Law Firm Breach via Unsecured Endpoint: Fenix24 Delivered Full Remediation and Built Ongoing Endpoint Resilience

The Challenge:

A large U.S. law firm had invested in most of the endpoint protection tools included in the Grypho5 Comprehensive Endpoint Management (CEM) package, but they were not enrolled in the CEM program. Without centralized management and oversight, critical tools were left misconfigured and unmonitored, exposing the firm to immense risk.

Attackers exploited one of these gaps through a vulnerable endpoint belonging to a retired attorney who still had access to Google Drive. Within an hour, thousands of sensitive documents were exfiltrated, exposing the firm to major reputational and client risk.

The Solution:

Fenix24 responded to contain and remove the threat actor. From there, we enrolled the firm into our CEM program, where tools such as CrowdStrike, eSentire, and Cisco Umbrella as well as firewall policies were thoroughly revised, adjusted, and optimized to close gaps and enhance endpoint protection.

Fenix24 also took over full management, monitoring, and maintenance of both existing and new endpoint tooling. Our team ensured proper configuration, patching, and alignment with Grypho5's gold-standard practices, which are built on our unique understanding of threat actor behavior and breach context. This helps prevent future breaches and reduces the risk of widespread damage from TAs.

The Outcome:

Today, the firm's environment is significantly more secure. Endpoints have been hardened, unnecessary access (like that granted to retired users) has been eliminated, and all critical tools are now properly configured and continuously monitored. With 24/7 endpoint management in place, the firm now has real-time visibility into endpoint activity and rapid response capabilities to detect and contain suspicious behavior.