UNITRENDS
A Kaseya COMPANY

DETECTING AND MITIGATING RANSOMWARE WITH UNITRENDS UNIFIED BACKUP

ADAM MARGET, Product Marketing Manager

MOHAMMAD AL-SHAFIE, Global Director, Sales Engineering

INTRODUCTION

Data lives in more places than ever before and is constantly under attack. Ransomware remains one of the most pervasive cyberthreats today. According to Corvus Insurance's Q3 2023 Global Ransomware Report, global ransomware attacks increased significantly, with their frequency increasing by 95% year-over-year.[1] As of October 2023, over 4,000 ransomware victims were listed on leak sites, surpassing the number of ransomware victims in 2022 (2,670).[1] Even more alarming are the financial costs associated with the resulting downtime. The Cost of a Data Breach Report 2023 found that the average cost of a ransomware attack increased 13% from $4.54 million to $5.13 million compared to the 2022 report.[2] When you factor in reputational, operational and other costs associated with a ransomware attack, the resulting downtime can be a death knell for businesses, particularly SMBs.

Amid this ever-expanding threat landscape, 70% of SMBs admitted the impact of a ransomware attack would be extreme or significant.[3] Ransomware's success in overcoming traditional security mechanisms places backup and disaster recovery solutions among the most important aspects of any cyber resilience plan.

Unitrends Unified Backup helps enhance cyber resilience by protecting critical workloads no matter where they are stored — on-premises, in cloud platforms or SaaS applications. Powered by AI and automation capabilities, Unitrends simplifies manual and time-consuming backup and recovery processes, enabling you to recover from data loss and cybersecurity incidents confidently. With regards to architecting, deploying and utilizing the Unitrends platform to safeguard against cyberattacks, we've identified five pillars of defense that, in combination, offer you the best protection against ransomware and enable 100% proof and confidence in recoveries to come:

In this paper, we expand upon these five pillars and take a closer look at these capabilities in the context of Unitrends Unified Backup platform.

1

SECURE

With annual revenue in the billions and growth projection in the double digits, ransomware has become a highly lucrative multibillion-dollar business model for cybercriminals today. The soaring popularity of open-source versions of ransomware and the proliferation of delivery models like Ransomware-as-a-Service (RaaS) make ransomware threats grow in number and complexity each day. New variants and more sophisticated techniques are increasingly coming to the fore, rendering many existing defense mechanisms inadequate. According to the AV-TEST Institute, over 450,000 new malware and potentially unwanted applications (PUA) are detected every day.[4]

Ransomware security in particular is a major concern for enterprises running Windows operating systems. Over 90% of ransomware leverages Windows-based executables.[5] According to the Common Vulnerabilities and Exposures (CVE) database, Microsoft has more than 748 vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 7 (High Risk).[6] Despite these vulnerabilities, Windows systems represent a huge share of the global OS market, with around 70% market share.[7] Windows is the prime target for threat actors, accounting for nearly 90% of all malicious files detected daily.[8] The sheer volume of Windows machines worldwide means cybercriminals will get the greatest returns by tapping into this market. In response to widespread attacks on Windows machines, many organizations are transitioning away from malware-susceptible Windows-based backup software.

By contrast, infections on Linux operating systems are far less common. Linux has a 3.82% market share of desktop OS and a 15.20% market share of server OS.[9, 10] In addition to being far less common, and thus less lucrative for prospective attackers, the hierarchical architecture of Linux systems makes them more difficult to compromise.

Unitrends understands the advantages of this solution and has the functionality to deploy a Linux-based virtual appliance for VMware ESXI, Microsoft Hyper-V and Nutanix Acropolis (AHV), or as a purpose-built, turnkey hardware appliance. Hardening of the appliance's kernel helps in creating a more secure system, and additional security measures can be implemented upon installation to limit the number of ports used by the appliance. The appliance forces you to change the appliance root password during initial installation, so be sure to select a secure password different from the default.

Unitrends appliances utilize agents to protect physical systems (and, in certain situations, for more granular protection of virtualized servers or applications). For the protection of Windows-based assets, Unitrends utilizes Secure Agent Pairing to automatically establish secure TLS communication between the agent and appliance. TLS encrypts data and authenticates the connection between appliances and agents, preventing unauthorized communication to the Unitrends agent.

You will also want to secure your backup server behind company firewalls. A backup server or appliance should never be on a public-facing IP address or unfiltered NAT. Many Unitrends customers deploy and operate their solution on air-gapped networks. This keeps the backup appliance completely isolated, without any loss of functionality (such as Unitrends predictive analytics engine for detecting ransomware anomalies). Your goal should be to make access to the system as difficult as possible for any potential attackers.

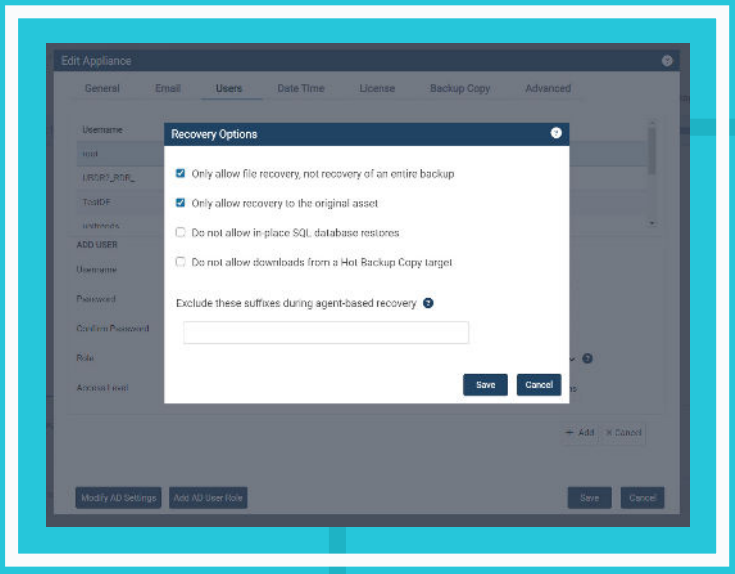
Beyond hardening of the appliance kernel, agents and environmental security controls, role-based access control (RBAC) enables individual self-service within a predefined scope. Active Directory authentication may also be enabled. Each user's scope may be defined by operations they can perform within the backup environment (i.e. Recovery Operator can only initiate a restore) as well as by systems and backups they have access to. If a particular user or group would benefit from self-service over a subset of your environment, you can easily configure user roles to meet those requirements without opening up unfiltered access to the full backup environment. RBAC can be applied at the appliance level, protected asset level and task level for each user. Each user account is assigned a role that defines the types of operations the user can perform on the appliance.

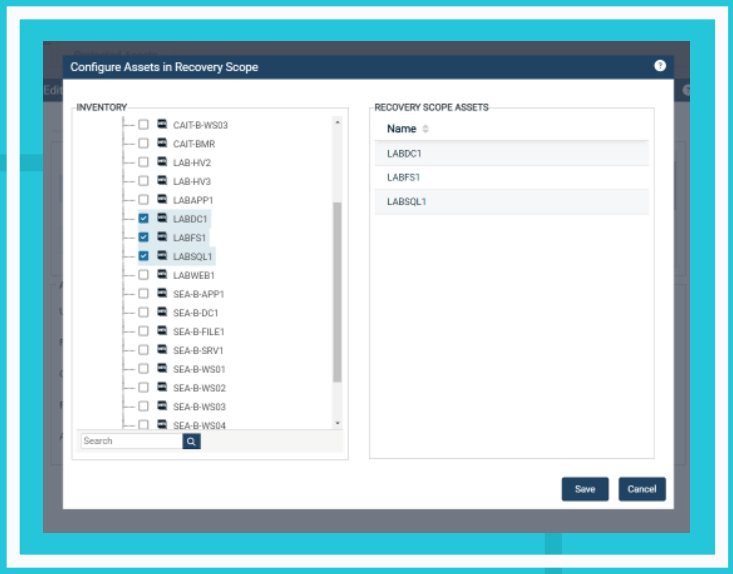
The example below shows screenshots of the configuration steps for adding a Manage level user assigned as a Backup/Recovery Operator for a specific set of machines with Recovery Options limited to only file-level recovery to the original protected asset. Additional options can be applied to further define what and how the user can recover (for example, recover only files, recovery only to the original asset, etc.).

