UNITRENDS
A Kaseya COMPANY

DETECTING AND MITIGATING RANSOMWARE WITH UNITRENDS UNIFIED BCDR

ADAM MARGET, Technical Marketing

MOHAMMAD AL-SHAFIE, Global Director, Sales Engineering

INTRODUCTION

Ransomware remains a pervasive threat. More than 300 million attacks have been documented over the last year, meaning an organization falls victim to ransomware approximately every 11 seconds.[1,2] Today, data lives in more places than ever before and is constantly under attack. Traditional security solutions such as antivirus are only a part of the solution. One could argue antivirus solutions alone are ineffective against ransomware, as a whopping 53% of organizations with multiple AV solutions in place still fell victim to an attack.[3]

With ransomware's high rates of success in overcoming traditional security mechanisms, backup and disaster recovery solutions are among the most important aspects of any cyber resilience plan today. Unitrends Unified BCDR platform protects all data no matter where it lives and injects automation and artificial intelligence to simplify time-consuming, manual tasks and eliminate risk. At Unitrends, we've identified five pillars of defense that, in combination, offer you the best protection against such ransomware attacks and enable 100% proof and confidence in your recoveries to come:

1 SECURE

2 PROTECT

3 TEST

4 DETECT

5 RECOVER

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

SECURE

Ransomware is soaring to new heights. In the last year, attacks increased by 62% globally and 158% in North America.[4] As threat actors look to cash in on easy paydays, new variants and more sophisticated techniques have been developed to more readily overcome an organization's defenses. More than 268,000 "never-before-seen" malware variants were identified in 2020 — a 74% increase year-over-year.[5]

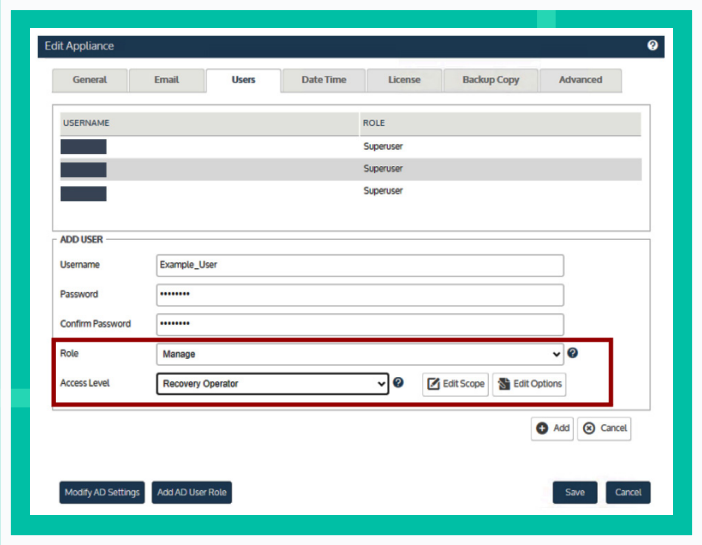
Ransomware security is a major concern for enterprises running Windows operating systems. According to the CVE database, Microsoft has more than 660 "dangerous" security gaps, with 357 vulnerabilities being attributed to Windows 10. Despite these vulnerabilities, Windows systems represent a huge share of the global OS market, with a 73% market share of desktop OS and 72% of server OS.[6,7] Windows is the prime target for threat actors and the sheer volume of Windows machines worldwide means cybercriminals will get the greatest returns by tapping into this market. AV Test's 2020 Security report revealed more than 78% of new malware in the last two years has been developed to target and penetrate Windows systems.[8]

