Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **May 2023**
Commissioned by **OpenText Cybersecurity**

Key Requirements for Backup and Recovery Services to Protect Against Modern Ransomware Attacks

Executive Summary

Modern ransomware attacks exfiltrate data for extortion, encrypt data for operational disruption, and delete backups to undermine recovery options. With the threat of ransomware increasing, organizations must ensure they have the capabilities to prevent, detect, neutralize, and recover from a ransomware attack. With backups increasingly under direct threat as part of the ransomware playbook, organizations face devastating consequences if they cannot rely on a modern backup and recovery service to outplay modern ransomware attack dynamics.

This white paper examines the dynamics of modern ransomware attacks and explores the key requirements that organizations and managed services providers (MSPs) should demand in modern backup and recovery services.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Modern ransomware attacks are sophisticated, malevolent, and complex**
  Threat actors probe for vulnerabilities in current defenses to find unguarded and weak points of entry, use multiple levels of extortion to maximize the likelihood of a ransom payout, and delete or compromise backups to reduce the ability of organizations to recover after a ransomware attack.
- **Threat actors can still make ransomware a lot worse than it already is**
  Ransomware gangs could pivot to data-wiping and data-morphing malware, and when sanctions on Russia are lifted, Russian ransomware gangs could unleash a new wave of attacks driven by fury and outrage at lost criminal profits.
- **To thwart ransomware attacks, organizations need to implement a modern backup solution**
  Organizations must have the ability to detect and disrupt ransomware attacks as quickly as possible, and strong recovery abilities if an attack is successful. A modern backup solution is essential for recovery.
- **Modern backup and recovery services must offer essential capabilities to assure recoverability for organizations**
  Policy-based backup, support for the diversity of physical and virtual servers in an organization's IT infrastructure, strong encryption to protect data and limit access to backup datasets, and integrated ransomware protections and anomaly detection are among the essential capabilities for organizations.
- **MSPs have several additional essential requirements from backup and recovery services**
  Multi-tenancy, customer provisioning, account management, billing, reporting, data protection, and customer branding, among others, are essential additional requirements for MSPs looking to grow new revenue streams from backup, restoration, and failover services.

Organizations must ensure they have the capabilities to prevent, detect, neutralize, and recover from modern ransomware attacks.

ABOUT THIS WHITE PAPER

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

Characteristics of Ransomware Attacks

The threat of ransomware is consistently rated a top concern in our cybersecurity surveys and of high priority to senior IT and security leaders.[1] Modern ransomware attacks exhibit the following threat dynamics:

- **Ransomware attacks are becoming more sophisticated**
  Threat actors target specific organizations, probing for vulnerabilities in current defenses to find unguarded and weak points of entry. Targeted phishing emails to trick unsuspecting employees to click a realistic-but-malicious link are frequently used in ransomware attacks, along with probing externally facing systems for unprotected or under-protected VPNs and remote access systems. High-profile ransomware attacks have been successful because the threat actor found a single point of entry, e.g., a legacy VPN with weak identity requirements.

- **Attackers increasingly use multi-level extortion designs to entangle victims in a complex web of compromise**
  Threat actors no longer rely only on malicious encryption in modern ransomware attacks. Additional levers for extorting victims are included, with data exfiltration a primary tactic. Exfiltrated data is used to blackmail the victim into paying a ransom, sold to the highest bidder, or published to cause reputational damage and regulatory action. Almost 90% of ransomware attacks in 2023 include data exfiltration as an additional trigger of extortion.[2] Several groups have pivoted to pure extortion based on exfiltrated files.[3]

- **Threat actors work to prevent organizations from being able to recover**
  Backups are commonly used by organizations to enable post-attack recovery without having to pay the ransom to gain access to decryption keys. However, threat actors increasingly seek to disrupt backup processes, delete backups, and compromise backup data with dormant ransomware to trigger another cycle of malicious unwanted encryption after recovery. Although early ransomware attacks were often single incidents, modern attacks chain multiple types of attack together.

