Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **April 2024**
Commissioned by **OpenText**

The Modern Cyberthreat Landscape Demands a Security-Driven Rethink of Backup Strategies

Executive summary

The modern cyberthreat landscape, with ransomware one of its most pernicious features, has transformed a quiet backroom IT maintenance process into a critical boardroom topic. Backup has become a strategic investment area for business resilience and disaster recovery. This transformation drives the need to revisit and reevaluate backup strategies from a security perspective, delivering a top-to-bottom refresh that encompasses questions such as backup philosophy, approaches, tooling, and scalability.

This white paper examines the transformation of the importance of backup strategies, profiles the modern cyberthreat landscape, and presents an updated list of essential requirements to enable a backup approach with business resilience and disaster recovery at its core.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Legacy and laissez-faire approaches to backup are no longer sufficient**
  The evolving nature of modern ransomware and other cyberattacks have transformed a once-upon-a-time IT maintenance process into the linchpin on which business recovery depends. Without a strong and enduring backup posture, ransomware and other cyberattacks will cripple or destroy an organization.

- **Cyberthreat actors are continually probing for new ways to compromise organizations and weaponize security protections**
  Ransomware attacks, data breaches, triple extortion campaigns, leveraging exploits, identity security compromise, distributing malware, phishing campaigns, and new identity attacks are included in the modern playbook of cyberthreat actors. Surviving this onslaught requires much more than luck.

- **Data backup is an essential strategy for security, business continuity, and organizational resilience**
  Data protection and hardened data backup have become essential elements in an architectural model to stop ransomware and other cyberattacks from unleashing unmitigable damage on organizations.

- **New requirements for strategic best practice for backup and recovery**
  What makes sense as strategic best practice for backup and recovery to counteract ransomware in 2024 and beyond is very different to what was sufficient five years ago. New requirements include strategically precluding ransomware from undermining business processes, engineering a backup data format that cannot be exfiltrated, anomaly detection in backup processes, and lifecycle management of multiple and changing media devices, among others.

The modern cyberthreat landscape has transformed a quiet backroom IT maintenance process into a critical boardroom topic.

ABOUT THIS WHITE PAPER

This white paper was commissioned by OpenText. Information about OpenText is provided at the end of the paper.

Evolving security requirements for data protection and resilient data recovery

The evolving nature of modern ransomware and other cyberattacks have transformed a once-upon-a-time IT maintenance process into the linchpin on which business recovery depends. Data protection and resilient data recovery have become architectural components in security strategies. Without a strong and enduring backup posture, ransomware and other cyberattacks will cripple or destroy an organization—through financial damage, reputational harm, lost data, and compromised business processes, if not complete cessation of activities.

As ransomware campaigns and extortion demands have become increasingly pernicious, the baseline approaches for protecting data to enable resilient recovery after a ransomware attack have become ever more strident.

FROM ACCESS CONTROLS TO AI-DRIVEN ANOMALY DETECTION

Access controls tie identities to system and data rights in systems and applications, respectively, but as credential compromise through phishing attacks and dark web access to harvested credentials has become increasingly common, access control alone is insufficient. It is essential, but no longer enough by itself.

Now strong access controls must be combined with AI-driven behavioral anomaly detection to prevent misuse of valid credentials for planting ransomware, exfiltrating sensitive data, and manipulating the desired state of the backup and restore environment.

Data protection and resilient data recovery have become architectural components in security strategies.

STRONGER AND MORE EXTENSIVE USE OF ENCRYPTION

Encryption of data in transit, at rest, and in use restricts who has access to what data and under which conditions, reducing the scope for data theft and misuse. Organizations make the highest use of encryption for data in transit and at rest, although homomorphic encryption for secure computation and other innovations is increasing the usage of encryption during run-time.

Safeguarding control communications in critical systems such as backup solutions is another area where encryption is playing an elevated role as ransomware becomes more devastating. Using encryption for this purpose is designed to stop man-in-the-middle attacks, eavesdropping, and the execution of unauthorized commands.

Most organizations find there is more they could be doing to strengthen how their data is protected across its lifecycle, as well as to prevent exploitation if compromised by a cyberthreat actor.

CYBER INSURANCE TO COVER RANSOM DEMANDS AND GAIN QUICK ACCESS TO DECRYPTION KEYS IS AN INCREASINGLY FLAWED MODEL

For some years, having sufficient cyber insurance cover was treated as an expedient way of being able to pay the get-out-of-jail fee after a ransomware attack. The insurance company would pay the ransom demand, the decryption key would be supplied, and the victim organization would quickly get back to business after reversing the malicious encryption process. It no longer works that way, however.