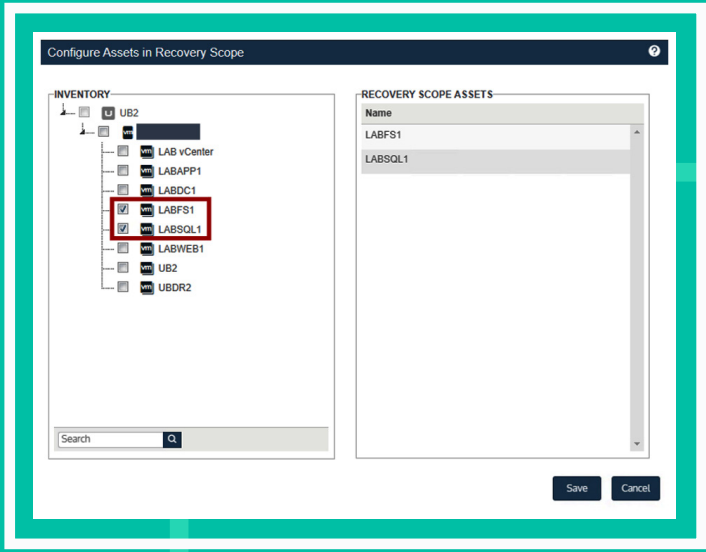
In response to widespread attacks on Windows machines, many organizations are transitioning away from malware-susceptible Windows-based backup software. By contrast, infections on Linux operating systems are far less common, with Linux capturing only 2% of the desktop OS market and 13% of servers.[9,10] In addition to a small market share, 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, Citrix Hypervisor 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 install, so be sure to select a secure password different from the default. You will want to secure backup server behind company firewalls. A backup server should never be on a public-facing IP address or unfiltered NAT. Many Unitrends customers deploy and operate their solution on an 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 and environmental security controls, Role Based Access Control (RBAC) enables individual self-service while also securing the system from unwanted access. Active Directory authentication may also be enabled. Each user's scope may be defined by operations they can perform within the backup environment as well as by systems and backups they have access to. If a particular user or group would benefit from self-service control 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 **Recovery Operator** for a specific set of machines. In this example, the user has permissions to run reporting, view jobs and perform recovery operations only (file, folder, VM) from backups and backup copies for the defined set of machines. 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.).





PROTECT

Unitrends offers compatibility for backup and recovery of more than 250 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 3-2-1-1 rule of backup at the very least. This means three (3) copies of your data, stored on two (2) different formats, with one (1) copy going off-site and one (1) copy that is immutable (unable to be modified). 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 to be 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).

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

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 on a hot target (such as a secondary appliance or Unitrends Cloud), where data is immediately available for recovery, and a 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.

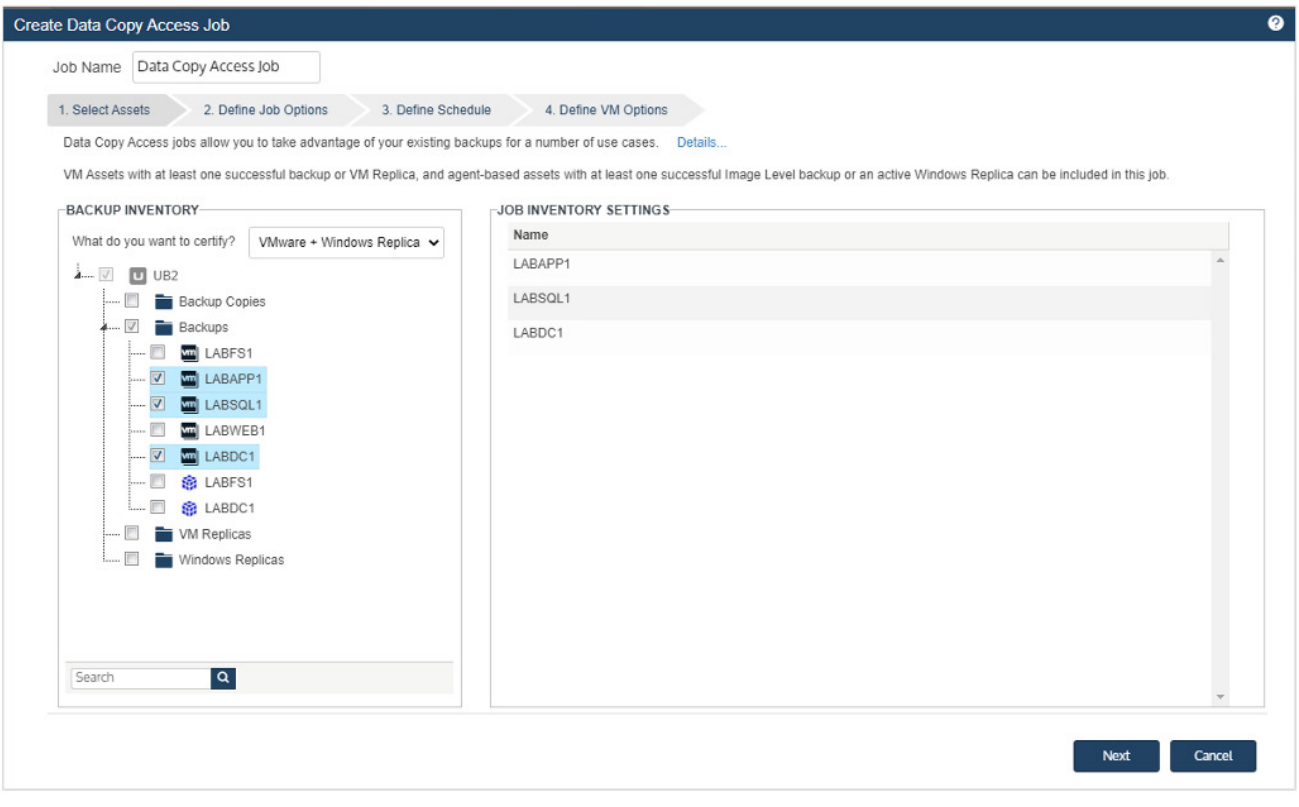
TEST

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.

