Securely restoring backups after a cyberattack

Recovering from a cyberattack is a high-stakes process for any IT organisation. After an incident such as ransomware or malware infections, restoring systems from backup is often the quickest way to regain operational stability. However, blindly restoring backups without verification can lead to reintroducing malicious files into the environment, putting the organisation at risk of reinfection and further compromise.

Challenge

Ensuring a secure backup restoration process

While having a regular backup strategy is essential for cyber resilience, backups themselves can become compromised in the event of an attack. Several challenges must be considered:

- Risk of infected backups
  Many cyberattacks, especially ransomware, can remain dormant within backup archives. If an organisation restores without proper scanning, the attack could resurface immediately.

- Trusting the integrity of backups
  Without a proper scanning mechanism, IT teams cannot be certain whether the backup data is safe to use. Manually verifying large-scale backups is inefficient and unreliable.

Solution

File Security Screener - a robust solution for secure restoration

A dedicated file sanitation solution plays a vital role in ensuring that only clean, malware-free files are restored to an organisation's IT infrastructure. By integrating the File Security Screener (FSS) - a high-performance, security-driven file scanning solution, IT teams can confidently recover their data while minimising risks.
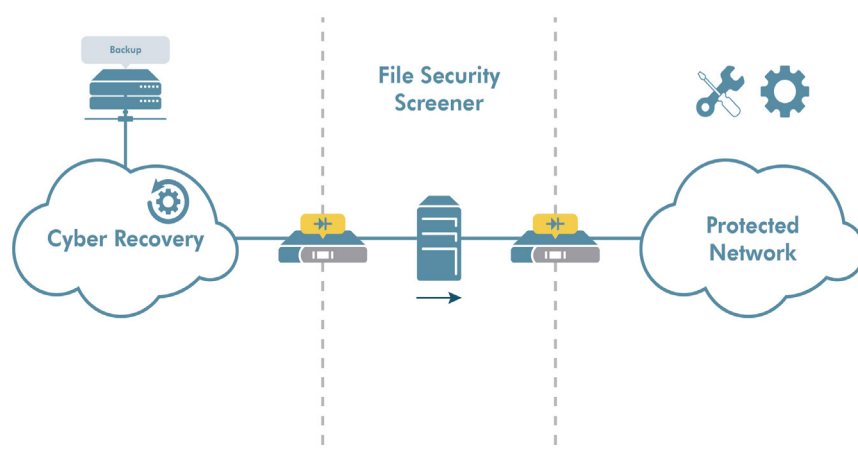
How the Process Works:

Extract Backup Files

The backup is mounted in an isolated environment to prevent direct exposure to production systems. The solution includes Advenica's data diodes for secure file transfer from source to destination, guaranteeing data can only flow from backup to production systems.

Deep File Scanning & Analysis using the FSS

Each file is scanned using advanced threat detection engines, including signature-based antivirus and sandboxing. If threats are detected, the scanning solution removes or neutralises malicious content, ensuring files remain usable.

Verified Restoration

Once the scanning process confirms that the files are clean, they can be safely restored to production systems.

This approach prevents reinfection, speeds up recovery, and ensures a higher level of confidence in the backup's integrity.

Advantages

Secure backup recovery with FSS

Implementing automated file scanning as part of a secure backup restoration strategy offers multiple advantages:

- Prevents reinfection – Stops hidden malware from being reintroduced into the network.
- Ensures compliance – Helps meet regulatory requirements for data security and incident response.
- Reduces manual effort – Eliminates the need for time-consuming manual verification of backup files.
- Accelerates recovery – Enables faster restoration with automated malware detection and removal.
- Enhances cyber resilience – Strengthens overall IT security by ensuring a clean, uncompromised recovery process.

Advenica provides cybersecurity solutions within encryption and network segmentation with the highest level of EU-and national approvals. We were founded in 1993 and are based in Malmö, Sweden, where most of our products are designed, developed, and manufactured. Advenica specialises in the sectors of defence, authorities, infrastructure, and industry. With decades of experience working with Sweden's national security, Advenica is known for delivering cybersecurity with exceptional service.

Read more on advenica.com

ISO 9001
CERTIFIED
ISO 14001
CERTIFIED