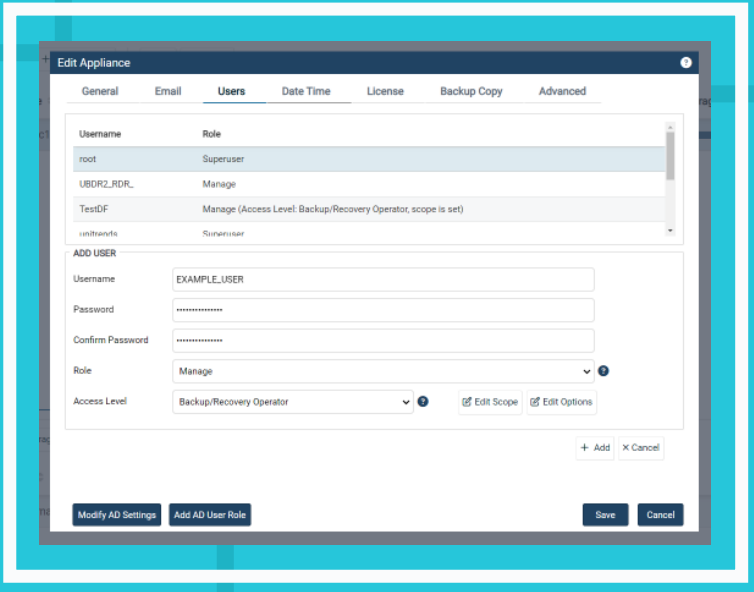
Enhancing security and management with Unitrends UniView

Unitrends UniView is a free, SaaS-based management platform providing UI and API integration across Unitrends backup and recovery modules, including Unitrends physical and virtual backup appliances, SaaS backup for Microsoft 365, Google Workspace and Salesforce, endpoint backup and backup for public cloud workloads.

Beyond unified management across modules and integrations, UniView offers additional layers of security for your backup environment. The UniView portal is protected by two-factor authentication (2FA) using a time-based one-time password (TOTP) authenticator application. From UniView, you can block access to the local UI of your backup appliance(s), ensuring that all users are verified by 2FA. UniView also allows you to restrict local network access, significantly reducing the attack surface of your Unitrends appliance.







2

PROTECT

Unitrends offers compatibility for backup and recovery of more than 200 versions of operating systems, hypervisors and applications. Regardless of whether your environment is largely physical servers, virtual servers or a mix of both, you can protect it with Unitrends.

A number of different backup approaches enable you to build a strategy to meet the unique needs of your environment. Leverage agent-based, agentless protection, or a combination thereof, to meet your recovery objectives. Consider the following:

Recovery Method	File-Level Protection	Image-Level Protection	Host-Level Protection	Application-Level Protection
Granular Item Recovery (files, folders)	✓	✓	✓	✓
Original Target	✓	✓	✓	✓
Bare Metal	✓	✓	✗	✗
Physical to Virtual (P to V)	✓	✓	N/A	✗
Instant Recovery (original or different host)	✓	✓	✓	✗
Replica(s)	✓	✓	✓	✗

Refer to the Unitrends Admin Guide for full documentation of best practices and supported methods.

Beyond local backup and recovery functions, it is strongly recommended that you follow the 3-2-1 rule of backup at the very least.

This means a minimum of three (3) copies of your data, stored on two (2) different formats, with one (1) copy going off-site or immutable (unable to be modified).

Unitrends offers a variety of options in order to achieve redundancy and immutability for your data. Immutable media may be rotational media, such as disk or tapes, that are physically disconnected from the network once the backup copy job is completed and is taken off-site and stored at a secure secondary location. Some vendors offer immutable storage via a cloud service. This includes our own Unitrends Forever Cloud. Once written to the cloud target, objects cannot be changed or deleted until the end of their specified retention period. Your appliance has the ability to access any backup copies replicated to the Unitrends cloud in an on-demand, self-service fashion. Backup copies are stored in the cloud in a ready-for-recovery state and are accessible right from your local appliance user interface (UI) without any egress or per-incident charges.

In addition to the Unitrends Cloud, Unitrends supports replication via Backup Copy to a variety of different targets and media:

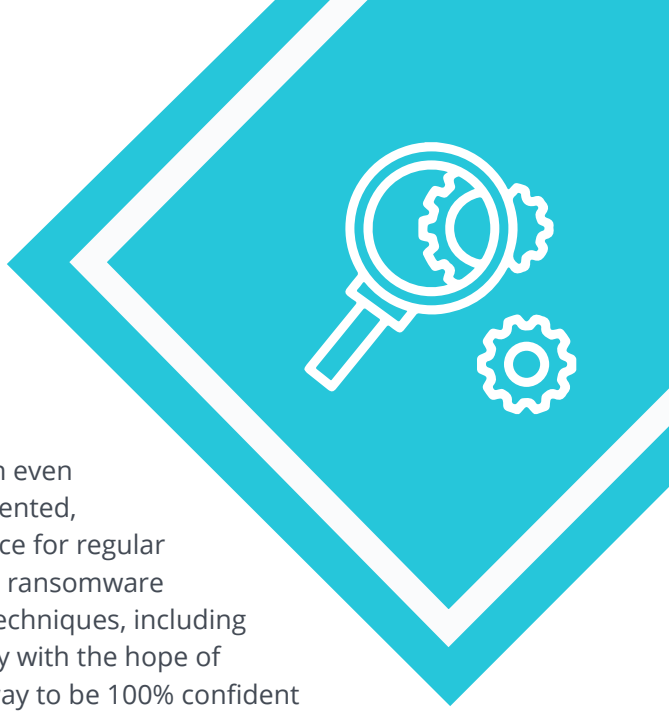
Backup Copy Target	Supported Protocols
NAS	CIFS, NFS
SAN	iSCSI, Fibre Channel
HDD/Disk	USB2, USB3, eSATA, SAS
LTO/Tape	SAS, SCSI, Fibre Channel
Public Cloud	› AWS S3, AWS S3-IA › Google Cloud Storage Standard › Google Cloud Storage Nearline › Rackspace › Wasabi Cloud › Azure Blob

The Unitrends backup appliance may be configured as a backup appliance, replication appliance (receiving and storing backup copies for DR), or both backup and replication, if it is necessary to have the appliance perform both roles.

When following best practices, it is recommended to store backups on your local appliance and on a hot target (such as a secondary appliance or Unitrends Cloud), where data is immediately available for recovery with a third copy on cold media, such as disk, that's taken securely off-site (off-network and immutable). Keep in mind that recovery from cold media, such as disk or tape, will have a longer Recovery Time Objective (RTO) as compared to a hot target. Use a combination of local and replicated backups to achieve local recovery objectives, meet long-term retention requirements, secure a copy of data from attacks on your local network, and enable disaster recovery.

