Intelligent IT

Beyond Endpoint Isolation

What Real Incident Remediation Looks Like

Isolating an infected endpoint feels like containment. It isn't. Real remediation requires understanding how the attack occurred, identifying all systems the attacker touched, and eliminating all pathways to re-infection. Many organizations declare incidents "closed" while attackers retain hidden access.

The Isolation Misconception

Disconnecting an infected endpoint stops immediate spread but leaves the core compromise unresolved. The attacker who reached this system typically stole credentials, moved laterally to other systems, or established persistence mechanisms. Isolation is containment; it isn't remediation.

Remediation Requires Five Steps

Investigation (What did the attacker access?) → Credential Invalidation (Reset every compromised credential) → Lateral Movement Analysis (Identify all systems touched) → System Restoration (Rebuild or restore from clean backups) → Validation (Confirm complete cleanup before return to service).

Each step is critical. Organizations that skip lateral movement analysis often discover weeks later that persistent backdoors remain active.

Identity is the Core Issue

Identity weaknesses appear in 90% of incident investigations. Compromised credentials are often the root cause—attackers gain initial access through stolen passwords, move laterally using legitimate access, and maintain persistence through credential reuse. If remediation doesn't address credential compromise, attackers regain access using the same stolen credentials.

Key Statistics

1.8B credentials stolen in H1 2025 | 90% of incidents show identity weaknesses | 94 days average to remediate compromised credentials

Complete Remediation

Organizations that best protect themselves aren't just faster at isolating systems—they're more rigorous about understanding what happened. True remediation requires investigating scope, identifying all attacker access, addressing root causes, validating cleanup, and documenting prevention measures. Unified Core provides security teams with visibility into exactly what attackers accessed and how they moved through networks, enabling remediation grounded in evidence rather than assumption.