UNITRENDS

CHECKLIST

5 PILLARS OF RANSOMWARE DEFENSE

Mission-critical data now lives in more places than ever before — in data centers, on endpoints, in clouds and in SaaS applications. Through all the change, one constant remains — your data is perennially under attack. Ransomware is on the rise and continues to be a disruptive force for organizations of all sizes, across all industries.

Over the years, ransomware attacks have evolved into a multi-billion-dollar criminal enterprise, growing in frequency, sophistication and severity. In 2023, *attacks rose by 70%* compared to 2022. The year 2024 is off to a similarly torrid start, with more than 1,000 new victims posted to leak sites in Q1 2024.

Ransomware groups are using advanced tactics to lessen the chances of successful recovery and increase the probability of victims having to pay the ransom. These techniques include double extortion attacks, delayed payload execution, neutralization of backups and use of wiper attacks.

Businesses paid over *$1.1 billion in ransom* in 2023, nearly doubling the 2022 numbers. Excluding payouts, the average cost of an attack (detection, escalation, notification, post-breach response and lost business) increased by 13% year-over-year to $5.13 million.

Authorities and industry experts alike tout a complete business continuity and disaster recovery (BCDR) strategy as the most certain way to resume operations after an attack. At Unitrends, we've identified five pillars of defense: Secure, Protect, Detect, Test and Recover. In combination, these pillars are the best protection against ransomware.

The following checklist breaks down these categories and is designed to help you understand the different options in the market today. We've also outlined questions to ask your vendor to help you determine the right BCDR solution for your organization today and in the future.

1 SECURE

2 PROTECT

3 DETECT

4 TEST

5 RECOVER

1. SECURE

In response to widespread attacks on Windows machines, many organizations are transitioning away from malware-susceptible Windows-based backup software. Beyond hardening of the backup appliance kernel and standard environmental security measures, additional controls (such as Role-Based Access Control) should be available for further customization.

CAPABILITY/ ATTRIBUTE	DESCRIPTION	
Fewer Point Products	A multivendor protection strategy increases IT complexity, risk and cost. Deploying an all-in-one solution means managing fewer licenses and service agreements, and saves on management and technician time.	☐
Purpose-Built Appliance	A purpose-built turnkey data protection solution is easier to install, upgrade, service and manage.	☐
Non-Windows-Based Backup Appliance (i.e., hardened Linux)	Over 90% ransomware is Windows-based files or programs. Running a solution on a different OS (such as Linux) differentiates the backup environment from production. Further hardening of the appliance kernel and the hierarchical nature of the Linux OS makes them more difficult to compromise.	☐
Immutable Storage	Immutable storage enables you to store data in a format that cannot be modified or removed. This secures backup data from ransomware changes since no external client can read, modify or delete data once it's been ingested.	☐
Role-Based Access Control	Role-Based Access Control (RBAC) helps secure the backup environment from unwanted access. Each user may operate within the environment under a defined scope, limiting the operations they can perform or the assets they have access to, as required.	☐
Multifactor Authentication (MFA)	Multifactor authentication increases the security of your backup environment by enforcing the use of a second authentication mechanism, such as a time-based one-time password (TOTP), in addition to the user's password.	☐
Immutable Audit Logs	Immutable logs and routine monitoring ensure data being handled by your backup and recovery systems is being appropriately managed and accessed by staff.	☐
AES Encryption	Encryption secures data privacy both at-rest and in-flight. In addition to encrypting data backups, office email communication should be secured and any removable storage devices (HDDs, USB drives) should be encrypted.	☐
Integrated Anti-Phishing Defense	The email threat vector is used in more than 50% of system intrusion (ransomware) attacks. Integrated anti-phishing defense empowers end users to defend against phishing and account takeover attacks. Solutions that provide visual cues (i.e., banner notifications) alert employees to external senders, spoofed and/or imitated users and enable them to quarantine suspicious emails while automating workflows and feedback loops to streamline IT review and investigation.	☐

Questions to ask vendors

1. **How do you guarantee backups are secure against ransomware?**
2. **How do you store backups? Are they in native formats susceptible to attack?**
3. **What level of encryption do you offer for data? Is data encrypted in-flight, at-rest or both?**

2. PROTECT

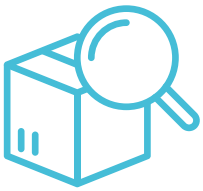
Whether your environment largely consists of endpoints, cloud applications (SaaS), cloud workloads (IaaS), physical servers, virtual servers or a mix of both, you need to be able to protect it all. Your solution should offer a number of different backup approaches to enable you to build a strategy to meet the unique needs of your environment. You may want to leverage agent-based, agentless protection, or a combination thereof to meet your recovery objectives.

