Case study:

When ransomware attacks

How Xcelocloud's MVSS365 support team handled a ransomware attack on healthcare infrastructure

When it comes to IT security in healthcare, hospitals are at the forefront. Attackers view hospital IT systems as an attractive target, as patient care is so critical and patient outcomes, and even lives, can be at stake. In these situations, a rapid response and visibility across all affected IT systems are needed, with staff in place who can diagnose problems across multiple vendors rather than focus on only a single vendor's devices.

The Challenge – Ransomware attacks critical healthcare

A healthcare provider customer was attacked with a ransomware exploit that froze their Epic EHR patient records, with the further threat that files would be erased unless a ransom payment was made. The hospital's SQL cluster housing critical Epic databases was encrypted by attackers. Backup systems were also compromised, even with SAN snapshots enabled, and despite Microsoft support's best efforts, the problem persisted, threatening permanent data loss.

Solution – Xcelocloud's multi-vendor support-in-depth

Unlike traditional vendor support that focuses on that vendor's specific problems, MVSS365 support services offer comprehensive multi-vendor expertise. Xcelocloud's Level 4 engineers identified an obscure fix, leveraging deep knowledge across VMware, SANs, and hard disk technologies. This holistic approach restored the SQL cluster and the Epic databases, preventing data loss, averting disaster, and restoring service rapidly.

Results – Data saved and trust earned

MVSS365 goes beyond first-line helpdesk and break-fix services to employ escalated support teams to address complex problems. This requires deep knowledge not only of multiple vendors' products but also an understanding of how they interact.

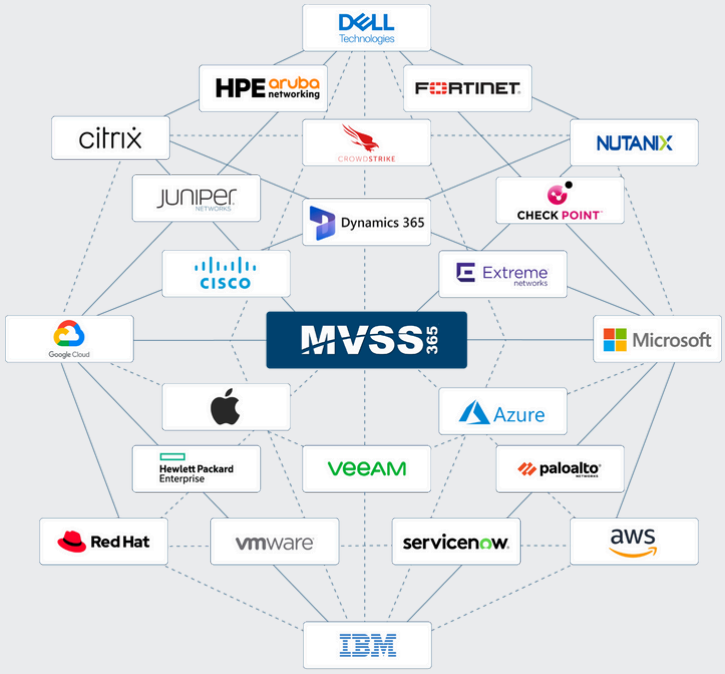
Why MVSS365 Managed Services?

MVSS365 managed services combine proactive monitoring, multi-vendor incident response, and deep cybersecurity expertise to help organizations avoid exactly these kinds of risks. By blending automation with vendor-agnostic engineering, MVSS365 empowers end-users to:

- Respond faster to outages
- Eliminate vendor finger-pointing
- Maintain business continuity during critical incidents

Xcelocloud's security practice extends across endpoint protection, cloud security, threat response, and compliance advisory—positioning us as a trusted partner in both prevention and rapid recovery.

Simplify multi-vendor IT support with MVSS365.



Takeaway

This case underscores the importance of having multi-vendor expertise during critical incidents. The MVSS365 team's ability to diagnose and resolve complex issues across VMware, storage systems, SQL, and Epic applications was key to recovering encrypted healthcare data, something traditional, vendor-specific support could not achieve. It also highlights the value of proactive managed services that go beyond basic monitoring to strengthen resilience, ensure business continuity, and prevent vendor finger-pointing. Even with backups in place, expert engineering made the difference. In moments that matter most, Xcelocloud earned trust by delivering rapid recovery and lasting confidence.