Legacy methods of testing, such as screenshot verification, may leave much to be desired when it comes to ransomware recovery, as 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 applications are recoverable.

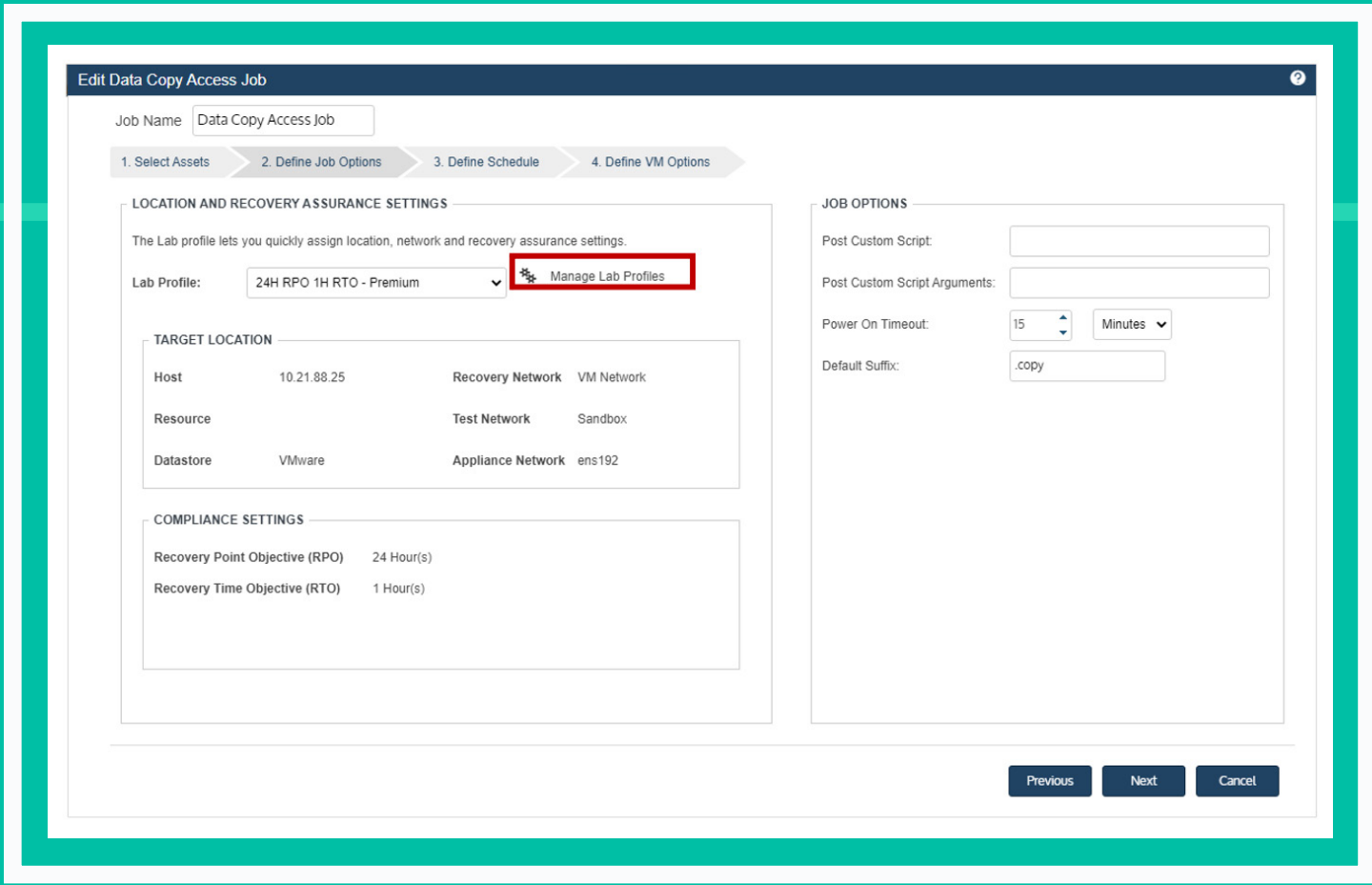
Unitrends helps organizations automate backup verification and recovery testing with Recovery Assurance. *Recovery Assurance* enables deep, application-level testing for both simple and complex environments and offers full control over configurations of boot order dependencies, networking and application 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 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.

