storage appliance based on an object storage ring architecture extends the data recovery capabilities across geographical distances to improve recovery certainty

and simplify DR. In leveraging its partnership with Sophos, Arcserve is in a unique position of offering a complete technology stack to address data backup, disaster recovery, and cyber-recovery.

The synergies between Arcserve and StorageCraft extend beyond technology. Arcserve has many long-standing value-added reseller and distributor relationships as the company is 100% channel focused. StorageCraft, for its part, has strength in managed service provider and cloud service provider channels where its products are designed with multitenancy in mind. It is not difficult to imagine the cross-selling opportunities. Moreover, Arcserve has a strong market position in EMEA and APAC — especially Japan — giving the combined entity a strong worldwide presence, with StorageCraft's large presence in North America. Arcserve targets medium- to large-scale enterprises, while StorageCraft is strongest in the SMB sector. The ability to scale solutions up or down can only broaden the range of potential buyers for both solutions.

CONCLUSION

Ransomware is a major risk for organizations, one where attacks are nearly inevitable. The consequence of a successful attack can last for months or even years. However, organizations cannot afford to take their eyes off the day-to-day data protection ball. User errors, system failures, datacenter disruptions, and natural disasters have not gone away even as they pale compared with malware. IT leaders need to reduce the risk of ransomware hits and optimize data availability on a day-to-day basis.

Today, most organizations find themselves compelled to integrate their data protection and data security systems while provisioning the necessary infrastructure, whether on premises or in the cloud. This requires time and effort by the IT staff and opens the possibility to accidental gaps that can lead to compromised systems. Arcserve, with its merging with StorageCraft and partnership with Sophos and Nutanix, can offer organizations a complete solution for data protection and recovery with malware and ransomware protection on an extensible, scalable storage platform. These solutions can address the needs of nearly all organizations, from SMBs to large-scale enterprises. As organizations bolster their defense and response to ransomware, we expect many of them to seek integrated solutions that reduce risk and save IT time and effort.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com