- **Timeframe from initial compromise to detonation is shrinking**
  The timeframe for ransomware detonation after initial compromise has been shrinking from months to weeks, days, and hours.[4] While more organizations have new cybersecurity protections to detect early-stage ransomware activity, ransomware groups are leveraging advanced toolkits to increase the speed of lateral movement, establishing persistence, and pre-detonation data exfiltration.

- **Ransomware attacks are growing in frequency, variation, and blast radius**
  Many indicators of ransomware attacks are increasing, including frequency of attacks (the number of reported attacks in five of the last six months are among the highest of the previous three years[5]), the number of ransomware variants detected in the wild (doubled from 2021 to 2022[6]), and the blast radius when organizations offering critical infrastructure are compromised by ransomware (e.g., the Colonial Pipeline attack compromised fuel delivery on the East Coast of the United States, affecting millions of consumers and businesses).[7]

Almost 90% of ransomware attacks in 2023 include data exfiltration as an additional trigger of extortion.

- **Proclivity to pay the ransom demand leads to serial infection via copycat attacks by other ransomware groups**
  Threat actors in different ransomware groups take cues from each other, which has become easier with data leak sites and dark web forums. Often, when one group succeeds in infiltrating an organization and getting paid to back off, other groups take note and try copycat attacks themselves. Organizations have fallen prey to serial infection because while they have recovered by paying the ransom demand, they haven't addressed the underlying vulnerabilities fast enough to prevent a different ransomware group from succeeding with another attack.

- **Cyber insurance is more difficult to get, and more costly, too**
  The rash of successful ransomware attacks in recent years has forced insurance providers back to their annuity calculators, driven by sharp declines in profitability caused by payouts to meet insurance claims. Affordability of cyber insurance has plummeted consequently, with some organizations facing premiums twice as high for half the coverage.[8]

- **Paying the ransom to decrypt data usually doesn't restore everything**
  Most organizations that suffer a successful ransomware attack consider paying the ransom demand as an expedient method of quickly getting back to business. While some conclude that paying the ransom only funds future malicious activity, many choose the expedient pathway. If the decryption key is given after the ransom is paid (and threat actors are getting better at doing so), there is no guarantee that the decryption key will unlock the encrypted data. Although many organizations that pay the ransom expect an easy recovery process, few find it flawless, seamless, and complete.

- **Specialization, coordination, and corporatization of ransomware groups**
  Early ransomware attacks were unleashed by small-time criminals acting alone. No more. Ransomware groups are corporatizing, with HR departments, finance groups, internal IT teams, pre-compromise technical specialists, and post-compromise negotiators. Ransomware groups can decide where their skills best come into play, with ransomware-as-a-service offerings readily available to new-entrant threat actors, business partner models for sharing the profits of criminal activity, ransomware toolkit providers offering advanced technologies that were previously only available to state-sponsored and nation-state groups, and initial access brokers (IABs) who sell access to a compromised system to the highest bidder. Specialization and coordination across the ransomware supply chain lower entry barriers for new threat actors and provide easy access to the most advanced toolkits.

- **An international threat, led by Russian gangs**
  Two-thirds of recent cyberattacks have been attributed to Russia,[9] and three-fourths of ransomware revenue goes to hackers linked to Russia.[10] Other states support ransomware groups (e.g., North Korea of Lazarus[11]). Some groups operate internationally without apparent state ties—e.g., the Royal group, which also attempts to delete backups almost immediately after infiltrating a target.[12]

Organizations that pay the ransom to regain access to their data expect an easy recovery process—yet few find it flawless, seamless, and complete.

How Ransomware Could Get Worse

Ransomware is already a leading cybersecurity threat for organizations, but it could still get a whole lot worse. For example:

- **From data encryption malware to data-wiping malware**
  The use of data-wiping malware—instead of just data encryption malware—renders compromised data irretrievable. Ransomware groups wouldn't offer decryption keys because the data would be gone forever. Strong and resilient backups would become essential to recovery. No backup, no business.