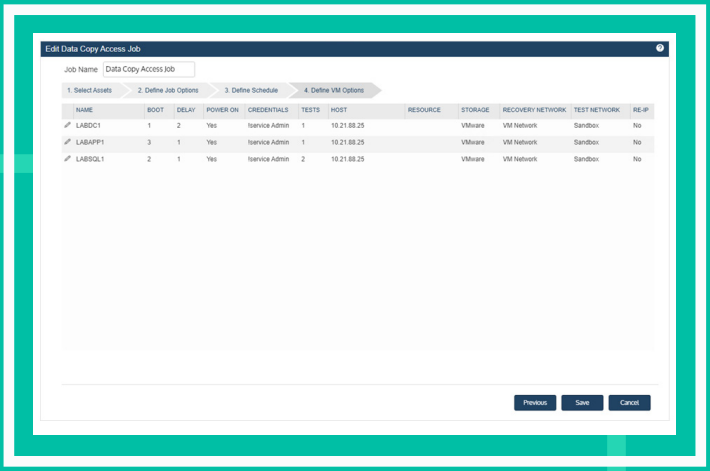
After determining the backups you want to include in your DCA job, the next step is determining the location in which you will run testing. DCA jobs can be created on your local source appliance, managed appliances or any distributed appliances. The DCA will create a VM for testing either on the appliance 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.

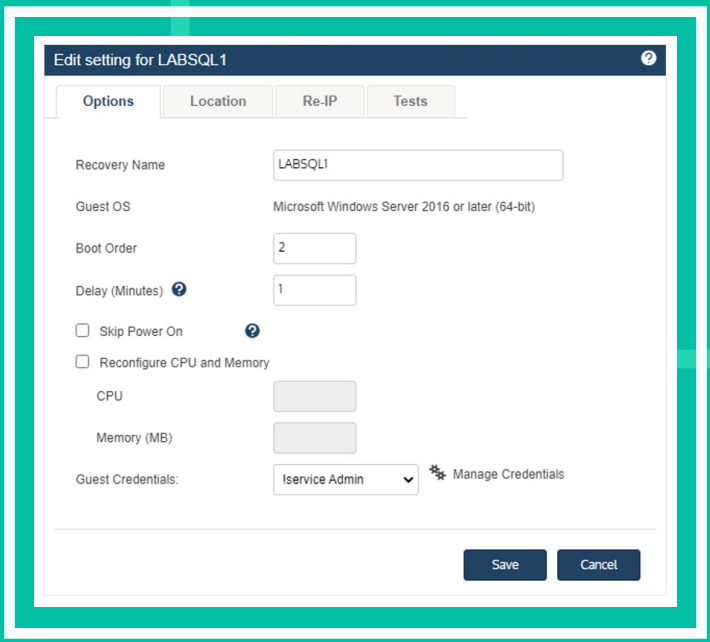
Once the job inventory and lab profile have been configured, you will need to set a custom schedule for testing and configuring VM Options. Configuration of VM Options is used to perform a number of different tests, from verifying service profiles, reconfiguring the recovery VM and executing application-level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

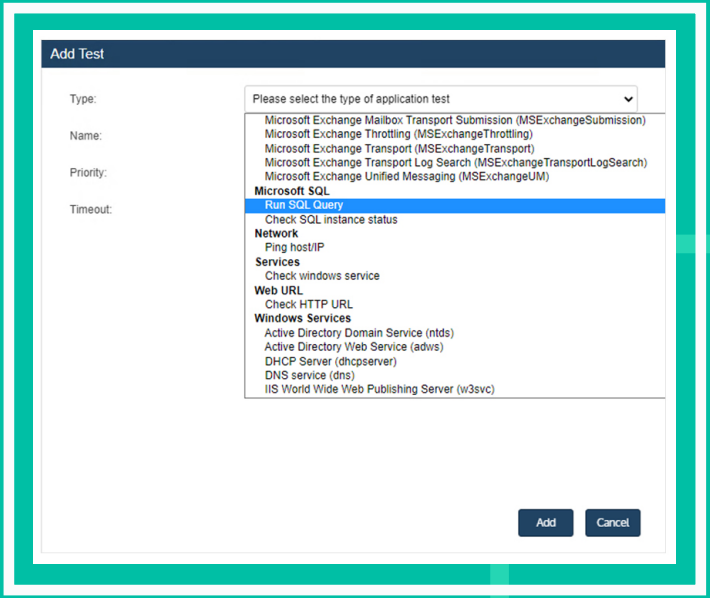
The screenshots below show the job inventory and a summary of the VM Options configuration and drill down into advanced configuration options for our SQL server LABSQL1.