3

TEST



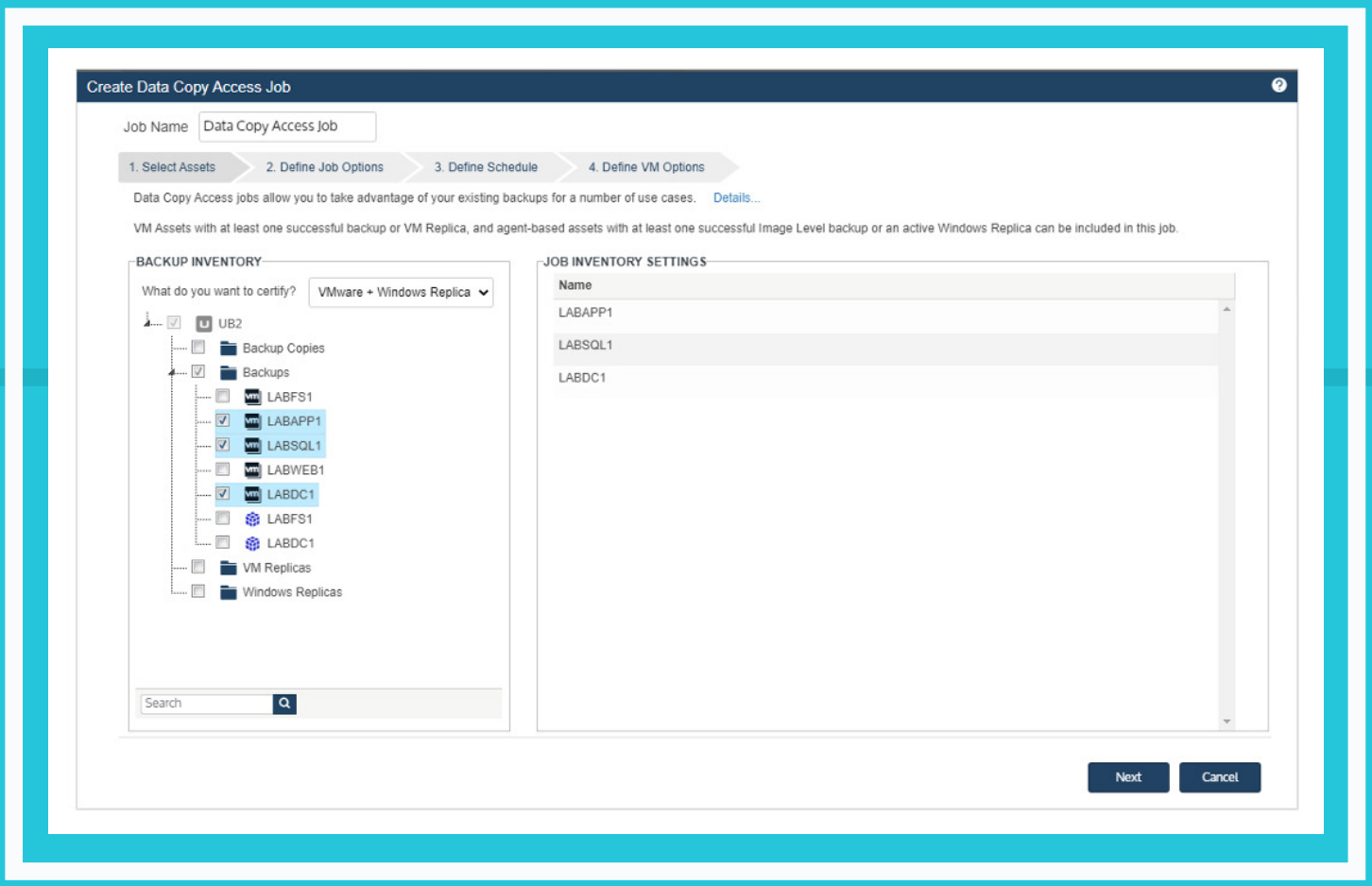
IT environments today are not always well suited for backup and often even less so for recovery. Once backup and recovery processes are implemented, configured and running in production, it is critical to establish a cadence for regular recovery testing to ensure valid, recoverable backups in the event of a ransomware attack or other downtime events. With the evolution of ransomware techniques, including attacking environmental utilities such as VSS, and periods of dormancy with the hope of having the malware backed up along with legitimate data[11], the only way to be 100% confident in a successful recovery is by testing your backups. This testing is also helpful for identifying clean points of recovery after an attack.

Some methods of testing, such as screenshot verification, may leave much to be desired when it comes to ransomware recovery since they don't provide a way of identifying data corruption within backups or whether applications and services are functional upon recovery. With regards to ransomware recovery, screenshot verification may leave users with a false sense of security. Ransomware contained within backups may not disable your operating system or boot volumes since it wants to display its ransom messages and instructions for providing payment upon login to the machine. To be fully confident in your DR strategy, you need proof that all data and services are recoverable at the application level.

Unitrends helps organizations automate backup verification and recovery testing with Recovery Assurance. Recovery Assurance enables deep, application-level testing for both simple and complex environments and offers full control over configurations of boot order dependencies, networking and application-specific tests. If you're looking for a quick test to simply determine whether a machine is bootable, you can leverage screenshot verification methods as well.

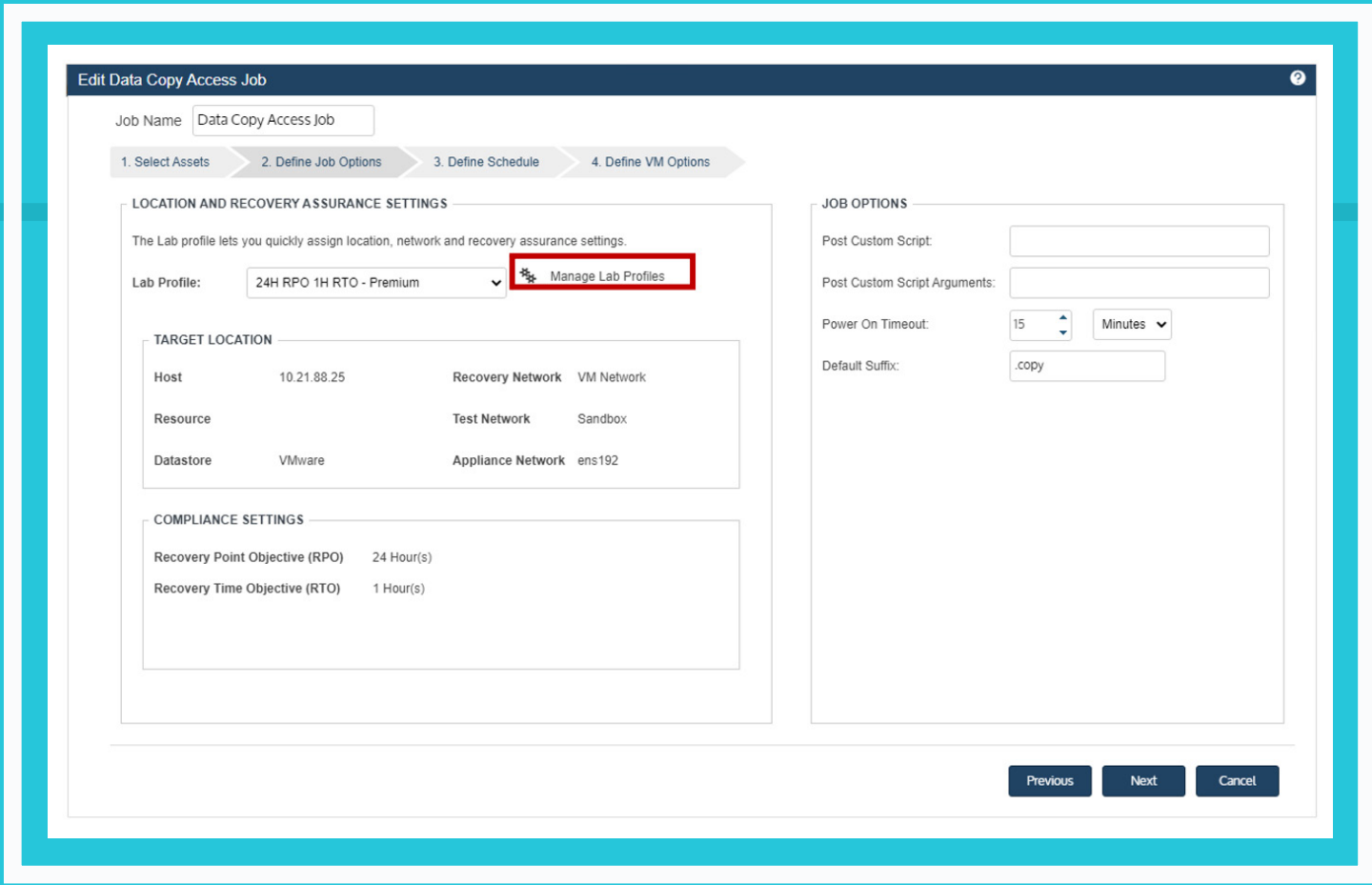
The only way to be 100% confident in a successful recovery is by testing your backups.

The screenshots below show how Recovery Assurance testing is configured via a **Data Copy Access (DCA)** job. In this case, we have VMware host-level backups of a domain controller, SQL host and an application server that will be tested. You can also test backup copies replicated to the appliance as well as any VM or Windows replicas.



Select from your backup inventory the assets you want to test.

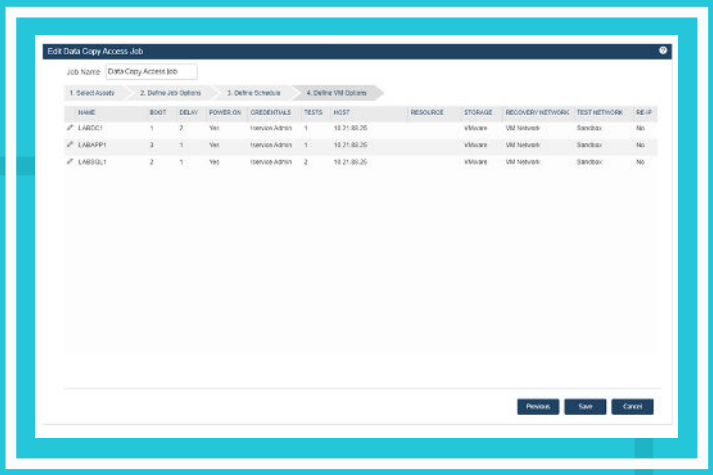
After determining the backups you want to include in your DCA job, the next step is determining the location in which you will run testing. DCA jobs can be created on your local source appliance, managed appliances or any distributed appliances. The DCA job will create a VM for testing either on the appliance directly (on-box DCA, Recovery Series physical appliances only) or on a selected virtual host (on-virtual host DCA). The steps required vary by where the DCA VMs reside. On-box DCA jobs will automatically create a lab profile for testing. For on-virtual host testing, you will need to create a lab profile that enables you to apply consistent settings across multiple DCA jobs. Depending on testing requirements, you can create additional profiles to test alternate locations and/or compliance settings for RTO and RPO tracking.