- **From data encryption malware to data-morphing malware**
  Ransomware groups could introduce data-morphing malware that changes business records and transactions, undermining the ability of the organization to deliver its promises to customers and suppliers. Data-morphing malware would programmatically change account balances, ownership records, purchase history details, loyalty program records, and more. Ransomware gangs would demand a ransom for unwinding the morphing calculation. Organizations without strong and resilient backups, including the ability to pinpoint when the data-morphing attack began, would be crippled and unable to function.

- **Russian ransomware gangs seeking payback for decreased opportunities**
  International sanctions against Russia for its invasion of Ukraine have decreased the level of ransomware activity from Russian gangs. What happens once the invasion ends and sanctions are lifted remains to be seen, but it is likely that Russian gangs will unleash a new wave of attacks driven by fury and outrage at lost criminal profits. The scope of damage, ransom demands, and negative long-run effects experienced by compromised organizations will not be lower than they were prior to the sanctions being imposed.

- **More exfiltrated data published as ransom payments are outlawed**
  Data is already exfiltrated in almost 90% of ransomware attacks, and ransomware gangs promise not to publish the exfiltrated data if their ransom demand is met. If jurisdictions clamp down on paying ransom demands—making them illegal and equivalent to conspiring with criminals—the frequency of exfiltrated data being published will increase.

Organizations without strong and resilient backups, including the ability to pinpoint when the data-morphing attack began, would be unable to function.

What Is an Organization to Do?

With the increased threat posed by ransomware—and the likelihood that ransomware will get worse going forward—organizations must have the ability to detect and disrupt ransomware attacks as quickly as possible, as well as strong recovery abilities if an attack is successful.

What are the key requirements for organizations looking for a backup-as-a-service offering? What additional key requirements are essential for MSPs looking to grow new revenue streams in serving their customers?

Backup as a Service: Key Requirements

Only a minority of organizations successfully recover all their data after a ransomware attack, even among those with backups. In other words, if backup is an essential recovery strategy, it must be done right. Organizations need a backup service that decreases the risks of modern ransomware attacks, assures customer trust, and minimizes business disruption. The most important requirements are:

- **Policy-based backups for all required data**
  All data to be covered by backup procedures should be captured by setting backup policies, not by waiting for employees to manually initiate a backup when they remember. A backup administrator must be able to establish a backup scope or job for a defined server or application, including configuring the frequency of capturing changes.

- **Works with all the systems and applications in your environment**
  A backup service must support the diversity of physical and virtual servers run by organizations, including current and legacy operating systems and application servers, e.g., current and legacy versions of SharePoint Server or Exchange Server. The longer the default list of supported systems and applications, the better, because exclusions of mission-critical systems render the option incomplete. Organizations must then negotiate with the vendor for customized support (higher risk) or find separate point solutions to capture data from unsupported systems and applications (more costly).

- **Strong encryption to protect data and limit access to backup datasets**
  Encrypting data during backup processes and persistently when backups are at rest assures the organization that its data is protected from breach and unauthorized access. The encryption process should ensure that not only threat actors are prevented from accessing an organization's data, but also the service provider offering the service. This requires designing the encryption process so at least one component is held solely by the organization and is inaccessible to the service provider. This means each organization holds the complete set of keys to decrypt their backup data, while the service provider does not.

- **Control over data storage locations to meet sovereignty requirements and regulatory directives**
  Organizations subject to data sovereignty requirements due to internal risk mitigation policies or external regulatory directives require the ability to control where backup datasets are stored. The backup and recovery service must offer the ability to specify geographical constraints on data storage.

- **Configuration, control, and optics for backup jobs and status**
  The configuration of all backup scopes or jobs must be accessible to authorized administrators from a unified interface. An administrator must be able to see which scopes have been established and the status of each backup job (e.g., complete, in progress, or incomplete due to an error). If multiple administrators require different levels of control over separate backup jobs, role-based access control must be available to limit which jobs administrators can view, modify, and delete. For MSPs offering backup services to organizations, multi-tenancy adds an additional scope for securely segregating customer data and administrator access on a per-customer basis.

