
WHAT'S LURKING
IN YOUR
SERVER CLOSET?
UNITRENDS
A Kaseya COMPANY

It's that familiar sense of unease, every time you clock in and check your backup logs, hoping today, the monsters won't come out to play.

Welcome to the life of IT professionals. On the surface calm, cool and collected — masters of their domain. Yet, deep down, they know something's always lurking in their server closets, causing network blips, service interruptions and data loss.

IT pros are constantly looking over their shoulders and thinking *"what if I'm next?"*

Unfortunately, it's not a matter of if but when.

This eBook aims to shed light on the monsters that lurk in your sever closet, wreaking havoc in your production environment, delaying strategic initiatives and causing major business losses.

This eBook also provides solutions on how to bring an end to their reign of terror, allowing IT pros to concentrate on business growth as well as their career without worry.

1. THE BCDR FRANKENSTEIN

When the BCDR stack is comprised of several unique vendors that do not integrate as "seamlessly" as the brochure claimed, IT pros end up with a monster of their own creation — the BCDR Frankenstein.

Today, data is creeping up everywhere and the only way to manage it is with a hybrid infrastructure. Workloads span across on-premises locations and the cloud, including IaaS, PaaS and SaaS. Since 2019, the percentage of workloads running on cloud services has grown by more than 33%.[1] However, there is a lack of native provider tools offered by these cloud platforms.

Businesses of all sizes use approximately 25 to 100 different SaaS applications.[2] When you account for traditional on-prem infrastructure and other cloud-based workloads such as IaaS/PaaS, one ends up with a highly fragmented IT environment. The lack of true workload integrations between BCDR vendors forces IT admins to jump between different interfaces to solve challenges and troubleshoot errors. This drastically brings down the efficacy of managing BCDR processes. Unaware of the cumulative impact, businesses continue with a broken BCDR model, ultimately impacting the overall productivity, innovation and performance of their IT departments.

Essentially, stitching together multiple point products in hopes of achieving complete continuity may not yield the desired results. By introducing complexity, you risk hampering recovery point objectives (RPO) and recovery time objectives (RTO) and expose your organization to unnecessary risk in the event of an outage or disruption.

2. THE VSS GOBLIN

A touch of mischief, a dash of annoyance and a hint of nastiness are all trademarks of this creature lurking in the Volume Shadow Copy Service (VSS) environment.

VSS is a native Microsoft utility that enables backup applications to safely back up locked and open files. It captures and creates snapshots of the system called shadow copies. This may include copies of MS Exchange, SharePoint or even Hyper-V data.

The VSS Goblin takes unfair advantage of the complexity of backup and recovery processes that arise when protecting multi-tiered and highly sophisticated applications. By impacting these dependencies, key aspects of the environment (VSS writers) that backup vendors rely on are damaged, affecting both production environments and backup files.

A guaranteed backup is impossible with VSS writers out of commission. You often have to manually troubleshoot to resolve such errors, costing IT precious hours of their time. This leaves IT departments on the edge, and with little to no confidence since they're dealing with unpredictable backups. That's sure to test any IT pro's sanity.

3. SPYNONYMOUS

Spynonymous, also known as the malicious insider, has only one mission — to search and destroy. It orchestrates social engineering attacks, like phishing and Account Takeover attacks (ATO), to gain hold of stolen credentials and subsequently — data.

Malicious insiders are dangerous, big-ticket threats since they possess blueprints of security infrastructure and exploit this knowledge to steal or leak data on their own or pass it on to hackers. Mitigating the consequences of malicious activity costs organizations $760,000 on average.[3]

In fact, Spynonymous banks on employee mistakes to gain headway into organizations and steal corporate data. With 53% of workforces admitting they use the same password for multiple accounts, carrying out successful corporate espionage becomes a walk in the park.[4]

HERE ARE SEVERAL WAYS DATA ESPIONAGE CAN TAKE PLACE WITHIN A NETWORK:

- ***Privileged users -*** These users hold all the usernames and passwords to a company's sensitive data. They use their high-level access to bypass cybersecurity protocols, making it an easy steal.

- ***Bottom-line employees -*** They can intentionally insert malware into the network by clicking on phishing links, ensuring the breach is widespread and effective.

- ***Third-party vendors -*** Hackers can breach a third-party vendor with a poor security infrastructure to gain access to the network.

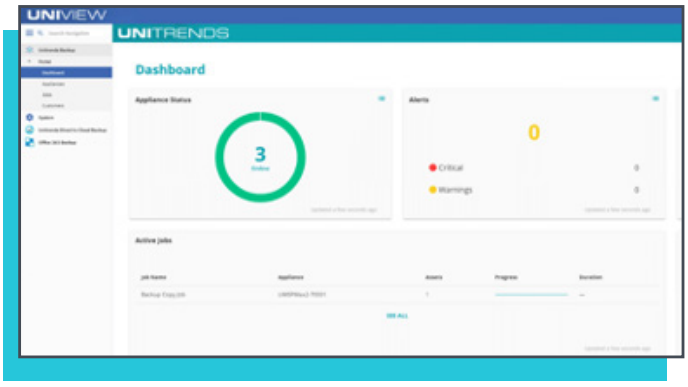
SolarWinds Orion was used as a springboard by hackers to gain access to several United States Government agencies including the Department of Homeland Security. Hackers compromised the Microsoft 365 email infrastructure, giving them access to the SolarWinds ecosystem. From there, automated updates to SolarWinds Orion were compromised and when the customer updated their software packages, hackers gained a foothold. The CISA characterized the attack as one of the most high-profile corporate espionage cases in recent years.[5]

PURGE ALL CLOSET MONSTERS WITH UNITRENDS

Unitrends is your one-stop solution for conquering the cyber monsters that lurk in your server closet and take away your peace of mind. Protect data across physical data centers as well as virtual environments, cloud-native workloads, and SaaS applications with ransomware detection, self-healing backups, dark web monitoring and much more.