Securing cyber insurance cover has become much more expensive and difficult to obtain—with premiums increasing by twice or more for less and less coverage, and insurance companies putting potential clients through a much more rigorous pre-qualification process. If the right security controls are lacking or insufficient, coverage is declined.

Even for those that do manage to tick all the boxes and secure insurance cover, paying the ransom to get the decryption key is no guarantee that all data will be restored. Few organizations regain access to all their data, and even fewer regain access as quickly and seamlessly as they want it.

INSUFFICIENT BACKUP APPROACHES UNDERMINE RECOVERY AFTER A RANSOMWARE ATTACK

Relying on backup to recover systems and applications after a ransomware attack has been a recommendation for several years. It makes perfect sense in theory, but for many organizations, a combination of insufficient controls over access to backup settings and a reliance on poorly hardened backup technologies has resulted in data backups failing to provide a pathway to recover after a ransomware attack.

This can take several forms across organizations:

- **Credential compromise and changing retention settings**
  Cyberthreat actors compromise the credentials of backup administrators and surreptitiously change retention settings to wipe years of data. What was assumed to be there is not.
- **Dormant ransomware for repeated infiltration**
  Dormant ransomware is strategically deposited by cyberthreat actors so it will be backed up along with mission-critical data, laying the trap for repeated ransomware infiltration as IT administrators turn to backup data sets to recover their data.
- **Non-immutable backups**
  Organizations discover too late that their backups were not immutable, resulting in backup data sets being erased or changed for the worst without their knowledge.
- **Shared responsibility model befuddlement**
  Confusion about the full meaning of a shared responsibility model between organizations and cloud providers results in backup and disaster recovery duties being overlooked by organizations. When moving their data to a cloud service, many organizations wrongly assume that the provider's guarantee on availability insures them against data loss too.

The net result is that many organizations discover too late that they can't recover all their data after a ransomware attack.

Many organizations find out too late that they had insufficient controls over access to backup settings and were relying on poorly hardened backup technologies.

THE END OF THE ERA FOR GOOD ENOUGH PROTECTIONS

The approaches above have contributed to increasing the strength of controls for preventing ransomware attacks, but cyberthreat actors have also raised their game. In the next section, we look at the dynamics of modern ransomware and other types of cyberattack.

Modern dynamics in cyberattacks

Cyberthreat actors continually probe for new ways to circumvent technical and human defense layers to capture account credentials, steal data, and otherwise monetize malicious endeavors. They attempt to compromise whatever they can to weaken the bargaining position of a victim organization and weaponize an organization's IT infrastructure and security protections. In this section, we look at modern dynamics of cyberattacks.

UNLEASHING RANSOMWARE ATTACKS

Cybersecurity risks in the form of ransomware attacks and data breaches continue to set the tenor of defensive and preemptive cybersecurity strategies at organizations. Data points from separate research studies aggregate into a compelling warning on the blast radius of a ransomware attack. For example:

- **Customers are most concerned about ransomware cyberattacks**
  Ransomware attacks were rated as the cyberattack of highest concern in SonicWall's 2023 Cyber Threat Report, followed by phishing and encrypted malware attacks.[1] Also in 2023, 84% of security leaders said that ransomware attacks represented the threat with the greatest impact on their cybersecurity strategy over the coming 12 months.[2]
- **Cybersecurity risks have the greatest negative impact on meeting strategic business objectives**
  Cybersecurity risks are rated as having a greater impact on the ability of an organization to meet its strategic business objectives over the next 12 months than geopolitical risk, social and reputational risk, and increasing regulatory complexity. These types of risks have often been viewed as intertwined inputs and outputs of each other, e.g., current geopolitical risk driving an increased likelihood of catastrophic cyber risk events.[3]
- **Unwanted encryption is no longer the only lever for extortion**
  Modern ransomware campaigns combine multiple levers for financial extortion, giving cyberthreat actors greater leverage in demanding a monetary payout for their malicious activities. Unwanted encryption plus data exfiltration plus threats of publishing stolen data to drive reputational harm and provoke an outsized regulatory response form the common playbook of ransomware gangs.
- **Backups are compromised to prevent recovery**
  Cyberthreat actors disrupt the integrity of backup processes in advance of a ransomware attack, for example by changing retention settings so less data is captured, deleting backup data entirely, or planting un-executed ransomware in data stores so it will be processed via standard backup procedures. When IT administrators seek to recover after the ransomware attack, they are faced with incomplete data, no data whatsoever, or a repeated cycle of recovery and infection as dormant ransomware is re-executed. Backup systems are now routinely targeted in almost all ransomware attacks with a focus on commonly used backup and recovery solutions and unpatched IT architectures with open exploits.

Modern ransomware campaigns combine multiple levers for financial extortion, giving cyberthreat actors greater leverage in demanding a monetary payout for their malicious activities.

