Egress and CrowdStrike Integration: Adaptive email threat detection and response

Identify and remediate human risk using augmented email, identity, and endpoint intelligence.

THE CHALLENGE

Phishing attacks lead to credential theft and lateral movement

The human element is the primary attack surface for cybercriminals, and people are most vulnerable when using email. What begins as a targeted inbound threat usually very quickly evolves into a costly outbound breach. Weaponized socially engineered phishing emails that prey on human fallibility underpins the cyber kill chain, leading to lateral movement across network and endpoint assets. While organizations have a variety of warning signals, they often aren't joined up, or worse lead to incorrect conclusions around where human risk truly lies. Without aggregated human risk scoring, correlated from email, endpoint, and other threat intelligence sources, organizations remain reactive to advanced human-led breaches.

THE SOLUTION

Dynamic threat detection and response

Egress' Intelligent Cloud Email Security and CrowdStrike Falcon® Identity Protection Risk Score are a powerful combination to help identify human risk and prepare organizations for threats before they materialize. By augmenting behavioral identity and endpoint data with email threat intelligence, cyber teams have clear visibility where risk lies and dynamic detection and response capability using an adaptive security architecture. Enabled by administrators in just a few clicks, analysts immediately gain access to real-time holistic human risk scores, shining a spotlight on areas of potential compromise not previously identified.

KEY BENEFITS

- Enables enhanced threat detection and automated response against advanced inbound and outbound email threats
- Provides holistic view of human risk resulting from activities and behavior from identity, endpoint, and email threat intelligence
- Delivers dynamic real-time policy management tailored to each individual's level of risk using an adaptive security architecture

Book a demo >

Unlock the full potential of CrowdStrike and Egress

Use case	Solution	Benefits
Holistic understanding of human risk using threat intelligence from multiple applications across the cyber ecosystem.	Aggregate multiple sources of data, including the CrowdStrike Falcon® Identity Protection Risk Score, via API, to accurately generate a unified view of human risk.	Correlate risk insights between identity, endpoint, and email threats to identify new areas of potential compromise.
Detection of advanced social engineering attacks, human error, and data exfiltration by email.	Combining contextual machine learning and neural networks to identify and neutralize targeted phishing attacks, misdirected emails, and data exfiltration.	Detect and defend against advanced inbound and outbound email threats that are typically missed by traditional security solutions.
Automatically apply security controls based on individual risk profiles.	Adapt email security controls dynamically based on aggregated threat intelligence.	Identify which individuals, departments, and geographies are most likely to cause compromise and modify security controls accordingly.

Crawford & Company, the largest publicly listed provider of claims management and outsourcing solutions globally, is excited to see our partners, Egress and CrowdStrike working together. This collaboration has provided previously siloed visibility into human risk that is now giving us actionable intelligence for the people in our company.

Combining telemetry from endpoints, identity, email threat intelligence and OSINT, we're not only able to talk about security being everyone's responsibility, but visualise it, shining a spotlight on areas and individuals we'd not previously considered as being a risk. More importantly, it allows us to become proactive in mitigating potential compromise with targeted education to those identified.