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.

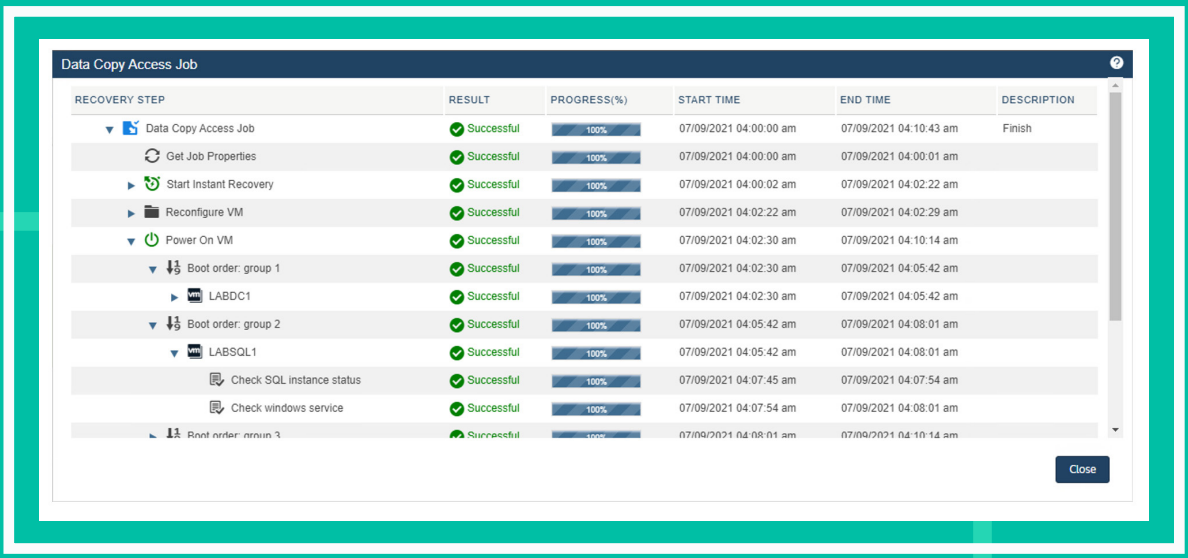




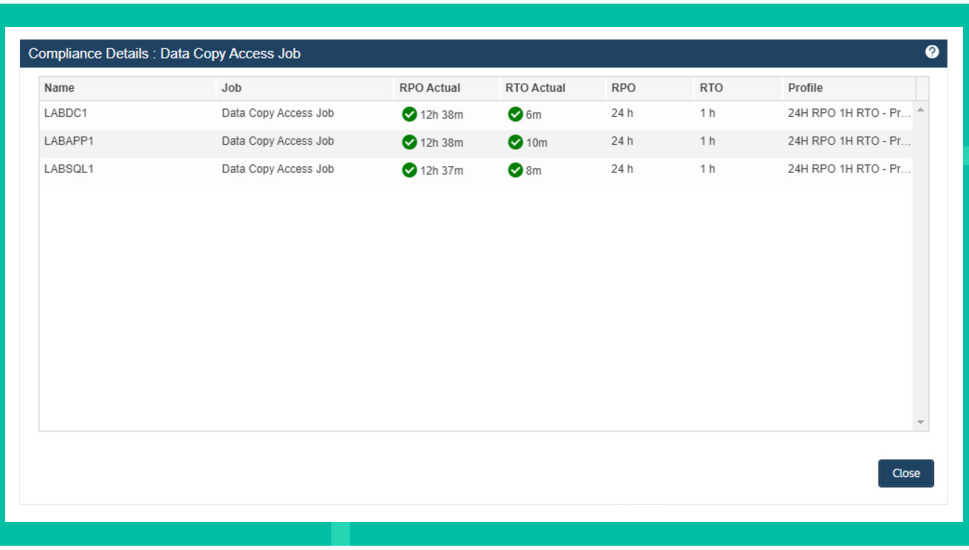
Choose from more than 50 canned application tests and/or write your own scripting to further customize your tests.

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.

