

# Case study: When the 'big one' happens



## How Xcelocloud's MVSS365 Multi-Vendor Services Team Navigated the 2024 CrowdStrike Outage

### Situation

In the summer of 2024, IT teams worldwide were blindsided by a major outage linked to a faulty CrowdStrike update. A corrupted file brought down tens of thousands of Windows-based systems, causing blue screens, service interruptions, and widespread business disruption.

The root cause? A complex interaction between CrowdStrike files and Microsoft Windows platforms. The impact was massive: IT organizations were left scrambling to determine fault domains, triage between vendors, and restore thousands of machines, fast.

### Challenge

The MVSS365 team was immediately called upon to support hundreds of impacted organizations across industries. In one notable example, a large educational institution faced the urgent task of restoring over 24,000 desktops across 300+ locations, without active users on-site, but with the fall semester quickly approaching.

In the commercial sector, the impact was more acute. Business-critical systems were down, and recovery guides circulating online required manual fixes using complex 32-character passwords. With no automation in place, IT teams faced an unthinkable task: manually inspecting every machine, with no time to spare.

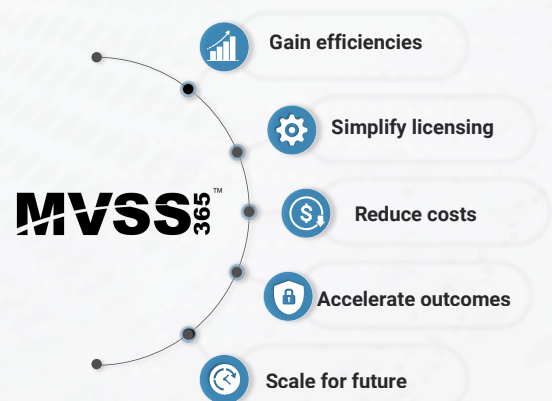
This wasn't a single-vendor problem; it was a multi-vendor crisis.

### Xcelocloud MVSS365 Advantage

As a leading provider of multi-vendor support services, Xcelocloud brings together global vendor expertise across Microsoft, VMware, CrowdStrike, and other leading platforms. Xcelocloud's MVSS365 multi-vendor support services, delivered by deeply skilled engineers, are designed to handle exactly this kind of scenario, where siloed support models break down, and cross-platform recovery is essential.

In this case, the MVSS365 team of multi-disciplinary engineers:

- Developed custom automation scripts to remediate issues across Microsoft Hyper-V, VMware, and Windows environments.
- Isolated and removed the faulty CrowdStrike files.
- Scanned, repaired, and rebooted affected virtual machines at scale and without manual touch.
- Avoided delays typically caused by vendor escalations, support queues, and finger-pointing.



## Results

The incident occurred late Friday. Thanks to Xcelocloud's rapid response, automation-driven approach, and deep technical coordination, thousands of customers' virtual and physical machines were restored by Monday morning, with:

- No need for Microsoft or CrowdStrike escalations.
- No user downtime in education environments.
- Minimal commercial disruption, even for organizations supporting global operations.

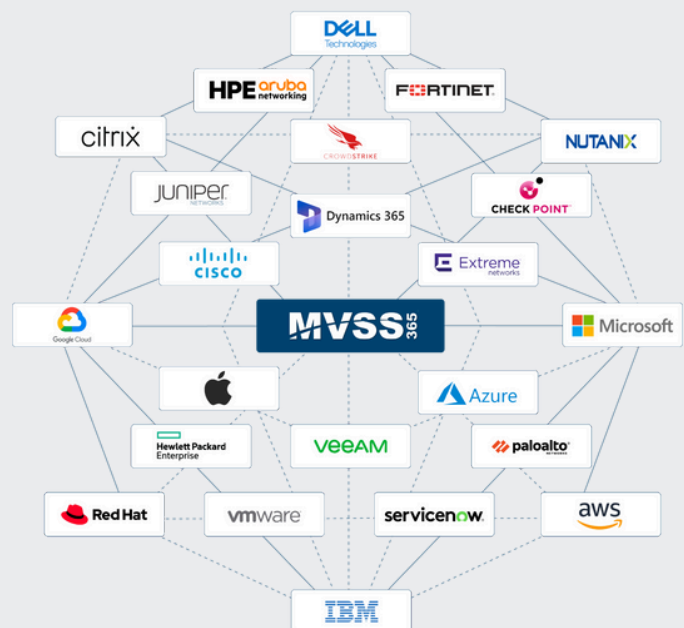
## Why Xcelocloud Managed Services?

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 MVSS365.



## Takeaway

The CrowdStrike incident revealed a hard truth: single-vendor support models don't scale in real-world crises. Complex environments demand a coordinated, multi-vendor response strategy that blends automation, engineering expertise, and trusted escalation paths.

MVSS365 can help organizations be better prepared for the next "big one". Contact the Xcelocloud account team about multi-vendor services and managed security offerings.