CAPABILITY/ ATTRIBUTE	DESCRIPTION	
Wide Coverage of Protected Assets	To reduce the number of point products you need to rely on, your backup solution should be able to natively support hundreds of versions of operating systems, hypervisors and applications.	☐
Policy-Based Management	Admins should have the choice of how backups are scheduled, either by entering a specific schedule or using intelligent, policy-based scheduling technology.	☐
Data Reduction	Data reduction (deduplication, compression) reduces the overall size of files and eliminates redundancy among stored blocks, making movement, management and storage more efficient.	☐
Global Deduplication	As stated above, consider solutions that offer global deduplication across the entire backup volume. This enables more efficient storage utilization than job-based duplication, which reduces blocks on a per-job basis.	☐
Support for Hyperscale Clouds	Today's solution should easily integrate with hyperscale clouds, such as AWS or Azure, to protect IaaS workloads, store backups for off-site and/or long-term retention requirements, and enable disaster recovery.	☐
Support for SaaS Applications	Your business continuity and disaster recovery platform should offer dedicated backup and recovery for SaaS applications. Storing data outside of the production cloud (such as Microsoft 365) ensures a copy of data is secure and isolated from attacks or errors against the tenant.	☐
Purpose-Built Cloud	A cloud provider offering a dedicated cloud provides a turnkey solution specifically tuned to meet the needs for immutable off-site storage, long-term retention and disaster recovery. Key functions are delivered as-a-service, reducing the reliance on internal IT to develop DR as a core IT competency.	☐
Direct-to-Cloud Endpoint and Server Protection	All data is important. For systems such as PCs or remote servers that are not easily protected with a physical or virtual appliance, consider a vendor offering direct-to-cloud solutions to retain and store data securely in the cloud.	☐

Questions to ask vendors

1. **How do you get data off-site? What types of targets do you integrate with?**
2. **Do you offer dedicated cloud services? If yes, what security controls are implemented?**

3. DETECT



The latest innovations in ransomware include variants designed to overcome backup defenses with phased attacks aimed at defeating backups in a number of ways, typically including the use of gestation periods or dormancy. In the fight against ransomware, early detection means faster recovery. Backup vendors are increasingly making use of predictive analytics and machine learning to recognize possible attacks and alert administrators of abnormal fluctuations of data as backups are ingested, providing insights into data anomalies not found by security solutions such as antivirus.

CAPABILITY/ ATTRIBUTE	DESCRIPTION	
Predictive Threat Detection	Your solution should use machine learning to detect an active infection in near real-time. Artificial Intelligence (AI) is used to identify anomalies in data. Automatic notifications alert admins, enabling them to take immediate action to slow the spread and speed up recovery efforts.	☐
Data Loss Prediction	Utilize intelligent tools that simulate different disasters and outage scenarios to determine how much data would be lost in a downtime event. This will help you refine your strategy and ensure RPOs are being met.	☐
Internal Anomalous Monitoring and Detection	Secure servers, data and network with an AI-augmented solution that identifies threats that traditional security tools can't such as misconfigurations, unauthorized logins, new devices being added to the network, gaps in backups, admin rights being granted and more.	☐
Dark Web Monitoring	At a time when workforces are remote and cloud email adoption is at an all-time high, businesses have an even greater need for strong cybersecurity defenses. A compromised account grants hackers access to your network. Once they are in your network, they can use stolen credentials to further spread the infection. Look for a solution that includes built-in dark web monitoring to alert you of compromised or stolen credentials. Automated alerts enable you to quickly take proactive steps to secure those accounts before any malicious activity occurs.	☐

Questions to ask vendors

1. **Does your solution analyze for abnormal changes to backup data?**
2. **Do you alert to environmental anomalies and/or misconfigurations?**
3. **Do you flag and alert where backups may be potentially impacted by ransomware?**

4. TEST

Once backup and recovery processes are implemented, configured and running in production, it is critical to establish a cadence for regular recovery testing to ensure valid, recoverable backups in the event of a ransomware attack or other downtime event.