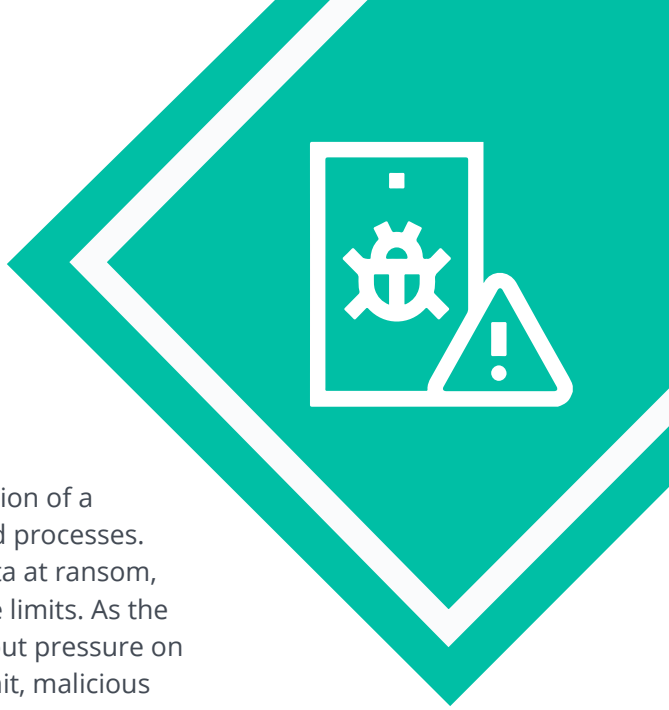
Recovery Assurance details the results of the application-level tests and indicates results as Successful/Warning/Failure. The Compliance Report presents results from RTO and RPO tracking as either Success (meets RTO and RPO) or Failure (fails to meet RTO, RPO or both). Insights from testing results 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.



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]

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.

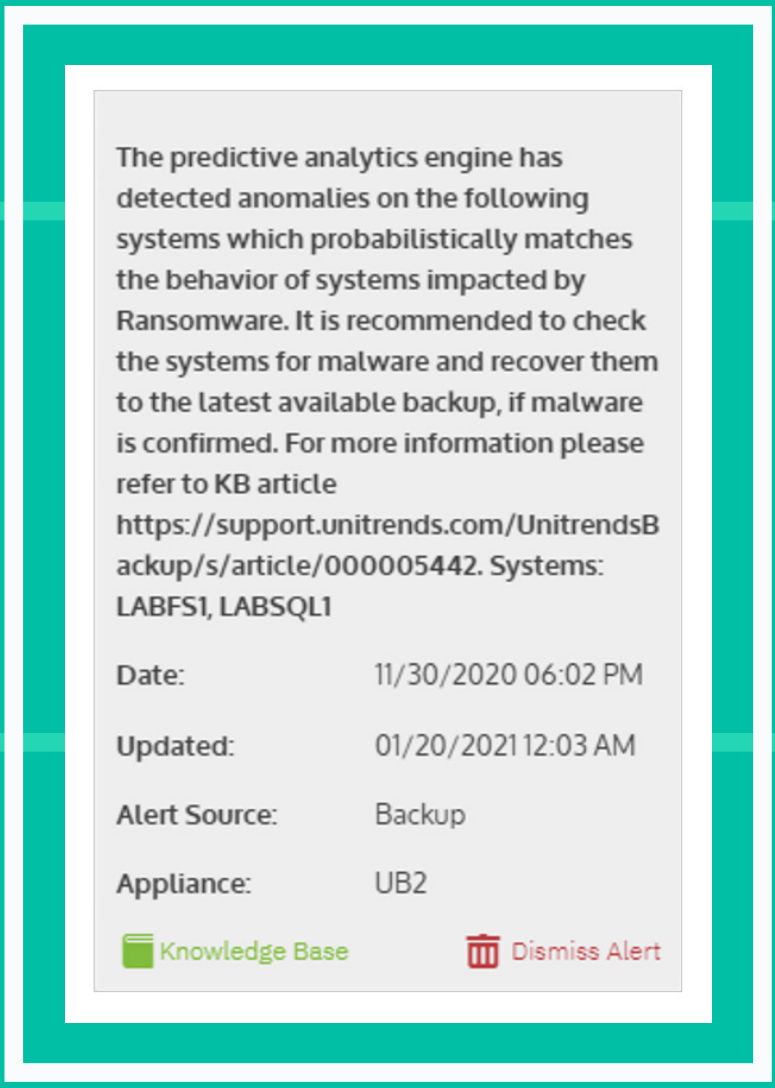
Deletion: Once the ransomware has spread as far as it can, the next phase involves deleting network-accessible backups. Backup files have known signatures that make them easy to target and encrypt. In addition to targeting file signatures, ransomware uses APIs published by backup vendors to delete backups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

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.[13]

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.[14] Traditional security tools are not sufficient as a standalone defense. In fact, 75% of organizations infected with ransomware were running up-to-date endpoint protection.[15]

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.



