

Early one morning, someone logged into the network with a real employee's remote-access credentials. Correct username, correct password. **The environment locked itself down before he could use them.**

## The Challenge

The login came from a workstation the security operations center had seen in other intrusions. Within moments, the account was authenticating to critical infrastructure: the domain controller, a SQL database server, and the virtualization host.

That's the ordinary shape of a modern breach. The attacker doesn't break down the door. He walks in with a key and starts trying every other door in the building.

Credential abuse was the top way in for attackers in Verizon's 2025 data, at **22%** of breaches.<sup>1</sup>

## The Solution

The client runs a layered managed security model: endpoint detection on every device, a 24/7 security operations center watching behavior instead of just known malware, and a containment-first posture.

When the malicious login was detected, every machine the compromised account had touched was isolated from the network automatically, within the same window, stopping lateral movement cold.

An MSI engineer traced the root cause in the VPN logs, disabled the exposed remote-access path at the firewall, reset credentials across affected accounts, forced fresh logins, fixed accounts set to never require a password change, then brought systems back online.

### Engagement Snapshot

|               |                                   |
|---------------|-----------------------------------|
| CLIENT        | Small Business, Sensitive Records |
| FOOTPRINT     | Single Site, On-Prem Servers      |
| RELATIONSHIP  | Managed Services, 24/7            |
| TIME TO CLEAN | About 4 Hours                     |

### By the Numbers

**~4 Hrs**

from first alert to a fully restored, verified-clean environment.

**29 Min**

average attacker breakout time in 2025. The fastest on record: 27 seconds.<sup>2</sup>

## The Results

The attacker got in and got nowhere: no ransomware, no data theft, and no downtime beyond a controlled morning of remediation. A breach that reached the domain controller ended as a bad morning instead of a headline.

**"If someone logs into your network tonight with a real employee's stolen password, what stops them in the first five minutes? If the answer is a person noticing in time, let's talk."**

<sup>1</sup> Verizon, 2025 Data Breach Investigations Report, April 2025. <sup>2</sup> CrowdStrike, 2026 Global Threat Report, February 2026.