- **Partner-in-crime ransomware models expand the number of attackers, ransomware variants, and access to advanced attack methods**
  Wannabe cyberthreat actors can quickly participate in ransomware attacks through partner-in-crime and ransomware-as-a-service models on the dark web. In return for sharing the financial proceeds of any successful attack, they gain access to evasions, exploits, and other advanced attack methods that were developed by or accessible only to nation-state actors and large cybercrime gangs.

LEVERAGING EXPLOITS

Application and security vulnerabilities offer equipped cyberthreat actors with a highway into stealing data, destroying backups, and planting ransomware. Threat patterns over recent years are denoted by:

- **Backup servers targeted by cyberthreat actors**
  A threat actor group based in Russia (and perhaps other groups, too) have targeted vulnerable backup servers after a security weakness in the backup software offered a way for unauthenticated users to establish control.[4] An exploit enabled access to encrypted privileged credentials stored in the configuration of the backup software.
- **More than 40% increase in disclosed vulnerabilities in just two years**
  The U.S. National Vulnerability Database (NVD) catalogued 28,800 vulnerabilities in 2023, up more than 40% from its 2021 trove. While not all these vulnerabilities are immediately exploitable, they demonstrate a rapidly expanding blueprint of potential avenues to drive compromise. Many organizations are years behind the curve in patching vulnerabilities despite fixes being readily available. Leaving vulnerabilities unpatched is a high-risk move irrespective of whether it is driven by automated prioritization that downplays some patches, fear of breaking mission-critical systems due to untested and opaque interdependencies, or just a lackadaisical attitude.
- **Nation-state actors targeting known bugs to deploy ransomware**
  CISA, the Cybersecurity & Infrastructure Security Agency in the United States, published a warning that state-sponsored groups from North Korea are using exploits of common vulnerabilities to gain initial access to networks.[5] Exploits for the Apache Log4j software library and unpatched remote access appliances grant network access that can be used to deploy ransomware.
- **If you have a fully functional exploit, cybergangs want to hear from you**
  Some cybergangs use a twist on common bug bounty programs to seek out fully functional exploits for high-risk vulnerabilities that they can resell to nation-state actors. Successful submissions can attract payments of multiple millions of dollars.[6]
- **Ransomware groups taking a calculated approach to ransomware attacks**
  Modern ransomware attacks are often targeted at selected organizations and industry sectors based on an assessment of security protections, scale of impact, likelihood to pay, and ability to pay. Some cyberthreat actors use exploits as part of their assessment process to decide whether a compromised victim has the financial wherewithal to pay a ransom demand.[7] Other cyberthreat actors are less interested in the financial return of an attack but instead seek to cause widespread disruption to state and country-level public services, which often puts central IT service providers in the headlights.

Many organizations are years behind the curve in patching vulnerabilities despite fixes being readily available.

- **Exploits are growing for IoT devices, too**
  It is not just IT systems and business applications that are under attack from the growing range of vulnerabilities available to exploit, but operational technology networks and organizations in critical infrastructure sectors that make extensive use of IoT devices. During 2023, the global volume of IoT exploit attacks increased by 15%.[8]

ATTACKING MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) was once viewed almost as an silver bullet in protecting accounts from compromise, but cyberthreat actors have fought back to turn overconfidence in MFA protections against the organizations that employ such schemes. MFA has become just another roadblock to drive around, not the impenetrable defensive layer it was originally positioned as.

Modern dynamics in attacks on MFA include:

- **Phishing toolkits routinely offer capabilities for bypassing MFA protections**
  Capabilities for intercepting and bypassing MFA protections have been included in many phishing toolkits for the past two years. These toolkits enable cyberthreat actors to build phishing websites that trigger MFA prompts, capture the resulting entries, and resubmit stolen credentials and MFA passcodes to the real site.
- **MFA bombing attacks flood a user with maliciously driven MFA prompts**
  Once a cyberthreat actor has gained valid credentials, getting through the MFA barrier is the next challenge. One method is MFA prompt bombing, where MFA challenges are repeatedly sent to the MFA app on the target victim's phone. Unless pre-warned, the victim thinks the repeated prompts are a system error and eventually approves one of the requests to make it stop.
- **Too many users rely on weak forms of MFA**
  All forms of MFA are not created equal, but while more hardened forms are available, many users continue to rely on the weakest ones.[9] For example, one-time codes distributed by SMS have been compromised through SIM swapping attacks. In a similar way, when email messages are used, a cyberthreat actor who has already gained surreptitious access to the victim's email account will be able to intercept the MFA codes—and any subsequent security warnings—to gain access to the other accounts owned by the victim. Personal mobile devices that have been compromised by malware and malicious apps can also be avenues for bypassing MFA protections.[10]
- **Threats to the issuance, setup, and lifecycle management of MFA tokens**
  Tightening controls around MFA protections in use to prioritize hardened approaches such as hardware keys is the right strategic direction. It is not, however, without a set of logistical challenges to deal with the processes of secure issuance, protected setup, and invulnerable replacement. Getting the right hardware device to the correct employee or contractor and ensuring it is set up properly offers multiple places where a determined cyberthreat actor can insert themselves into the process. Resets, too, offer an area fraught with risk where a cyberthreat actor can impersonate an employee (with or without the help of AI capabilities) to request a new MFA device to replace the one they claim to have lost.