CAPABILITY/ ATTRIBUTE	DESCRIPTION	
Application-Level Certification	Legacy methods of testing, such as screenshot verification, leave much to be desired since they don't provide any means of identifying data corruption within backups or whether applications and services are functional upon recovery. Look for a solution that certifies backups at the application level, often through use of scripting, to verify workloads will perform as expected upon restore.	☐
Compliance Tracking	To understand whether or not your current backup strategy is sufficient to meet the RTOs and RPOs demanded by your organization's SLAs, ensure your solution enables tracking and reporting of Recovery Point and Recovery Time Actuals to ensure goals are being met.	☐
Automated Testing	Many organizations are unable to test backups and disaster recovery, often due to the significant investment of manpower and time required to execute it. Look for a solution that automates testing in a pre-determined, isolated environment on a set schedule according to predefined parameters such as boot orders, machine reconfiguration and application verification.	☐
Audit-Mode Restore	Audit Mode is a method of recovery by which you can selectively verify that particular machines can be recreated from any given recovery point. Isolated from production (no network connectivity), audit-mode restores verify that machines are booting correctly and that data is accessible. Upon verification, the audit-mode instance can be safely torn down.	☐
Exportable Reports	Your solution should provide exportable reporting on the outcomes of all testing to support compliance with your DR plan.	☐

Questions to ask vendors

1. **How does your solution test for recovery? Do you have an approach more thorough than screenshot verification?**
2. **What automation is available for recovery testing?**
3. **How does your solution report on the outcomes of testing?**

5. RECOVER

The required recovery efforts following a ransomware attack will vary from case to case. When the infection is caught early on, replacing infected files may prove sufficient. In other cases, rebuilding a portion or the totality of your environment may be required. After an attack, you need to have several options available to restore operations as quickly as possible.

CAPABILITY/ ATTRIBUTE	DESCRIPTION	
File Recovery	Should the infection be caught early on and contained to specific systems, removing the malware and recovering any infected files may prove sufficient. Your solution should make it intuitive and easy to find and restore individual files from backups with only a few clicks. Indexed search capabilities and self-service capabilities (with role-based access control) enable quick recovery.	☐
Flexible Recovery Options	Your solution should be flexible in both how you can recover assets and where you can recover data to. Look for solutions that support a wide range of recovery modes including physical-to-virtual (P2V), V2V, V2P and replicas.	☐
Instant Recovery	In the wake of an attack, it is imperative to respond as quickly as possible to stop the infection, investigate, remove the threat and recover. If a server or VM is attacked, your appliance should be able to orchestrate failover to bring applications back up from your most recent verifiable backup with a near-zero RTO.	☐
Bare Metal Recovery	Bare Metal Recovery (BMR) technology is used for disaster recovery of protected assets. BMR enables system and application recovery across servers from different vendors and hardware configurations.	☐
Disaster Recovery-as-a-Service (DRaaS)	Reduce cost, complexity and time-to-recovery in the wake of an attack with DRaaS. DRaaS providers deliver rapid spin-up of critical systems and applications in a secure cloud location and help you reroute user traffic until the on-prem site is operational.	☐

Questions to ask vendors

1. **Can you deliver near-zero RTOs for VMs, databases and file shares?**
2. **What recovery options are available for recovery to alternate/dissimilar targets?**
3. **Do you index files for search capabilities?**

CONCLUSION

Defense against ransomware requires a multipronged, continuous effort from end-user training and awareness to security controls and a well-tested BCDR strategy. Unitrends, as part of your BCDR solution, provides protection against and enables quick recovery from these advanced threats **through our five pillars of defense:**

SECURE, PROTECT, TEST, DETECT AND RECOVER.

LEARN MORE

TODAY!