UNITRENDS
A Kaseya COMPANY

CASE STUDY CONFIDENTIAL
UNVEILING LESSONS LEARNED FROM DATA DISASTERS

TOP SECRET

With more than half of businesses (59%) experiencing a ransomware attack in 2023, the data protection stakes have never been higher. Companies across various industries face unique challenges in keeping their data secure and recoverable.

While many success stories go untold, we're peaking behind the curtain to share four powerful, confidential case studies that illustrate the importance of unifying people, processes and technology to deliver resilience and ensure a successful outcome when the outlook looks bleakest.

In this eBook, we unveil untold stories of companies falling victim to sophisticated cyberattacks and how Unitrends backup and recovery technologies, alongside the often-unseen heroes in technical support, empowered the victims to overcome these attacks. We will reveal important lessons learned from these case studies, as well as practical insights and expert tips that you can implement immediately to protect your valuable data effectively.

Table of Contents

Case study 1: Overcoming cyberthreats involves understanding regulatory requirements (including insurance) and how to adhere to them

Situation

A large manufacturing company, managing approximately 200TB of data and more than 700 virtual machines (VMs), deployed Unitrends appliances and cloud (for off-site retention and Disaster Recovery-as-a-Service) since its small IT team did not have the capacity to continue maintaining its existing disaster recovery site. The company deployed Unitrends backup appliances alongside their existing backup solution, which was to remain in place until they were fully onboarded into the Unitrends cloud and enrolled in DRaaS. However, as the company was onboarding into the cloud and building out a documented disaster recovery (DR) plan – crucial to meet both business SLAs and cybersecurity insurance requirements – attackers took advantage of this brief window of vulnerability to strike.

Event summary

The company was hit with ransomware, resulting in the encryption of all production data (more than 780 VMs) and the data on the solution provided by their other backup vendor. However, the Unitrends backups, residing on a hardened Linux appliance outside of the attack surface, remained unaffected by the attack. After quarantine, triage and mitigation, the customer prepared for recovery. However, before recovery could begin, a legal stakeholder revealed that the company's cyber insurance provider required independent, third-party scans to determine the intrusion point and assess the health of the recovery. If the data was restored prior to being validated with an insurance-approved tool, their policy would not pay. The company was able to recover its data only after completing these scans as part of the insurance audit.

Recovery operation

Unitrends Support sprang into action to support the customer's recovery efforts since the company did not yet have a documented DR plan — this was still in progress along with its Disaster Recovery-as-a-Service onboarding. Since the local infrastructure was usable, although compromised, the company opted to recover locally instead of using the cloud.

With Unitrends Data Copy Access, the customer was able to automate the spin-up of isolated, **on-demand labs** to recover the VMs in batches for further analysis. The company used VMware's Carbon Black solution, a tool approved by its insurance provider, to run third-party scans to confirm the data was clean and met auditing requirements. Once a machine passed the scan, it was pushed live in the production environment using automated orchestration from Data Copy Access.

Three IT admins and the director of IT (who had never been hands-on with the product before) completed this process for all **789 VMs in just over 48 hours.**

> “It would have taken us months to recover all of our data with our previous solution.”
>
> — [redacted] [REDACTED]

TOP SECRET

Key takeaways

- A **hardened Linux appliance architecture** has a much better chance of surviving an attack compared to Windows-based backup software.
- Cyber liability insurance providers often have clauses that many people are unaware of, imposing more challenging requirements to receive payouts. The company leveraged automated testing from Unitrends to address these challenges.
- The immutable **Unitrends Cloud** was on standby, ready to assist in recovery if necessary. This capability is a critical part of a comprehensive backup strategy.

Download our checklist to discover the top five reasons cyber liability insurance claims are denied and how to proactively prepare to avoid any issues.

Case study 2: Backup technology alone is not enough — strategy is vital

Situation

A non-profit institution operated two sites, each equipped with a Unitrends backup appliance. The appliance in Site 1 backed up the data from Site 2, and vice versa, ensuring they had two copies of their data: one production copy and one backup, with the backup copies from one site stored at the other. However, the organization was not creating a third copy of their data (recommended to be a backup copy stored off-site and immutably), which is a crucial aspect of the 3-2-1 rule for data protection.