Manage Lab Profiles to configure Target Location and Compliance Settings.

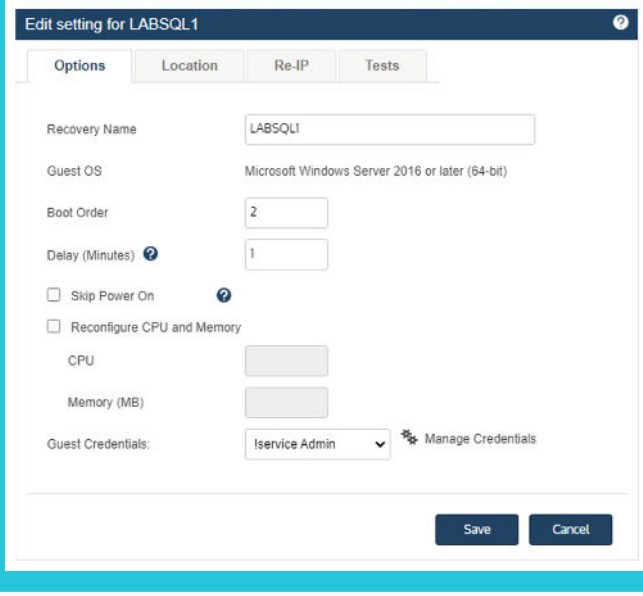
Once the job inventory and lab profile have been configured, you will need to set a custom schedule for testing and configuring VM Options. Configuration of VM Options is used to perform a number of different tests, from verifying service profiles, reconfiguring the recovery VM and executing application-level tests to validate data integrity and service functionality. This deep level of testing certifies backups at the application level. You can leverage 50+ canned application test scripts or write your own custom arguments.

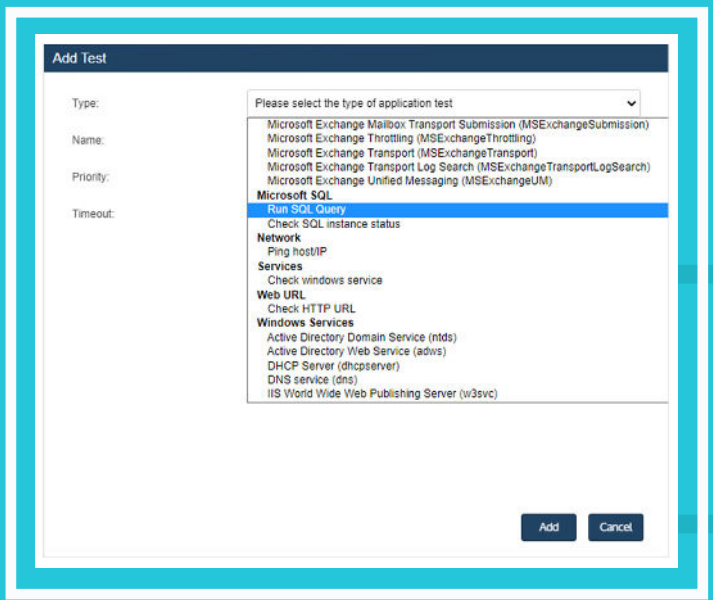
The screenshots below show the job inventory and a summary of the VM Options configuration and drill down into advanced configuration options for our SQL server LABSQL1.



A guided wizard assists in configuring boot orders, defining credentials, application tests, and more under the Define VM Options step.

Customize settings for each individual recovery instance.