If backup is an essential element of an organization's recovery strategy, it must be done right.

- **Intelligence to sense anomalies that could indicate compromise**
  Anomalies in the shape of data backup flows offer early indications of potential ransomware compromise. Abnormal and unexpected reductions in the number of files being backed up could be due to malicious or accidental deletion, while unexpected increases could be due to maliciously encrypted data. In both cases, anomalous behavior should trigger automated and manual intervention.

- **Hardened security controls over changing backup settings and erasing data**
  If threat actors can compromise the system administrator's credentials for the backup system, they can change backup settings or erase backup data in advance of detonating a ransomware attack. Either less data is backed up (since the change in settings reduces the scope of captured data) or current backups are unavailable. Change and erase requests should be difficult to execute without supplementary approval and obfuscated standdown periods, utilizing controls such as strong multi-factor authentication, escalation workflows, and recycle bins.

- **Data must be backed up to more than one location**
  Recovery requires multiple equally valid and independently strong alternate pathways to decrease the risk that any given pathway is compromised, inaccessible, or unusable. The principle of 3-2-1 (three copies of data, stored on two forms of media, with one copy offsite/off-network/air-gapped for disaster recovery) continues to set the essential minimum for data backup. While every backup as a service offering includes cloud storage to deliver 1-1-1 of the above, fit-for-purpose services address the remaining 2-1-0 through on-premises and other storage options. Relying on a single backup in the cloud is too risky.

- **Orchestrated restoration to account for inter-system dependencies**
  Servers and applications usually must be started following a stepwise process to account for system dependencies. For example, directory and database servers usually need to be up and running before the application servers that rely on these are spun up. When multiple systems are being restored after a cyber incident, orchestrated restoration means the initial servers are restored and instantiated before the others. Organizations need the ability to configure a restoration process coordinating interdependencies across multiple systems.

- **Facilitate testing of backup datasets for confidence in recovery**
  Organizations must be able to easily test that their backup datasets are complete, reliable, and work as expected in a recovery situation. When organizations stake the recoverability of their business and operations on backup, restoration, and failover services, regular and routine testing is essential. Complete restoration of a given server is a baseline requirement, along with enabling more granular access to specific files, folders, and other data. Repeated testing builds competence and resilience in backup and IT administrators in preparation for an actual incident.

- **Going beyond backup with complementary recovery and resilience capabilities**
  Some backup vendors are innovating beyond the confines of the traditionally defined backup and restoration category, extending their offerings into complementary recovery and resilience use cases. For example, one adjacent use case is failover for short-term recovery when a primary server is unavailable. This is possible because there is a full and up-to-date backup of data for the physical and virtual systems enrolled in the backup service, and spinning up a working system when an incident or accident disrupts the original system enables the organization to keep working.

Change and erase requests in backup datasets should be difficult to execute without supplementary approval and obfuscated standdown periods.

- **Complementary pre-attack detection, mitigation, and prevention**
  Including ransomware and other malware variants in backup datasets compromises the future ability to recover—because restoring from a ransomware-riddled and malware-compromised backup after a devastating ransomware incident merely allows the cycle of malicious infection and disruptive encryption to begin again. Pre-attack detection, mitigation, and prevention capabilities are complementary to investing in a hardened recovery ability. Organizations must ensure they have both—either via wider offerings from their backup vendor or via a third party.

KEY ADDITIONAL REQUIREMENTS FOR MSPs

The essential minimum for MSPs looking to grow new revenue streams from backup, restoration, and failover services is that the key requirements for organizations are offered. If so, additional capabilities for MSPs are essential:

- **Multi-tenancy incorporated as a fundamental design decision**
  A backup, recovery, and failover service that works for MSPs must have multi-tenancy as a fundamental design decision. This means that administration capabilities for an organization, backup datasets, and system access are segregated for each customer, ensuring no intermingling of data across customer boundaries. At the same time, the MSP must have access to separate capabilities that enable unified administration across all customers.