MFA has become just another roadblock to drive around, not the impenetrable defensive layer it was originally positioned as.

DISTRIBUTING MALWARE

Malware aims to destroy, corrupt, or undermine the integrity of data, applications, and systems. In whatever form it takes, malware stops organizations from being able to rely on their data and systems to operate business processes. Modern dynamics of malware attacks include:

- **Intelligent malware uses evasive tactics to bypass detection technologies**
  Cyberthreat actors are attempting to design malware that is impervious to anti-malware engines, with one study finding that almost all (98%) of malware used at least one evasive tactic, while a third used six or more evasive tactics.[11] This increased use of evasive tactics and polymorphic adaptations means that organizations must ensure they have the capability to eliminate malware before it captures a foothold in their networks and to exclude malware objects from restores.
- **The malware category is increasingly becoming synonymous with ransomware**
  Many of the most common malware variants over the past five years have actually been ransomware or laid the foundation for a subsequent ransomware attack, such as Emotet, Ryuk, LockBit, and Conti, among others.[12] Ransomware provides a path to profitability that is highly attractive to cyberthreat actors.
- **Malware volumes are rising**
  In 2023, the global volume of malware detected by SonicWall increased by 11% to 6.06 billion, the highest volume it had detected since 2019.[13] This included almost 300,000 malware variants that had never been seen before. While attack patterns vary year to year and by industry, malware as a category remains a significant threat to the integrity of business data.
- **Destructive wiper malware on the rise, too**
  Wiper malware takes a significant step beyond ransomware as a monetary play into destruction as a military, political, moral, or hacktivist one.[14] Such malware variants wipe data from compromised systems (including backups stored directly on the system), thus offering no way back for organizations affected—unless strong and resilient backups have been created. One security vendor recently tracked a 53% increase in wiper malware activity across a three-month timeframe.[15]
- **Data-morphing malware is a potential threat**
  Malware and ransomware gangs could pivot to data-morphing malware that programmatically changes business records and transactions, altering what the organization believes it knows about its customers and suppliers and rendering it unable to meet its commitments. Financial transactions, account balances, ownership records, order history details, and more could be programmatically changed to drive a level of confusion that prevents the organization from operating as it should. A ransom would be levied to unwind the morphing calculus. Without strong and resilient backups, organizations impacted by data-morphing malware would be crippled and unable to function.

Many of the most common malware variants over the past five years have actually been ransomware or laid the foundation for a subsequent ransomware attack.

CRAFTING PHISHING CAMPAIGNS

Phishing attacks remain a primary vector for cyberthreat actors to slip through security defenses to steal account credentials, gain system access, install malware, or grab a foothold for a ransomware infection. Modern phishing attacks:

- **Continue to grow in number**
  In the year from October 2022 to September 2023, an anti-phishing vendor tracked a 1265% increase in the number of malicious phishing emails detected, and a 967% increase in the number of credential phishing attempts detected.[16] With email accounts under increasing rates of attack, preventing attacks from reaching the inbox has become of critical importance.
- **Leverage AI to increase the plausibility of messages**
  Generative AI services are being leveraged by cyberthreat actors to dynamically alter the subject, tone, urgency, style, and overall plausibility of new phishing email messages.[17] The use of AI for crafting phishing messages truncates the time involved from hours to minutes, granting cyberthreat actors greater efficacy in preparing targeted phishing campaigns and more time for sending a higher volume of them.
- **Pivot to new forms to bypass existing protections**
  Over the past year, emerging image-based and QR code phishing attacks have skyrocketed in number, resulting in the vast majority of organizations being compromised by one or more attacks.[18] Existing email security defenses have often proven incapable of detecting all incoming image-based and QR code attacks, letting through attacks that employees then assume to be benign. One study found that PDF documents that contained malicious elements, such as QR codes, increased in frequency from one in five to one in three during 2023.[19]

PIVOTING TO IDENTITY ATTACKS

Although credential theft remains a key goal of phishing attacks, some cyberthreat actors have pivoted over the past year to leverage previously stolen or breached credentials just to log into target environments.[20] With billions of compromised credentials available on the dark web, cyberthreat actors can bypass the need for an initial phishing campaign by selecting credentials to purchase for their preferred targets. In 2023, the abuse of valid credentials for identity attacks was the most frequently occurring initial access vector for cyberattacks, tying for first place with phishing attacks for the first time.