Ransomware Detection Unitrends Dashboard Alert

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, but 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:

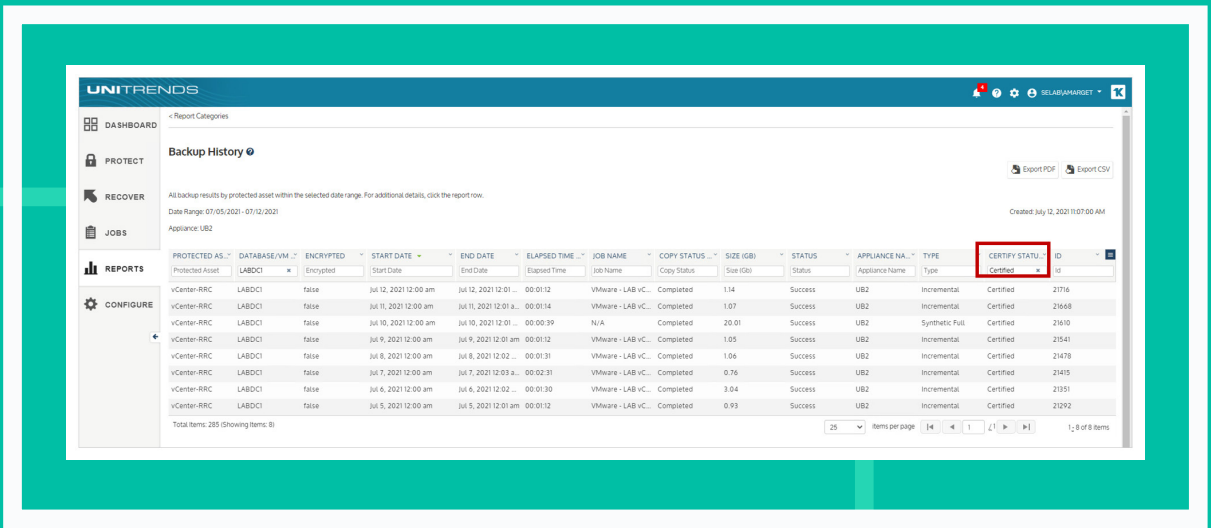
1. **Isolate Impacted Systems:** Unitrends use of predictive analytics for ransomware detection gives you a leg up when combating fast-moving attacks before they propagate fully. The success of a ransomware attack is predicated on how quickly it can spread across your network. Responding as quickly as possible can greatly impair the infection from spreading and reduce the impact to 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, as well as removing 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 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.



Adjust date range and other columns to filter backups points certified by Recovery Assurance testing.

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. Recent findings from cybersecurity vendor Cybereason report that 80% of organizations that paid a ransom experienced a second attack, and nearly half believe the second attack was carried out by the original perpetrator.[16] In many cases, decryption does not go as expected either. The encryption methods used by these malwares are not always clean. Despite a rise in victims paying the ransom (32% in 2021 compared to 26% in 2020), newer findings report that as many as 92% of organizations who paid didn't get all of their data back while nearly one-third (29%) failed to recover even 50% of their data.[17]

- **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, it's encrypted and held 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 in 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 RECOVERY

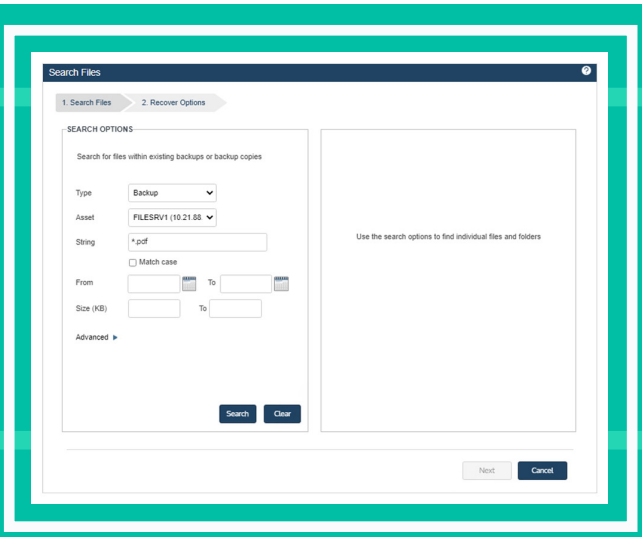
There are a number of backup approaches you can leverage with Unitrends to meet the needs of your environment. As outlined in the "Protect" section, Unitrends supports File, Image, Host and Application-level backups. Your recovery goals (RTO, RPO, granularity, flexibility) should be used in part to inform 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:

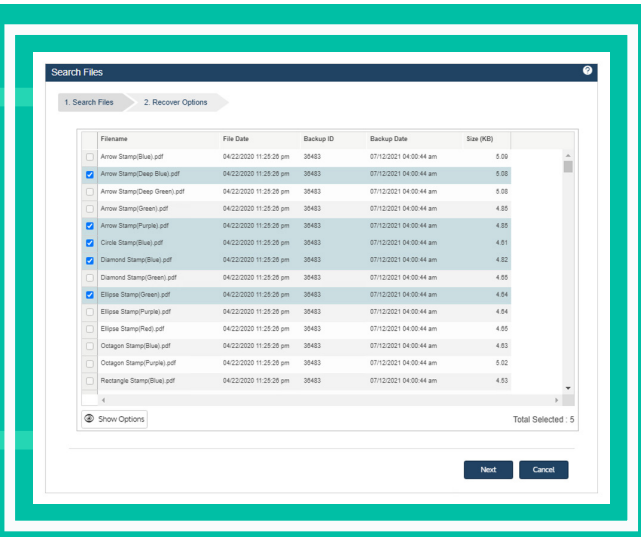
Instant Recovery: In the wake of an attack, it is imperative to respond as quickly as possible to stop the infection, investigate, remove the threat and recover. Once you are ready to restore impacted systems, Unitrends Instant Recovery enables you to quickly recover VMs running any operating system. 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.

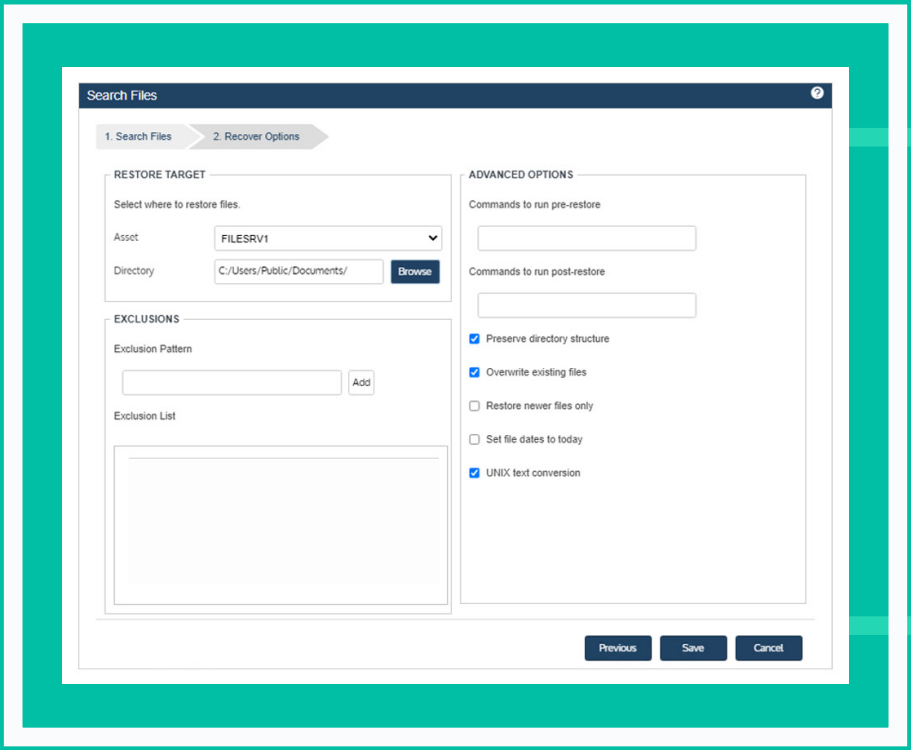
Granular Item (File/Folder) Recovery: Should the infection be caught early on and contained to specific systems, removing the malware (as discussed above) and recovering any infected files may prove sufficient. You can recover and restore individual files and/or folders from File, Image and Host Level 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 multi-pronged, 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

- This document is intended as an educational tool to supplement, not replace, existing ransomware response, remediation and disaster recovery plans.
- This template is made available "as is," without warranty, and is free from liability for damages resulting in the use of the information provided in this template.
- Customization of the template, strategies and techniques defined within, and testing of your remediation and recovery plans, is a requirement for success.

Sources

1) www.statista.com
2) www.blackfog.com
3) www.knowbe4.com
4,5) www.securitymagazine.com
6) gs.statcounter.com
7) www.statista.com
8) www.av-test.org
9,10) www.statista.com
11,12,13) securityboulevard.com
14) spinbackup.com
15) purplesec.us
16) searchsecurity.techtarget.com
17) www.forbes.com

ABOUT UNITRENDS

Unitrends Unified BCDR enables our customers with a platform to address the challenges of today with a complete and agile solution designed to backup, 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