Event summary

On Monday, the end user's environment was breached by a threat actor, stemming from a credential compromise that occurred due to weak passwords.

As often occurs, the cybercriminals moved laterally to establish a foothold in the network. In doing so, they discovered the Unitrends backup appliances. Knowing backups can provide recovery from a ransomware attack, the criminals attempted to access the backup infrastructure through the appliances' local UI console. Within five attempts, the attackers successfully guessed the password for the Unitrends appliance. The password was simply the company name in lowercase letters, followed by the number "1."

Once the attackers gained access to a valid administrator account, they deleted all the backups and encrypted the production data. They then demanded a ransom of $750,000 from the non-profit organization.

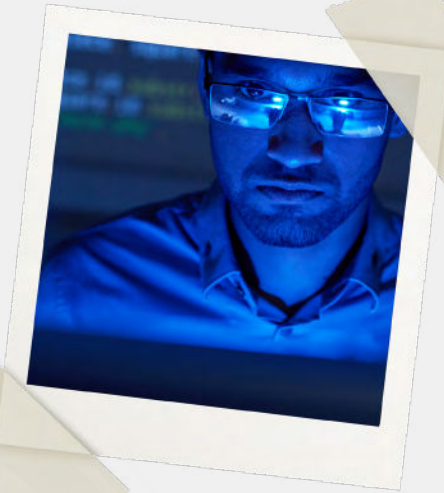
Recovery operation

The non-profit institution worked together with its cyber liability insurance provider to negotiate the ransom down to $450,000, which they ultimately paid. Unfortunately, the decryption key didn't work, leaving the organization's data unusable and resulting in a waste of money. Heading into the weekend with the situation looking bleak, the customer was racing against the clock to save their business.

Meanwhile, a skilled technician from Unitrends L3 support noticed a glimmer of hope in one of the organization's backup appliance databases. He diligently worked to reconstruct the organization's backups while the organization attempted (and failed) to unlock data with the decryption key.

By the following Tuesday, the Unitrends L3 technician had not only reconstructed the backup data but had also successfully recovered the organization's critical accounting systems.

> **“If we aren’t running by Wednesday, we are shutting the doors of our business for good.”**
>
> — [redacted] [REDACTED]



Key takeaways

- You are only as safe as your passwords are strong.
- Resilience lies at the intersection of people, processes and technology.
- **The 3-2-1 rule is a must:** Always have a copy of your backups. Overcoming ransomware attacks involves more than just technology — strategy and the people supporting our customers play a significant role.
- The immutable **Unitrends Cloud** is the most resilient option for combating malware attacks. The likelihood of simultaneously compromising an on-premises environment, the Unitrends appliance and the Unitrends Cloud, along with the customer’s data, is very low.
- Unitrends UniView provides enhanced security, including multifactor authentication (MFA) and the ability to block access to an appliance’s local UI to enforce MFA and/or single sign-on (SSO), and is available free of charge to all users.
- The integration of KaseyaOne with Unitrends UniView provides robust protection against a wide range of threats, including unauthorized access, via two-factor authentication (2FA) and single sign-on (SSO), including the use of third-party identity provider (IdP) SSO, such as Okta and Passly.

Case study 3: When Windows-based backup software failed...twice!

Situation

The end customer had an IT setup that was co-managed with a managed service provider (MSP). The organization's internal IT director trusted the previous backup vendor so much that he was reluctant to make any changes to their backup solution — until a second attack occurred.

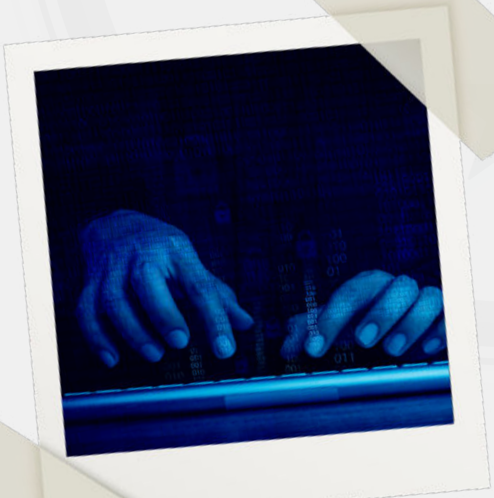
Event summary

The company had previously experienced a ransomware attack that deleted its backups, which used Windows-based backup software. **Over 90% of ransomware** consists of Windows-based executables.