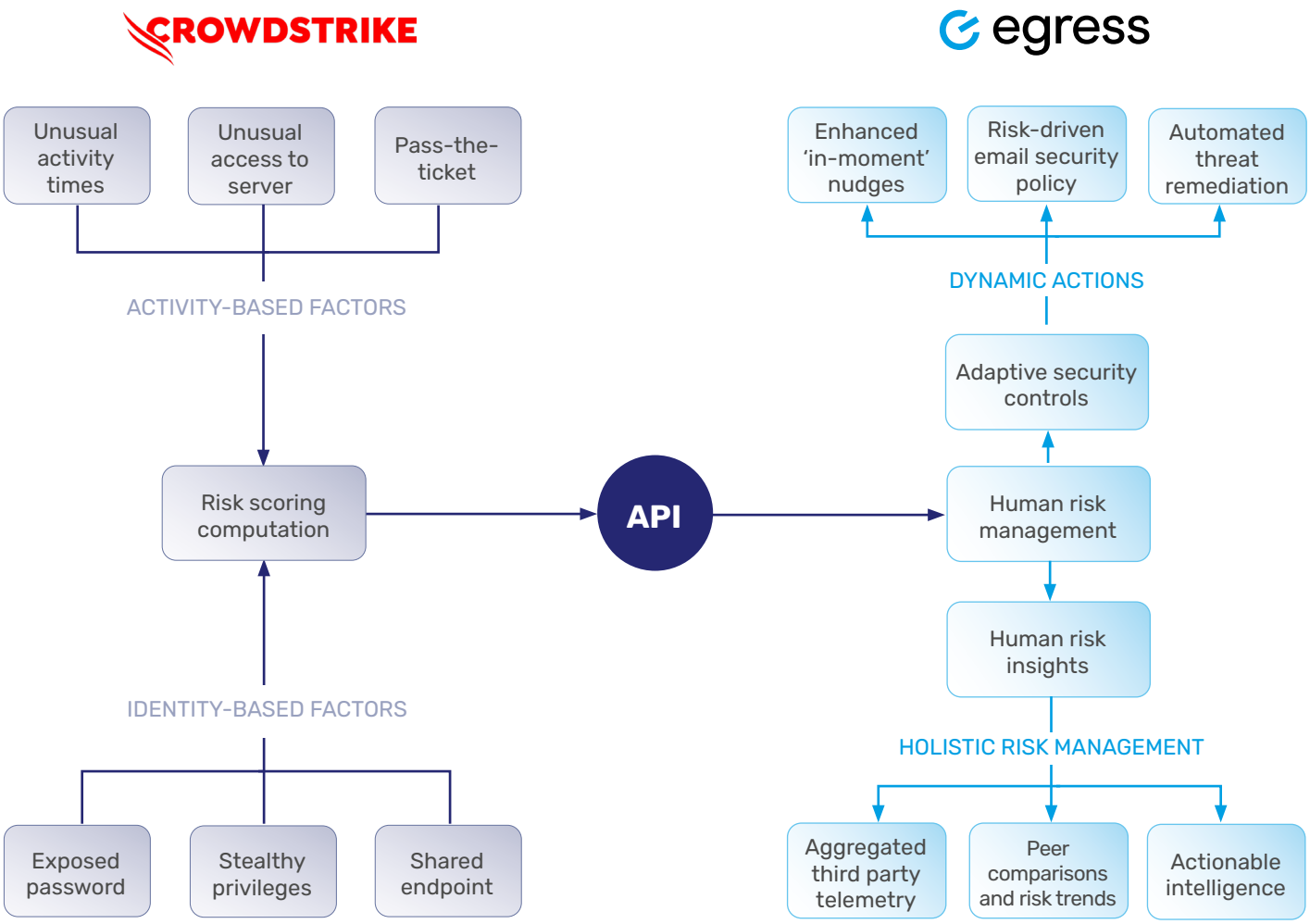
Matt Nears, VP, Global IT Security

Technical solution

The CrowdStrike Falcon® Identity Protection Risk Score enhances Egress' Intelligent Cloud Email Security platform by sending long-lasting and transient activity-based factors consolidated into a single user risk score. This CrowdStrike score is weighted against risk telemetry from Egress to create an aggregated human risk score that is leveraged dynamically to adapt security controls.

Using AI to identify and neutralize advanced threats, coupled with an adaptive security architecture that continually assesses human risk, CrowdStrike and Egress help deliver proactive cloud email security without any administrative overhead.

Out-of-the-box integration delivering aggregated threat intelligence



About Egress

Egress is the only cloud email security platform to continuously assess human risk and dynamically adapt policy controls, preparing customers to defend against advanced phishing attacks and outbound data breaches before they happen. Trusted by the world's biggest brands, Egress is private equity backed with offices in London, New York, and Boston.

www.egress.com