- **Unified capabilities for managing customers**
  Provisioning, account management, setup for initial and recurring billing, reporting, data protection, customer branding, and more are needed by MSPs. Unified capabilities that enable administration at both the customer and service levels are essential.

A backup, recovery, and failover service that works for MSPs must have multi-tenancy as a fundamental design decision.

Conclusion

If organizations rely on backup datasets to recover after a ransomware attack, it is essential to do backup right. There is no point using a legacy backup solution that cannot outplay the realities of modern ransomware. We strongly recommend that organizations ensure they are using a backup solution that is fit for purpose against modern ransomware attacks.

About OpenText Cybersecurity

Ransomware attacks are becoming more sophisticated, which is why businesses need a modern backup and recovery solution to protect their business-critical data. Carbonite Server Backup is a scalable, secure solution with flexible deployment models, including cloud, on-premises and hybrid configurations that offers multiple layers of data protection so businesses can bounce back quickly after an attack.

Server Backup offers comprehensive, reliable, and proven security protection and support for over 200 operating systems, platforms and applications including physical, virtual, and legacy systems. It offers businesses a straightforward and reliable backup and recovery solution that securely preserves data confidentiality, integrity and availability while minimizing downtime for your day-to-day operations. For customers who want a white-gloved approach for implementation, management and recovery, we offer Carbonite Cloud Disaster Recovery to ensure continuity of IT operations and rapid recovery of your mission-critical systems—so you can bounce back from disasters even faster.

While a robust recovery solution is essential, it is just one element needed to help your business be more cyber resilient. OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention to detection and response, to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time contextual threat intelligence, OpenText Cybersecurity customers benefit from high-efficacy products, a compliant experience, and simplified security to help manage business risk.

Visit https://www.carbonite.com/products/carbonite-server-backup.

opentext™ | Cybersecurity

www.opentext.com

@OpenTextSec

+1 800 499 6544

[1] Osterman Research, CISO and CIO Investment Priorities for Cybersecurity in 2023, February 2023, at https://ostermanresearch.com/2023/02/15/orwp_0356/

[2] BlackFog, The State of Ransomware in 2023, March 2023, at https://www.blackfog.com/the-state-of-ransomware-in-2023/

[3] Bill Toulas, BianLian ransomware gang shifts focus to pure data extortion, BleepingComputer, March 2023, at https://www.bleepingcomputer.com/news/security/bianlian-ransomware-gang-shifts-focus-to-pure-data-extortion/

[4] FortiGuard Labs, 2H 2022 Global Threat Landscape Report, February 2023, at https://www.fortinet.com/resources-campaign/fabric-mesh/2022-global-threat-landscape-report

[5] BlackFog, The State of Ransomware in 2023, March 2023, at https://www.blackfog.com/the-state-of-ransomware-in-2023/

[6] Douglas Jose Pereira dos Santos, Key Findings from the 1H 2022 FortiGuard Labs Threat Report, August 2022, at https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings

[7] Steve Ranger, Ransomware Just Got Very Real. And It's Likely to Get Worse, ZDNet, May 2021, at https://www.zdnet.com/article/ransomware-just-got-very-real-and-its-likely-to-get-worse/

[8] Carolyn Cohn, Insurers run from ransomware cover as losses mount, November 2021, at https://www.itnews.com.au/news/insurers-run-from-ransomware-cover-as-losses-mount-572963

[9] Simon Kennedy, Goldman Analyst Warns Cyberwarfare Could Inflict Economic Costs, Bloomberg, March 2022, at https://www.bloomberg.com/news/articles/2022-03-07/goldman-analyst-warns-cyberwarfare-could-inflict-economic-costs

[10] Joe Tidy, 74% of ransomware revenue goes to Russia-linked hackers, BBC News, February 2022, at https://www.bbc.com/news/technology-60378009

[11] 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

[12] Cybereason, Royal Rumble: Analysis of Royal Ransomware, December 2022, at https://www.cybereason.com/blog/royal-ransomware-analysis