With billions of compromised credentials available on the dark web, cyberthreat actors can bypass the need for an initial phishing campaign by selecting credentials to purchase for their preferred targets.

CONCLUSION

With the growth in the type and volume of these cyberattacks, any organization that manages to avoid even one attack becoming an incident is extremely lucky. For those wanting more certainty than being in the lucky 1%, new requirements for backups to counter security threats have become paramount.

New requirements for data protection and data backup to stop ransomware

Data backup has become an essential security, business continuity, and organizational resilience strategy that plays double duty as a critical protection and recovery strategy in a ransomware attack.[21] Data backup is no longer a mere IT maintenance procedure—and by implication, the rules of the game have changed. What makes sense as strategic best practice for backup and recovery to counteract ransomware in 2024 and beyond is very different to what was sufficient five years ago. Data protection and hardened data backup have become essential elements in an architectural model to stop ransomware attacks from unleashing unmitigable damage.

STRATEGICALLY PRECLUDE RANSOMWARE ATTACKS FROM UNDERMINING BUSINESS PROCESSES

When data is the lifeblood of an organization, protecting it is a matter of life (business success, loyal customers, strong supply chain) and death (financial harm or ruin, reputational damage, customer churn). Doing backup in the right way using the best methods considering an up-to-date enterprise assessment of security threats and risks is the only principled way to ensure that data can be recovered when it must be. Intentionally continuing to rely on substandard backup solutions, insufficient data backup approaches, and non-existent methods of detecting malicious activity is an invitation for great harm to befall the organization.

To strategically preclude ransomware attacks from undermining business processes, data, and marketplace vitality, organizations must prioritize an expanded set of requirements for backup solutions. This re-evaluation must result in strengthening security controls in advance of a ransomware incident, which increases the velocity of effectively getting systems and applications back online—and employees back into productive work.

To strategically preclude ransomware attacks from undermining business processes, data, and marketplace vitality, organizations must prioritize an expanded set of requirements for backup solutions.

NON-EXFILTRATABLE BACKUP DATA FORMAT, NOT SIMPLE COPIES

If they can, cyberthreat actors will steal and weaponize data from backup solutions for use in extortion demands. Preventing this from happening relies on several core architectural approaches in a backup solution.

The first is the use of a data format by the backup solution that doesn't make sense to the cyberthreat actors if it is exfiltrated. It is engineered by the backup solution specifically for the purpose of backup. It is not a simple copy of operational data, a binary clone, or even a snapshot of the file system. Checks and balances must be used during the process of creating backup data to ensure that what has been captured is an accurate reflection of the source data. The result of this first approach is obfuscated data that protects against data exfiltration.

The second approach is that data is written immediately to multiple backup media targets, without staging or caching to preclude data manipulation and data theft. The backup solution must orchestrate the writing of backup data to more than one backup target, verify that the data has been backed up correctly, track the location of all backup data for use in recovery situations, and protect the backup media that has been created. These are essential capabilities of the backup solution to be operationalized in line with how the organization configures the desired options.

OBFUSCATION AND ENCRYPTION TO PREVENT UNAUTHORIZED ACCESS TO BACKUP DATA

Computational obfuscation of source data prior to backup introduces a first level of protection against data exfiltration. By changing source data into a different format ready for backup, exfiltration results only in nonsensical data that cannot be used to demand an extortion payment from the organization. This obfuscation should still allow for compression and deduplication to minimize and optimize backup storage demands. By this stage, only a properly constituted recovery process that is duly authorized through the backup solution can regenerate the obfuscated data into a usable and readable format ready for use in business processes.

Additional levels of encryption can be employed across the obfuscated backup data to further tighten data security, protect data when it leaves safe premises, and enable applicable regulatory requirements to be met. If the worst-case scenario happens and a cyberthreat actor manages to steal backed-up data, they only have obfuscated and encrypted data which they have no way to piece back together again. Leveraging strong encryption ciphers and approaches on the inbound side of data backup processes means that malicious attempts to circumvent encryption protections on the recovery side will fail by design.

The increased use of encryption in backup demands strong and resilient management of encryption keys. Without such an approach, a ransomware or other cyberattack could compromise the ability of an organization to use its own encryption keys, thus preventing access to their own data and rendering inaccessible every downstream system that relies on encryption. The key management system must be designed to survive a disaster, routinely tested to ensure those plans work, and be able to orchestrate the safe movement of keys for use at recovery time.

Encrypt backup data to further tighten data security, protect data when it leaves safe premises, and meet applicable regulatory requirements.