A SINGLE VIEW TO INCREASE EFFICIENCY

Stop sifting through multiple BCDR solutions and manage all backups from a single, elegant portal with UniView. Unitrends UniView unifies best-of-breed approaches with centralized management and intelligent alerting so you can focus on what matters and manage all the approaches you need to protect your data, whether you leverage hybrid cloud backup appliances, direct-to-cloud backup or Microsoft 365 backup — they're all accessible through a single pane of glass.

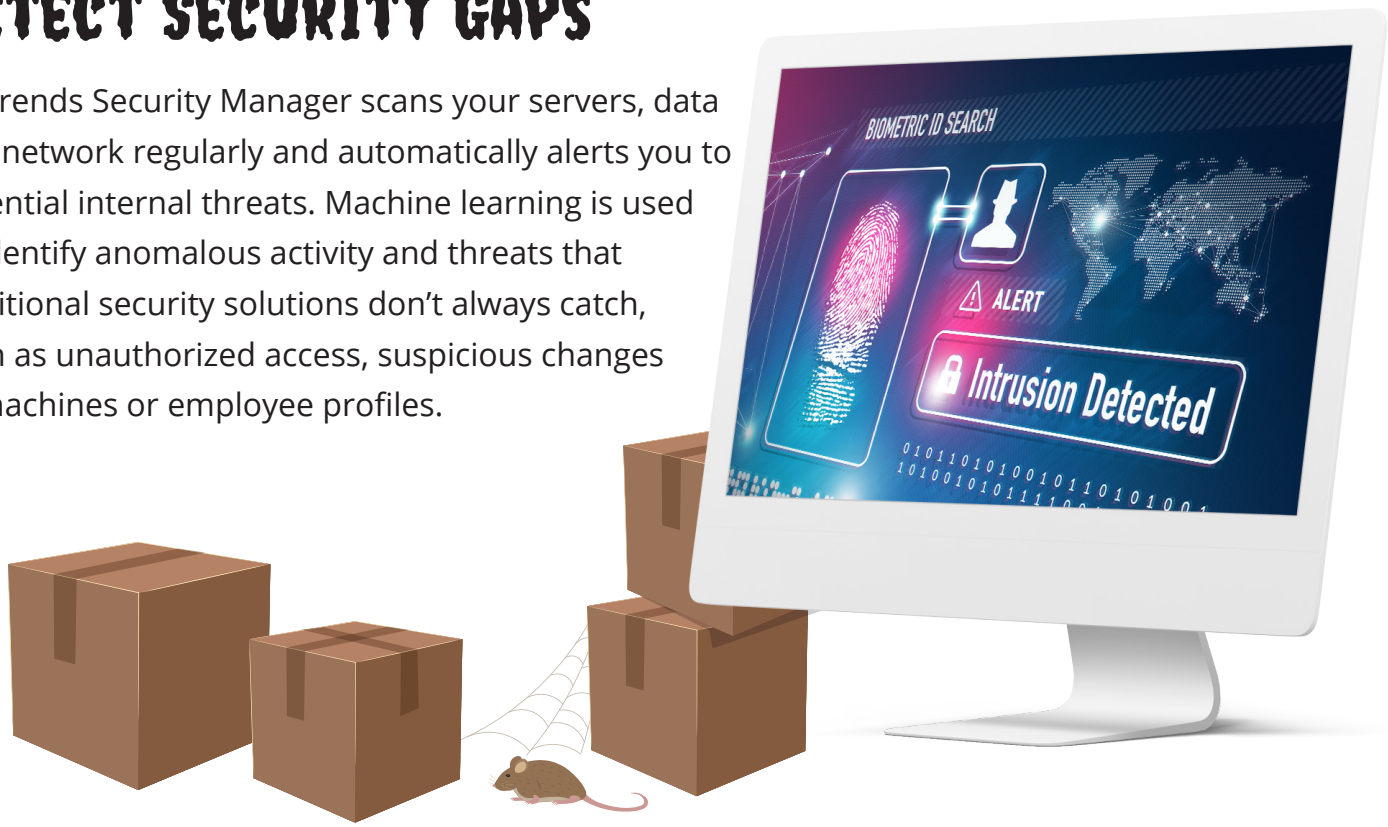


FIX VSS ERRORS AUTOMATICALLY

Unitrends Helix ensures clean, consistent backups by automatically fixing environmental issues, including VSS errors, before they can impact backups. In fact, Helix demands zero effort. Simply deploy it to start monitoring your environment, identifying issues and remediating them autonomously.

DETECT SECURITY GAPS

Unitrends Security Manager scans your servers, data and network regularly and automatically alerts you to potential internal threats. Machine learning is used to identify anomalous activity and threats that traditional security solutions don't always catch, such as unauthorized access, suspicious changes to machines or employee profiles.



Sources
1. https://hostingtribunal.com/blog/cloud-computing-statistics/
2. https://www.bmc.com/blogs/saas-growth-trends/
3. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures
4. https://www.securitymagazine.com/articles/92331-of-people-admit-they-reuse-the-same-password-for-multiple-accounts
5. https://news.clearancejobs.com/2020/12/18/cisa-solarwinds-compromise-puts-government-and-national-infrastructure-at-grave-risk/

WP-2111-ENG-A