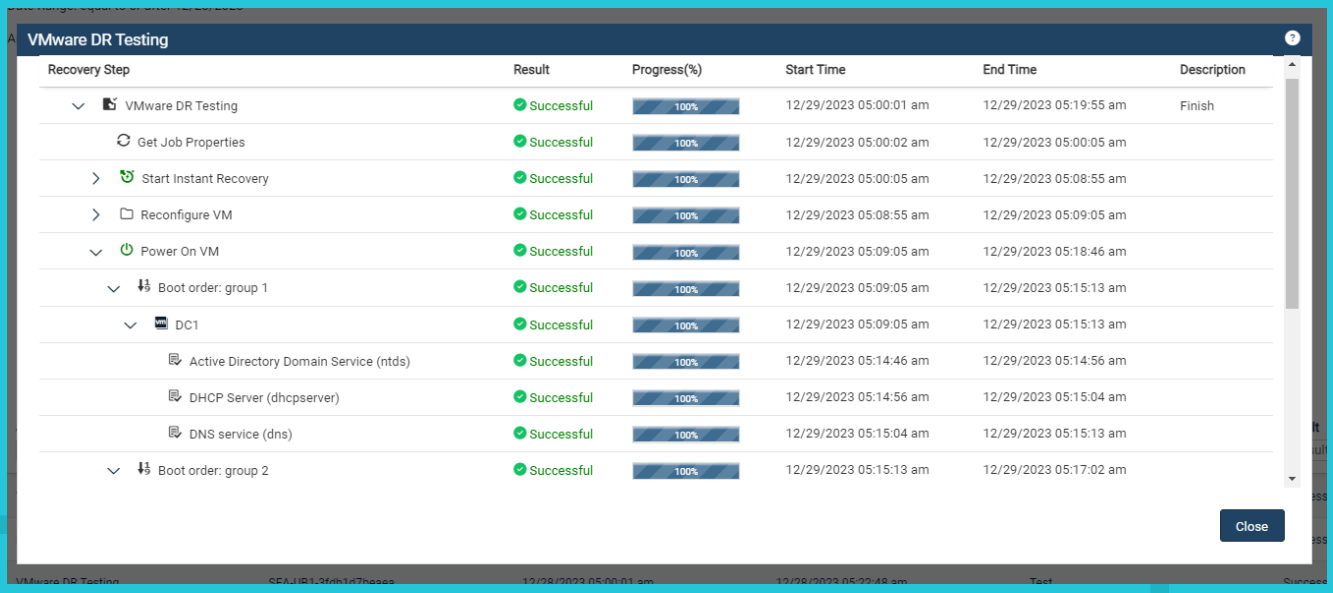




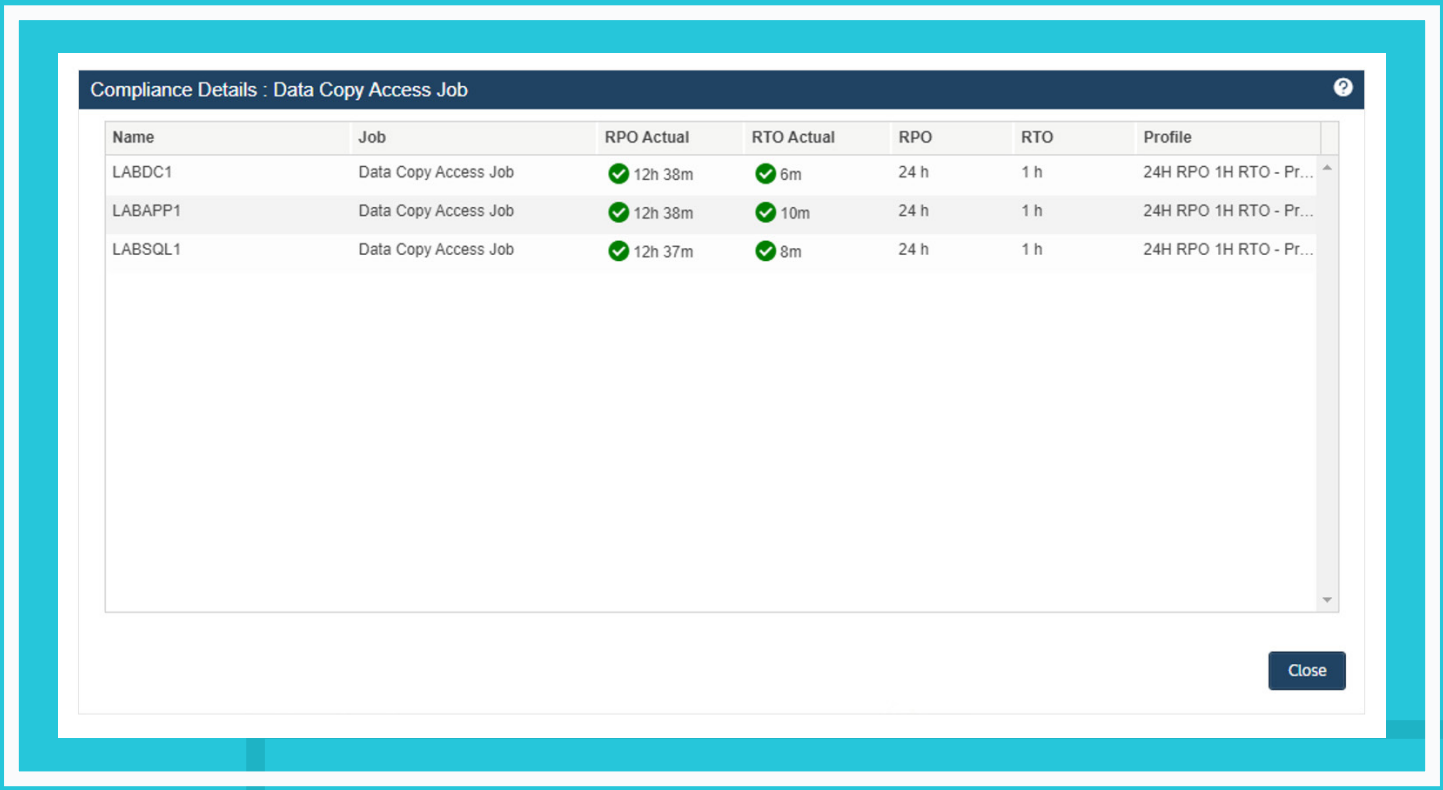
Choose from more than 50 canned application tests and/or write your own scripting to further customize your tests.

Data Copy Access automates testing for both simple and complex environments to provide 100% proof and confidence in your recovery to come. The job runs according to the defined schedule and produces two key reports: Recovery Assurance and Compliance. Reporting functionality is native to the appliance; you do not need to add proxies, third-party databases or resources beyond the configured testing location (for on-virtual host testing). You can export either report in .csv or .pdf formats directly from your appliance.

Recovery Assurance details the results of the application-level tests and indicates results as Successful/Warning/Failure. The Compliance Report presents results from RTO & RPO tracking as either Success (meets RTO and RPO) or Failure (fails to meet RTO, RPO or both). Insights from testing results can be used to adjust schedules and/or backup approaches to better meet compliance, address environmental issues impacting restore and identify any bad backups in advance of needing them for recovery efforts.



Each step in the recovery process is detailed, from which you can identify potential risks and errors, and perform any remediation required prior to an actual DR event.

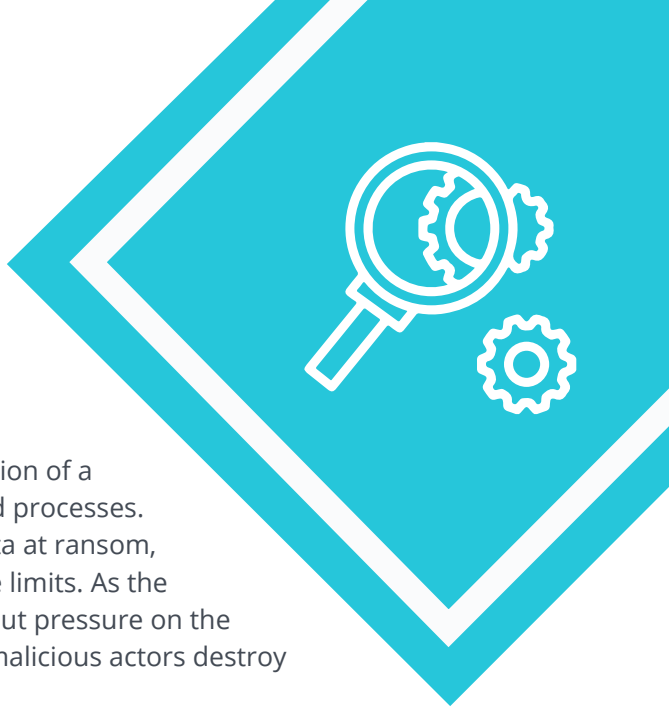


Machine spin-up and application-level tests are executed and RTO is validated. Recovery Assurance tests your most recent backups, providing you with an RPO relative to your testing schedule.

In addition to orchestrating Recovery Assurance, the Data Copy Access job also offers **Instant Lab** and **Failover** modes. Instant Lab enables access to production data in fully functional virtual machines (VMs) contained within preconfigured, isolated testing labs. Prior to restoring machines into production, the Instant Lab may be used to spin up machines from backups for additional testing. This may include the use of third-party cybersecurity tools to perform scans and ensure that backups being used in recovery efforts are clean and free of malware or ransomware, in addition to Recovery Assurance tests that validate functionality.

4

DETECT



Early generations of ransomware detonated their payload upon infection of a system, immediately encrypting data through transparent background processes. Once complete, the malware deletes the encryption key and holds data at ransom, usually demanding payments in stages based on pre-determined time limits. As the ransom goes unpaid, the malware starts to delete files at random to put pressure on the victim. If the ransom still isn't paid at the expiration of the time limit, malicious actors destroy their side of the key, leaving the data irreparably damaged.

Both industry experts and IT practitioners have long touted backup (collectively, "backup" may refer to dedicated backups, replicas or snapshots) as the best defense against ransomware. Unfortunately, cybercriminals know this as well and ransomware merchants are constantly trying to up their game to overcome security and backup defenses. The latest innovations in ransomware include variants designed to overcome backup defenses with phased attacks that aim to defeat backups in a number of ways, typically including the use of gestation periods or dormancy.[12]

While conventional ransomware attacks usually demand ransom after data encryption, novel attacks often utilize a double-pronged strategy. The attackers first gain access to the victim's network without their knowledge and spread laterally as far as possible, exfiltrating the maximum organizational data. It's only then they will carry out ransomware deployment. The damage would have already been done by the time the victim learns about the infiltration. When organizations refuse to pay the ransom, the hackers release portions of the data to heighten the pressure on them. The report by BlackFog found that 89% of ransomware attacks exfiltrate data, making them a growing concern for businesses of all sizes.[13]

Unitrends appliances are constantly on the search for ransomware threat conditions.

The three critical aspects of these sophisticated attacks are:

01

Gestation

Modern ransomware does not detonate and encrypt immediately. The gestation period is designed to give the malware time to spread as widely as possible from machine to machine, typically by using the permissions of the systems it has infected. It's also the time during which data exfiltration is carried out.

02

Deletion

Once the ransomware has spread as far as it can, the next phase involves deleting network-accessible backups. Backup files have known signatures that make them easy to target and encrypt. In addition to targeting file signatures, ransomware uses APIs published by backup vendors to delete backups autonomously.