USE ENCRYPTION FOR OPERATIONAL COMMAND INTERACTIONS, TOO

Encrypting all commands between an authorized control interface for the backup system and the rest of the backup infrastructure minimizes the ability for backup commands to be intercepted through man-in-the-middle attacks. Requiring encrypted commands also removes the possibility of threat actors seeking to circumvent the backup system by issuing non-encrypted commands hidden in malware code.

BACKUP SOLUTIONS MUST ASSESS DATA STREAMS FOR MALWARE AND DORMANT RANSOMWARE

Assessing data to be backed up during the backup process for the presence of malware and dormant ransomware ensures that backups are created free of corruption. Detection of malicious files during backup procedures should trigger warnings to check and secure source data repositories, instantiate an incident response process to track and mitigate the originating infection, and eliminate the malicious files from the backup data set. When multiple independent assessment tools work together to check and verify data, the likelihood of an unexpected compromise is significantly reduced. If undetected malware is backed up, the backup software should allow malicious code or data to be skipped during the restoration process to avoid reinfection.

BACKUP SOLUTIONS MUST IDENTIFY ANOMALOUS PATTERNS

Abnormal or unexpected fluctuations in the volume and/or nature of data being presented for backup should trigger high urgency alerts. If data volumes suddenly diverge from established patterns, it could indicate that a malicious actor has deleted critical business data or changed retention settings. Likewise, if the types of files being presented for backup suddenly deviate from the norm, it could indicate the presence of unwanted malicious encryption, e.g., a ransomware infection. When a backup solution can intelligently assess current patterns against historical baselines, it provides early warning of potential compromise and should trigger investigation and remediation activities.

BACKUP SOLUTIONS MUST ACCOMMODATE MULTIPLE BACKUP DEVICES AND ACCOUNT FOR CHANGING MEDIA REQUIREMENTS

Backup devices are many and varied, covering different types of physical, virtual, and cloud approaches. A backup solution designed so organizations are resilient to ransomware attacks must accommodate multiple types of backup devices, depending on the current and shifting preferences of the organization using the solution. Organizations should be able to switch and change between backup devices on their schedule, not locked to a specific vendor's roadmap.

Retention requirements vary by industry and data type. For example, healthcare organizations aiming to provide whole-of-life care to patients must have a structured and secure process to manage patient data for 70 to 100 years. By implication, it is essential that organizations can seamlessly migrate data backed up on today's best-in-class media to newer forms of media as the time passes and technology changes. This requires a backup data format that is agnostic of today's system, path, and architectural dependencies and the ability to copy backup objects to newer media formats. The media catalog—the master index of what has been backed up and how to regenerate usable data—must also be protected against loss and corruption.

Business-critical archiving solutions must be safeguarded with a strong backup solution to protect against data loss due to traditional and emerging cyberthreats. It is a massive risk for any organization to have only a single copy of important data, even if that is stored in an archiving solution.

By intelligently assessing current backup data patterns against historical baselines, anomalies signaling potential compromise can trigger early warning signals.

IMMUTABILITY TO PREVENT RANSOMWARE FROM DESTROYING BACKUP MEDIA

Data on backup media that can be changed, modified, or overwritten can be corrupted and destroyed by ransomware and other cyberattacks, thus undermining the core purpose of the backup solution. If backup media is corrupted, this eliminates it as an option for post-ransomware recovery.

Immutability means that data cannot be changed, modified, or overwritten, thus ensuring a valid backup is available. Immutability has become a core requirement for advanced backup solutions so that what is backed up can be restored. Immutable backups need the ability to securely interact with the backup software to report which data is stored and keep the backup media catalog up to date.

Air gapping is a common and established approach for creating an immutable backup data set. Risk can be further reduced by using multiple different target media architectures that eliminate the dependency on a single restoration pathway. Having multiple independent options available increases the likelihood of a prompt and complete restoration after a disaster, even if a site is inaccessible for some reason.

EMBRACE THE MODERN BACKUP PRINCIPLE OF 3-2-1-1-0

3-2-1 is the legacy principle for backup, stipulating that three copies of data should be stored on two different forms of media, with one of those stored off-site for disaster recovery.

The new-generation 3-2-1-1-0 principle hardens backup protections by adding two requirements for the modern cyberthreat landscape.

- The first addition is the digit 1 in fourth place, indicating that at least one backup copy is stored in such a way that it cannot be compromised by ransomware, e.g., it's stored offline, it's air gapped, and/or it's immutable. This can be achieved using WORM options, backup tapes, data vaulting, and other approaches that preclude access using a network connection and prevent physical access to the media.
- The second addition is the digit 0 in fifth place, which indicates zero backup errors because the backup solution self-assesses that the data it backed up is valid and can be used for recovery. This verification process means that backup errors are detected almost immediately, allowing proactive remediation efforts to identify and resolve outstanding errors.