In response, the company's management brought in an MSP to assess new solutions. Unitrends was included in the evaluation process, and a **Linux-based backup appliance** was provided for assessment. During the evaluation, another attack occurred, once again deleting the backups from the customer's existing software-based solution.

Recovery operation

Backups in the Unitrends appliance survived the attack, allowing the customer to recover quickly and easily. Without hesitation, the company decided to purchase Unitrends backup and recovery solutions for its entire environment.



> “At the end of the day, what matters most is the safety and security of our business.”
>
> — [redacted] [REDACTED]

Key takeaways

- Backups are often the first target of cyberattacks.
- Attack techniques, such as Active Directory attacks, virtual host takeover (VM escape) and leveraging high-scoring CVEs (more than 6,000 attributed to Microsoft), are common due to the proliferation of the **Windows OS.**
- Compared to **Windows-based backup** software, a hardened Linux appliance architecture is significantly more likely to withstand an attack.

TOP SECRET

Case study 4: The value of a partner with 35+ years of experience

Situation

A large Canadian organization operates across multiple data center locations, including hosting with a third-party data center partner. The end user deployed Unitrends at the locations they manage directly. Their data center provider was hit by malware, which impacted backups from the other two vendors. The organization and their hosting provider were unable to recover any data. It was then that Unitrends Support and Product Management teams were engaged. When Unitrends attempted to run a backup against non-encrypted production data, Volume Shadow Copy Service (VSS) calls resulted in the targeted asset immediately and permanently going offline, highlighting the urgency of the situation. The malware triggered when backups ran, holding data hostage.

Event summary

The customer's data center provider suffered a malware attack, which immediately crippled both backup vendors' solutions, rendering them completely useless for recovery.

The malware didn't immediately lock up the organization's production data. It appeared that running backups against a machine would trigger the attack on that machine, making it impossible to back up without the data being held hostage.

The primary path to saving the data was to find a way to copy it out of the production data center to a new location without triggering the malware.

Recovery operation

Unitrends' Director of Product Management and the skilled support team behind him leveraged the flexibility of Unitrends to change the way Unitrends backed up data.

The team discovered that the customer's hosted VSA instance was still connected to assets at the hosting provider that remained online. We provided a Unitrends virtual appliance free of charge, to aid in recovery efforts.

Focusing on SQL data, the Unitrends team modified file-level backup settings to not call VSS and leveraged the VSA to kill running services and free up in-use files. Once they were able to successfully back up a small SQL instance, they moved on more critical data.

The uninfected data was successfully backed up to the virtual appliance using the modified backup process, a creative workaround that only a company with years of experience could offer. The virtual appliance was then used to restore data to virtual infrastructure at the customer's site.

> “Ransomware attacks have become increasingly sophisticated, particularly with the aid of AI tools.”
>
> — [redacted] [REDACTED]

Key takeaways

- Malware continuously evolves its attack methods, making recovery scenarios unpredictable. To effectively counter these threats, it is essential to have a highly flexible set of backup and recovery options.
- Having a dedicated team of experts with the maturity and sophistication of Unitrends significantly enhances customers’ chances of successfully overcoming an attack.

TOP SECRET

Protect your data confidently with Unitrends

Over 90% of IT professionals across the globe believe that **security threats are becoming more frequent or severe.**

Cyberattacks are becoming increasingly complex and unpredictable, making it essential for organizations to be prepared for any recovery scenario. A flexible backup and recovery system ensures your mission-critical data can be restored quickly and efficiently, minimizing downtime and potential losses.

Expert vendor support is also crucial for maintaining operational continuity. Experienced professionals bring a level of maturity and proficiency that can make a significant difference during a crisis.

At Unitrends, we combine resilient backup and recovery solutions with a dedicated team of experts, giving businesses like yours a better chance of surviving and thriving despite the growing threats.

Don't wait until it's too late. Request a call today to discover how Unitrends can protect your business from evolving cyberthreats.

Speak With an Expert

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

UNITRENDS
A Kaseya COMPANY