VIGILANT

SUCCESS STORY

Vigilant 365™ Helps Stop Microsoft 365 Account Takeover

See why this tech company chose Vigilant to provide enhanced detection for their Microsoft applications to keep their sensitive information secure.

Targeted Threat Insights

Increased Visibility

Peace of Mind

BUSINESS CHALLENGE	VIGILANT TECHNOLOGY SOLUTION

With most employees working remotely, a mid-sized Tech Company had an urgent need to secure email – especially since so much of the information passing via email was highly sensitive in nature. The majority of end users were accessing Microsoft 365 directly from the Cloud, which increased the attack surface exponentially for the organization. This scenario creates a "perfect storm" opportunity for attackers to strike a single application from a multitude of vectors, leaving the entire company at risk.

The proprietary methodology behind Vigilant365™ alerts you to early signs of email compromise by delivering targeted threat insights that enable IT teams to correlate and streamline account activity data to identify and remediate suspicious activity faster. The Intelligent Alerting system feature also allows teams to gain greater visibility into their Microsoft 365 environments.

OUTCOME

There was an attempted login from another country when an executive from the company was logged in within the U.S. With improbable login rules, and support correlating the data, the Client was alerted to the potential account takeover and able to prevent unauthorized access to the executive's account. Client then followed the recommended actions to change account credentials.

Why Vigilant365™?

Vigilant365™ is different than a spam filter. It intelligently alerts on potential email compromise and account takeover by monitoring, aggregating and analyzing key information indicating potential threat activity across your entire Microsoft 365 environment. By adding another layer of detection beyond network and endpoint, Vigilant365™ monitors threat activity at the account level to help you guard against the data and revenue loss that malicious attacks can cause.