03

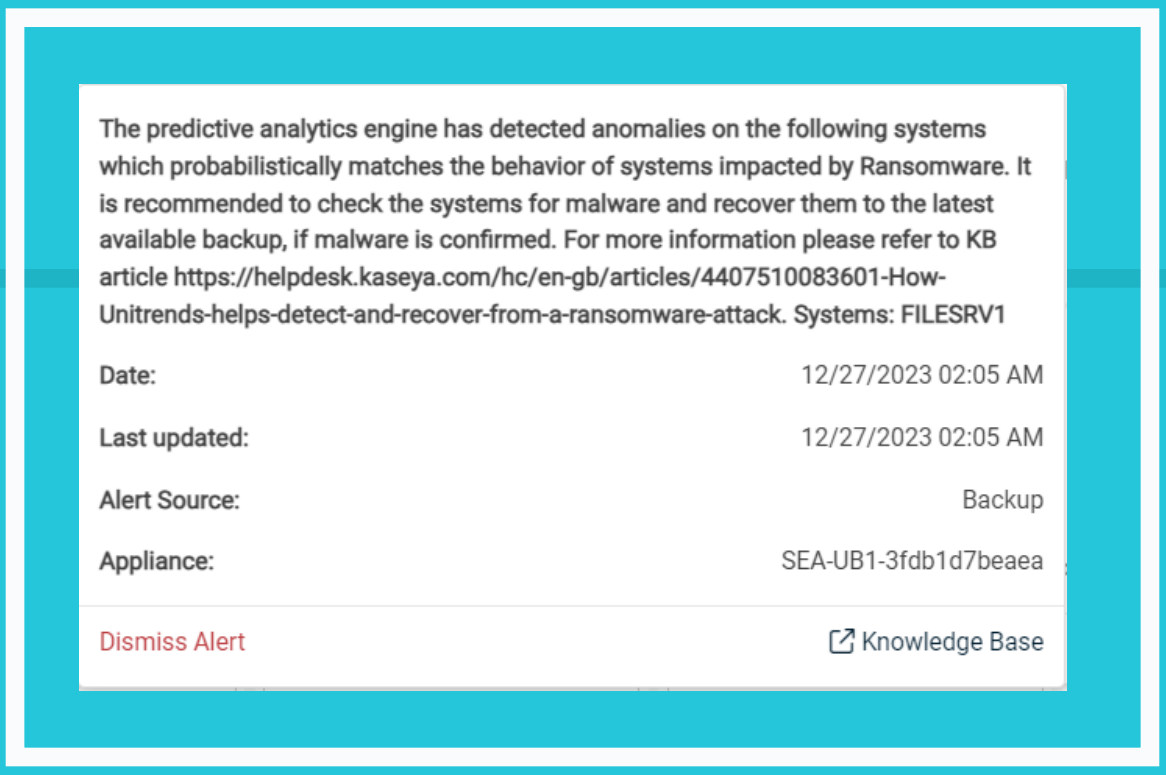
Dormancy

Once spread, ransomware typically does not encrypt or delete backups immediately. With access to data, threat actors may begin extracting data to later use for extortion. The malware may lie dormant for one, three, six or even "n" months before detonation. Dormancy poses a challenge because malware is backed up along with legitimate data, creating an attack loop. When infected backups are used in recovery, the malware remains present and will detonate again.[14]

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. This provides visibility beyond antivirus and security tools since traditional AV solutions compare the code they scan to the code that exists in their database. This means that it may be months before AV providers catch up to newer variants, to say nothing of zero-day threats. Traditional security tools are not sufficient as a standalone defense. In fact, most organizations infected with ransomware run up-to-date endpoint protection.

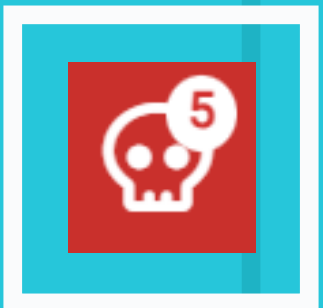
Unitrends appliances are constantly on the search for ransomware threat conditions. Predictive analytics and machine learning run during every backup, analyzing data based on a number of heuristics, including data entropy (the randomness of file changes, not just change rates), to identify backups infected with ransomware. Upon detection, email and dashboard alerts are immediately sent to administrators and all suspected backups are flagged with an icon in the UI to prevent recovery attempts using infected backup files.

The below screenshot is an example of the dashboard alert. Unitrends communicates the potentially infected systems, the appliance that detected the anomaly, the process during which abnormalities were detected (in this case, a Backup Job), as well as the initial date of the alert and subsequent updates. Use this information in coordination with Backup History and Recovery Assurance reports to identify your most recent, clean, recoverable backup point.



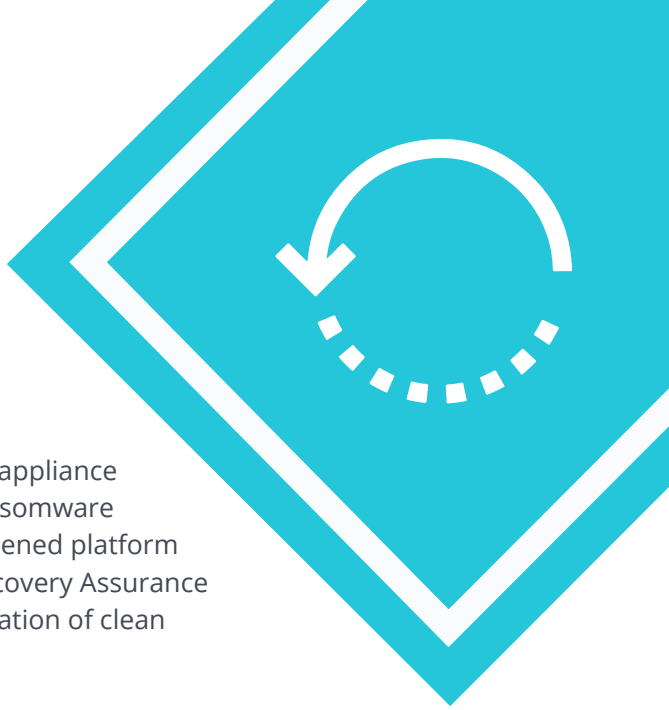
Example of a Unitrends Ransomware Detection alert, identifying system, time detected and alert source.

The icon at the top of your UI displays as a red skull icon when a predictive analytics engine alert is triggered.



5

RECOVER



Unitrends helps protect the backup environment — from a hardened appliance kernel to various options for offline, immutable storage — against ransomware in a number of ways. However, no defense is 100% effective. The hardened platform in conjunction with our predictive analytics engine and automated Recovery Assurance testing provides insights into the onset of an attack as well as identification of clean recovery points.

Should you fall victim to a ransomware attack, it is critical to isolate the infection to stop the spread before working towards recovery. In response to an attack, consider the following steps:

1

Isolate impacted systems

Unitrends uses predictive analytics for ransomware detection that gives you a leg up when combating fast-moving attacks before they propagate fully. The success of a ransomware attack is predicated on how quickly it can spread across your network. Responding as quickly as possible can greatly impair the infection from spreading and reduce the impact on your organization. Upon detection or suspected infection, first isolate all devices in question from other computers and storage devices. Shut down infected machines and disconnect them from all network communications, both wired and wireless, and remove any external storage devices. Be warned that there may be more than one “patient zero” and malware may be lying dormant or not yet visible on some systems. Treat all connected and networked devices with an abundance of caution and apply measures to ensure asymptomatic systems are not infected. Powering off any devices that have not yet been infected can help contain the damage. Additionally, suspend all backup schedules until you have a full understanding of the infection origins and spread, and have completed all security forensic efforts to identify impacted systems and any potentially affected backups.

2

Identify the ransomware

Ransomware will often identify itself when it asks for ransom. A number of online resources are available to help you identify the ransomware. Identifying the strain helps to understand how the malware behaves, what files it encrypts, where it hides its code within your device(s), and what options may exist for removal and recovery. You may start by assessing any machines that were accessed by "patient zero." Checking the ransomware registry will help identify encrypted files since the malware uses the registry to know which files to decrypt when the ransom is paid. Consult your security team or the proper authorities to conduct forensics. Identification of the ransomware strain is also useful when reporting the attack to the authorities, which is a recommended step.

3

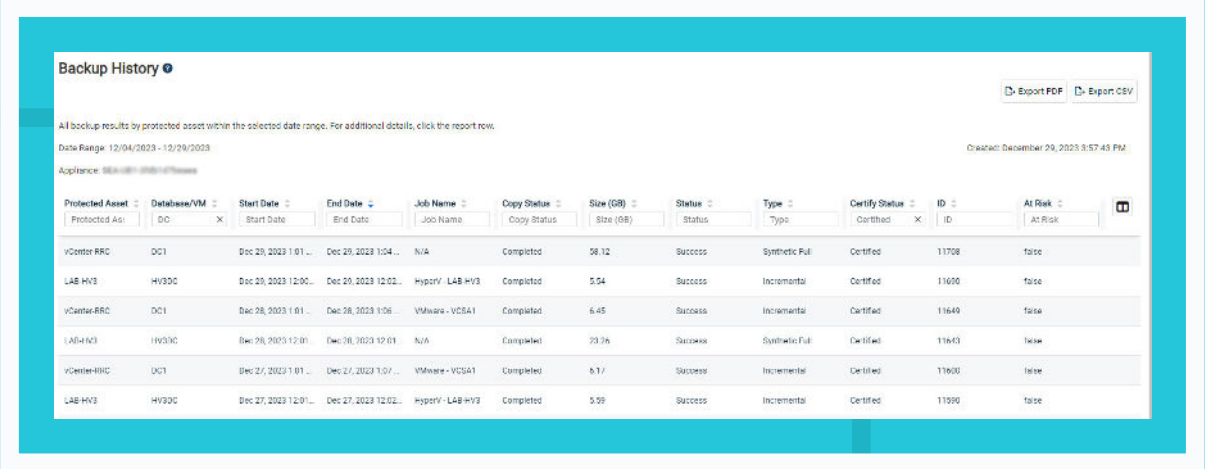
Report the attack

The FBI encourages victims to report ransomware incidents regardless of the outcome. This provides law enforcement and cyber defense organizations with a greater understanding of the threat and may prove useful in investigations and other ongoing cases.