The new-generation 3-2-1-1-0 principle hardens backup protections for the modern cyberthreat landscape.

Relying on a single backup in the cloud or storing all backup data in one data pool or target architecture is an extremely risky proposition for any organization.

Making 3-2-1-1-0 work in this age of IT and data proliferation—or indeed any alternative backup scheme—requires an orchestrated and disciplined approach that must be driven by the backup solution. Achieving 3-2-1-1-0 cannot rely on human actors shuffling tapes between storage cabinets and offsite storage locations, for example. The backup solution must offer capabilities for placing data across the selected target backup devices in support of 3-2-1-1-0 strategies—or any alternative strategic design selected by the organization.

BACKUP SOLUTIONS MUST LEVERAGE HARDENED MFA TO PROTECT SETTINGS

If a cyberthreat actor gains access to an administrator's account for the backup system, they can manipulate important settings to degrade backup efficacy. Hardened forms of MFA, such as authenticator apps on corporate-managed devices or cryptographic hardware keys, must be prioritized over simpler and less secure forms of SMS codes, email notifications, and the use of unmanaged personal devices.

ZERO TRUST APPROACHES TO LIMIT COMPROMISE

Using zero trust principles during the configuration of a backup system means the identities of individual components are repeatedly checked and verified during its operation. Hardening this process means a greater reliance on identities portrayed cryptographically rather than in plain text. The use of hardened zero trust approaches minimizes the possibility for cyberthreat actors to spin up fake backup components (e.g., a fake backup server or control interface) as part of a campaign to compromise and corrupt data through ransomware.

Other zero trust approaches are also valuable, such as data encryption being configured on a per-client basis. Reducing the number of network ports from an unmanaged or random collection to a tightly defined and limited set is another example.

SCALE AS THE ORGANIZATION GROWS

A backup solution chosen when the organization is small and growing rapidly must be able to scale over time as the organization increases in size, breadth, and complexity. It is better to avoid being forced to migrate to a new backup system during an organizational growth phase because the original backup system was never designed for higher data volumes and system demands.

High availability features, support for heterogeneous platforms and deployment options, robust disaster recovery protocols, and the ability to seamlessly perform retention and media management on a massive scale are important capabilities for all organizations from day one, even if they are not used until day 658 or even year 10. Designing scalability into the solution also encompasses architectural flexibility around backup data formats and freedom from dependencies due to specific system and path designs, as we have previously discussed in this white paper.

Avoid being forced to migrate to a new backup system during an organizational growth phase because you selected something that was never designed for higher data volumes and system demands.

COMPLEMENT CYBERSECURITY STAFF WITH PROCESS DISCIPLINE

The inability to locate, hire, and retain enough cybersecurity professionals with the requisite skills is a well-known problem facing organizations across the globe. It's partly a supply issue and partly a cost one. Backup solutions built for the modern era must deliver disciplined processes and repeatability to complement the cybersecurity staff an organization does have. For example:

- **Enabling regular testing and finetuning of recovery processes**
  If backups play the linchpin role in enabling an organization to recover after a ransomware attack, recovery must be documented thoroughly and tested regularly. This drives assurance that everything is working as it should and gives cybersecurity professionals the ability to build maturity into their playbook for collaboration and coordination outside of a high-stress situation.
- **Abstracting backup operations and restoration process for cross-skilling**
  Normalize and standardize backup operations and restoration processes regardless of source applications and destination systems, so that what works for one application or system works for them all. Using software with built-in intelligence to hide the nuances of specific source applications means that cybersecurity professionals with knowledge of one application or system can use that knowledge for the others, too.

- **Avoiding dependencies and vendor lock-in across the lifecycle**
  Design backup and restoration processes in a way that avoids dependencies and vendor lock-in across the lifecycle of the solution. Aligning with an open, flexible solution means that the organization is free to choose preferred target backup devices at any time, without being subject to the limitations of proprietary hardware (e.g., supply chain issues, unpatched security vulnerabilities, architectural limitations, and high prices, among others). This makes a significant difference for the organization and the cybersecurity staff that are managing the backup solution.

During a ransomware attack, software and people have to work together under urgency to recover quickly and completely. Organizations cannot afford to depend on cybersecurity staff rebuilding everything from the ground up—it is an improbable route to a successful restoration. It is, however, one almost guaranteed to drive burnout and turnover among current staff.

Conclusion

As modern cyberattacks have become increasingly advanced, organizations must stop relying on simple backup strategies. Business recovery and resilience in the face of an increasing threat landscape depend on organizations strengthening their data backup and restoration fundamentals.