4

Validate your backups

As discussed previously, advances in ransomware include operations to disable or damage backups. In preparing for recovery, you must ensure you have clean, validated backups. Unitrends Recovery Assurance testing validates backups down to the application level. Combine this with predictive analytics to identify the time at which anomalies were detected. You can cross-reference Recovery Assurance and alert timestamps against your Backup History report to identify backups that may be at risk. See the below screenshot for an example of filtering columns on the Backup History report to show all backups of the protected asset (LABDC1) that have been certified by Recovery Assurance in the defined date range.



Should you need to recover further back than your on-appliance retention, import data from Backup Copies that were replicated to an immutable target such as the Unitrends Cloud or removable hard drives.

5

Confirm retention

Investigation, analysis and remediation efforts take time following a ransomware attack. These timelines may be impacted when engaging with cyber insurers as well. During this time, it may be in your best interest to extend on-appliance retention (retention of local backups) so that backups do not expire prior to completion of remediation efforts, thereby ensuring you have clean, recoverable backups from prior to the infection.

6

Determine your options

The required recovery efforts following an 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 have several options:

Pay the ransom

Authorities and industry experts agree it's generally a bad idea to give in to the ransom demand and pay up. Payment encourages further criminal behavior and emboldens the attackers with each successful ransom paid, perpetuating the cycle and increasing the ransoms demanded of future victims. As per the recent report, ransomware groups are using multiple extortion strategies to maximize damage to victim organizations.[14] In many cases, decryption does not go as expected either. The encryption methods used by these malwares are not always clean.

Do nothing and accept the data loss

Organizations who lack a sound business continuity and disaster recovery strategy, or are unable to find a decryptor, may choose not to recover their damaged files. Naturally, a strong ransomware remediation plan should be developed, implemented and tested following any such attack to ensure rapid response and recovery in the event of a future attack.

Try to remove malware, select restores of affected system(s)

Depending on the type of ransomware, removal ranges from simple to impossible. Lightweight scareware attacks install a malicious program that can be removed in minutes, but the more common and well-known variants fall into the filecoder or encryption ransomware category. These are much more challenging to remove. While you may manage to remove the malware itself, you still need to decrypt valuable files to access your data. Rather than deleting your data, the malware encrypts and holds it hostage until you pay for the decryption key. Every filecoder has its own method of encryption, making it more difficult to remove than other forms of malware. Compounding this problem, most ransomware deletes itself after a period of time to avoid being studied and decrypted. If you're able to identify which type of ransomware has infected your system, you may find a legitimate ransomware decryption tool, such as those offered by Avast Antivirus and others. Should you look for a decryptor, proceed with caution. Ransomware often uses enterprise-grade encryption, which is impossible to crack. There's a criminal aspect to decryption as well, with threat actors looking to take advantage of people in this situation by tricking them into downloading more malware under the guise of fast, effective decryption.

Wipe system(s) and rebuild from backups

The most reliable way to be certain that ransomware has been eliminated from a system is to completely wipe all devices and reinstall from scratch. Reformatting hard drives will ensure no remnants of malware remain on the system. A complete rebuild is an intensive effort and you may be tempted to use a System Restore point to bring a machine back to a running state. This is not recommended, however, since ransomware often buries itself into obscure places throughout the system making it difficult to root out. This may include hiding in Temp folders, .INK files and the Windows Registry, where the malware modifies registry keys to establish a foothold within the network and deploy additional malware each time the OS is launched. Recovery from (tested) backups ensures you can restore affected machines to their most recent, clean recovery point. Comprehensive testing, as with Unitrends Recovery Assurance, is critical to any ransomware remediation strategy.

Unitrends helps protect the backup environment — from a hardened appliance kernel to various options for offline, immutable storage — against ransomware in a number of ways.

UNITRENDS RECOVERY

There are a number of backup approaches you can leverage with Unitrends to meet the needs of your environment. As outlined in the "Protect" section, Unitrends supports File, Image, Host and Application-level backups. Your recovery goals (RTO, RPO, granularity, flexibility) should be used in part to inform your backup strategy. While the options detailed here are not all-inclusive, we have identified a few key recovery processes that may prove valuable in recovery from a ransomware attack.

Consult the **Unitrends Administrator Guide** for additional documentation and consider the following recovery approaches:

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. Once you are ready to restore impacted systems, Unitrends Instant Recovery enables you to quickly recover VMs running any operating system. Instant Recovery enables you to recover a failed machine from VMware or Hyper-V Host-Level backups or from a Windows Image-Level backup. To perform instant recovery, you specify the recovery point (from a backup or backup copy) and a target location where the recovered VM will reside. Unitrends creates a disk image recovery object directly on the appliance and spins up a new VM on the target host. By directly injecting data into the recovery object, your VM will be available in minutes. After creating the recovered VM, instant recovery migrates data from the on-appliance recovery object to the new VM. The recovered VM remains fully operational during the migration.

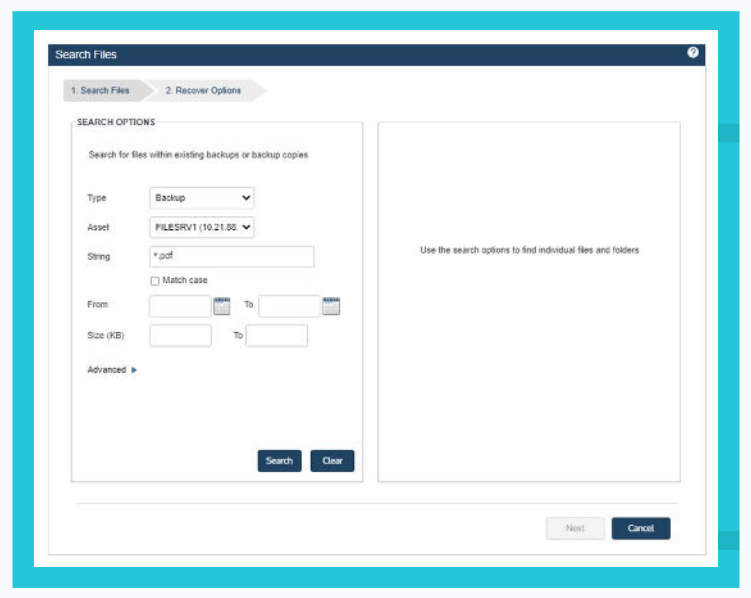
Supported Backup Types

Host Level (VMware*, Hyper-V*), Image Level (Windows*)

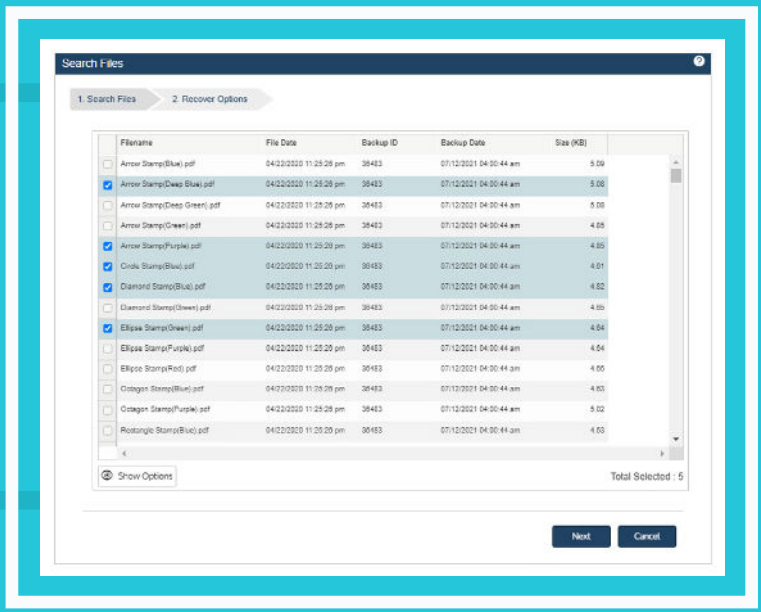
*See the **Compatibility Matrix** for details.

Granular Item (File/Folder) Recovery

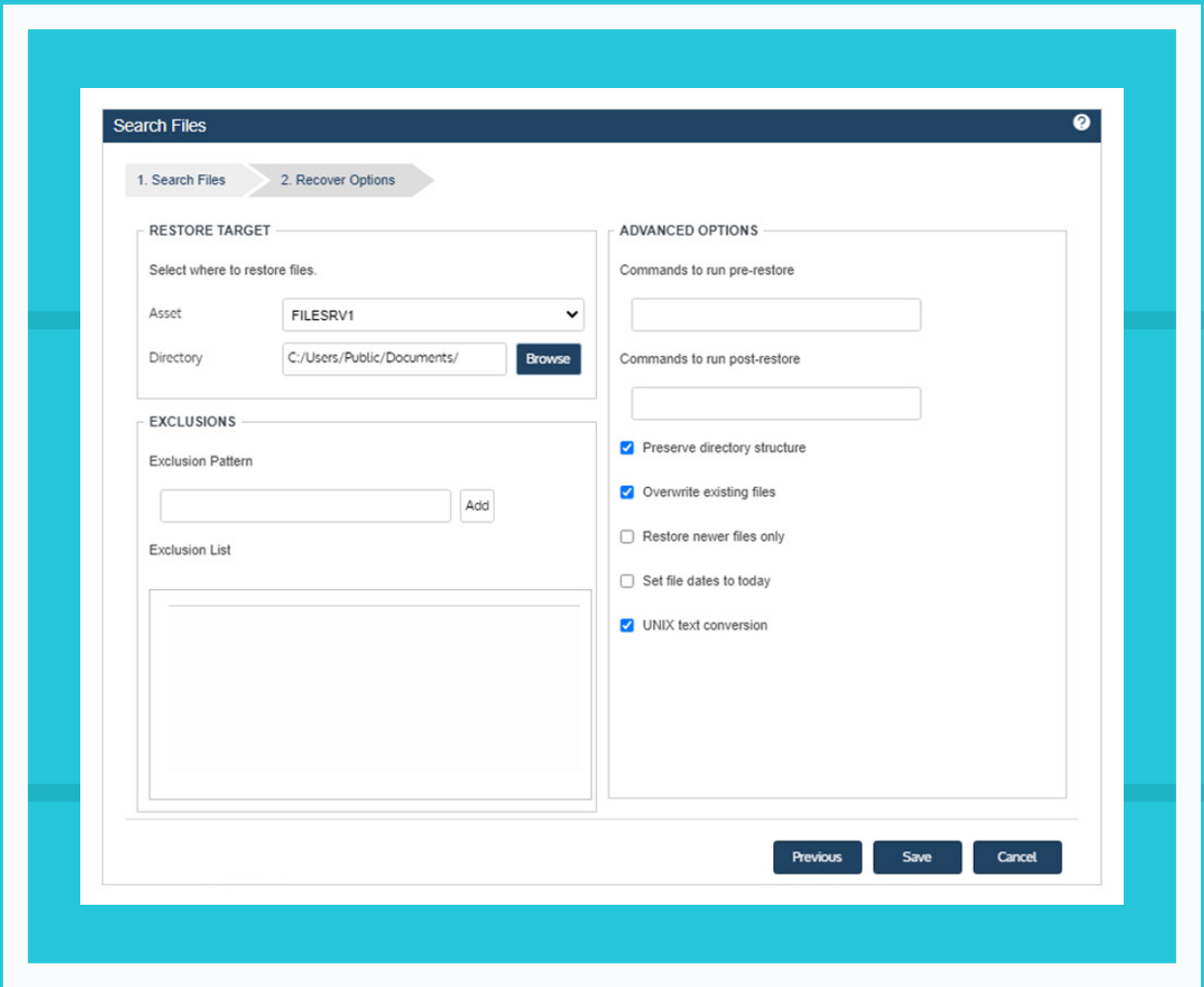
Should the infection be caught early on and contained to specific systems, removing the malware (as discussed above) and recovering any infected files may prove sufficient. You can recover and restore individual files and/or folders from File, Image and Host Level backups by searching the file tree of any protected asset or by searching for specific parameters with indexed file search. See the screenshots below for an example of Unitrends Search File function to easily locate and restore files.



Customize your search based on Type, Asset, File String (wild cards supported), Date Range and File Size. Select one or more files from the same backup to recover.



Once files have been selected for recovery, determine the target recovery location and place files specifically within the Directory, and adjust Advanced Options as needed.

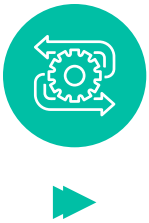


Recover to the original target or another asset, set Directory path and Advanced Options as required.

Supported Backup Types

File Level*, Image Level*, Host Level*, Application Level*

*See the Compatibility Matrix for full details.



Bare Metal Recovery

Unitrends Bare Metal technology is used for disaster recovery of protected assets. Bare Metal Recovery (BMR) enables you to perform disaster recovery directly from a file-level or image-level backup. For Windows assets, Unitrends provides Unified Bare Metal protection, which reduces recovery time, provides additional recovery points, increases on-appliance retention (by eliminating the need for bare metal backups) and simplifies the DR process. Unified BMR is performed by using the Bare Metal Recovery Wizard and standard 32-bit and/or 64-bit ISO images, eliminating the need to create bare metal ISOs for each protected asset. In many cases, recovery to dissimilar hardware is supported. See the **Compatibility Matrix** for all systems supported with Bare Metal Recovery.

Supported Backup Types

File Level (Windows, Linux, pSeries/AIX, Solaris SPARC, etc.)*, Image Level (Windows)*

*See the **Compatibility Matrix** for full details.

CONCLUSION

Defense against ransomware requires a multipronged, continuous effort in the form of end-user training and awareness, security controls and a well-tested BCDR strategy. As part of your BCDR solution, Unitrends provides protection against and recovery from these advanced threats via our five pillars of defense: Secure, Protect, Test, Detect and Recover.

IF YOU'RE INTERESTED IN LEARNING MORE ABOUT

WHAT UNITRENDS CAN DO FOR YOU AND YOUR ORGANIZATION,

GET IN TOUCH WITH US TODAY.

DISCLAIMER

1. This document is intended as an educational tool to supplement, not replace, existing ransomware response, remediation and disaster recovery plans.

2. This template is made available "as is," without warranty, and is free from liability for damages resulting from the use of the information provided in this template.

3. Customization of the template, strategies and techniques defined within, and testing of your remediation and recovery plans, is a requirement for success.

Sources:

1 https://www.corvusinsurance.com/blog/q3-ransomware-report?utm_campaign=FY23-Q4-Quarterly%20Ransomware%20Report&utm_source=ransomware%20blog&utm_medium=press

2 https://www.ibm.com/reports/data-breach

3 https://www.datto.com/resources/ebook-dattos-smb-market-report-for-msps

4 https://www.av-test.org/en/statistics/malware/

5 https://expert-advice.org/security/ransomware-attacks-are-on-the-rise-again/

6 https://www.cvedetails.com/vulnerability-list/vendor_id-26/Microsoft.html?page=1&cvssscoremin=7&year=2023&order=1&trc=1019&sha=fb3955e0fab8edcd1618e9496e10af97755431e2

7 https://www.statista.com/statistics/218089/global-market-share-of-windows-7/

8 https://www.kaspersky.com/about/press-releases/2023_rising-threats-cybercriminals-unleash-411000-malicious-files-daily-in-2023

9 https://gs.statcounter.com/os-market-share/desktop/worldwide

10 https://6sense.com/tech/server-and-desktop-os/linux-market-share

11,12 https://securityboulevard.com/2020/10/ransomwares-next-target-backup-data/

13 https://www.blackfog.com/what-you-need-to-know-about-data-exfiltration/

14 https://www.scmagazine.com/news/ransomware-victims-clobbered-by-repeat-attack

ABOUT UNITRENDS

Unitrends Unified Backup enables our customers with a platform to address the challenges of today with a complete and agile solution designed to back up, secure and recover all workloads. The platform encompasses protection for traditional data center infrastructure as well as cloud-based workloads, SaaS data and the data being generated on endpoint devices such as laptops and remote PCs. Purposeful integrations with security tools provide end-to-end protection against cybercrime and human error, inject automation and artificial intelligence to simplify complex systems, and provide a unified experience with visibility across a complete backup infrastructure.

Learn more by visiting www.unitrends.com

UNITRENDS
A Kaseya COMPANY