Backup solutions built for the modern threat era must deliver disciplined processes and repeatability to complement the cybersecurity staff an organization does have.

About OpenText

OpenText Data Protector is an enterprise-grade data backup and recovery software solution designed to help organizations protect their critical data across physical, virtual, and cloud workload environments. It provides centralized management of backup and recovery operations, enabling IT administrators to efficiently protect and recover their data across a wide range of platforms and applications. With Data Protector, organizations automate backup and recovery tasks, reduce the risk of data loss, and improve reliability and efficiency of their IT operations. Data Protector delivers secure, compliant backups of all your company data from a single management point. Fast restoration ensures operations quickly return to normal, minimizing revenue loss and maintaining reputation.

Visit www.microfocus.com/en-us/portfolio/data-backup

opentext™

www.opentext.com

@OpenText

+1 800 499 6544

[1] SonicWall, 2023 SonicWall Cyber Threat Report: Charting Cybercrimes Shifting Frontlines, February 2023, at https://www.sonicwall.com/resources/white-papers/2023-sonicwall-cyber-threat-report/

[2] Scale VP, Cybersecurity Perspectives 2023, July 2023, at https://www.scalevp.com/insights/cybersecurity-perspectives-2023/

[3] World Economic Forum, Global Cybersecurity Outlook 2023: Insight Report, January 2023, at https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

[4] Bill Toulas, Hackers target vulnerable Veeam backup servers exposed online, April 2023, at https://www.bleepingcomputer.com/news/security/hackers-target-vulnerable-veeam-backup-servers-exposed-online/

[5] CISA, #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities, February 2023, at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a

[6] Immanuel Chavoya, The Year of Zero-Days - Defending Against the Million Dollar Threat, August 2022, at https://www.brighttalk.com/webcast/5052/538225

[7] Jeff Burt, Microsoft to enterprises: Patch your Exchange servers, January 2023, at https://www.theregister.com/2023/01/28/microsoft_patch_exchange_servers/

[8] SonicWall, SonicWall Threat Data Exposes Depths of Cyberattacks; Propels the Need for Managed Service Providers, February 2024, at https://www.sonicwall.com/news/sonicwall-threat-data-exposes-depths-of-cyberattacks-propels-the-need-for-managed-service-providers-msps/

[9] Robert Lemos, Cyberattackers Double Down on Bypassing MFA, March 2023, at https://www.darkreading.com/threat-intelligence/cyberattackers-double-down-bypassing-mfa

[10] Matt Kapko, Multifactor authentication is not all it's cracked up to be, October 2022, at https://www.cybersecuritydive.com/news/multifactor-authentication-weaknesses/633399/

[11] Opswat, Deep Content Disarm and Reconstruction, September 2020, at https://www.opswat.com/technologies/data-sanitization

[12] OpenText Cybersecurity, Nastiest Malware 2023, October 2023, at https://community.webroot.com/threat-reports-176/nastiest-malware-2023-355907

[13] SonicWall, 2024 SonicWall Cyber Threat Report, February 2024, at https://www.sonicwall.com/threat-report/

[14] Dmitry Bestuzhev, BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows, November 2023, at https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows

[15] Derek Manky, Key Findings from the 2H 2022 FortiGuard Labs Threat Report, February 2023, at https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022

[16] SlashNext, SlashNext's 2023 State of Phishing Report Reveals a 1,265% Increase in Phishing Emails Since the Launch of ChatGPT in November 2022, Signaling a New Era of Cybercrime Fueled by Generative AI, October 2023, at https://www.prnewswire.com/news-releases/slashnexts-2023-state-of-phishing-report-reveals-a-1-265-increase-in-phishing-emails-since-the-launch-of-chatgpt-in-november-2022--signaling-a-new-era-of-cybercrime-fueled-by-generative-ai-301971557.html

[17] Osterman Research, The Role of AI in Email Security, August 2023, at https://ostermanresearch.com/2023/08/21/orwp_0358/

[18] Osterman Research, Fortifying the Organization Against Image-Based and QR Code Phishing Attacks, March 2024, at https://ostermanresearch.com/2024/03/07/ironscales-image-based-qr-code-phishing/

[19] SonicWall, 2024 SonicWall Cyber Threat Report, February 2024, at https://www.sonicwall.com/threat-report/

[20] IBM, IBM Report: Identity Comes Under Attack, Straining Enterprises' Recovery Time from Breaches, February 2024, at https://newsroom.ibm.com/2024-02-21-IBM-Report-Identity-Comes-Under-Attack,-Straining-Enterprises-Recovery-Time-from-Breaches

[21] Osterman Research, Ransomware Attacks: Strategies for Prevention and Recovery, October 2022, at https://ostermanresearch.com/2022/10/14/orwp_0355/