

Assess Your Cross-Domain Attack Risk

Adversaries are moving faster and across multiple domains. Use this checklist to find out what your risks are.

Today's cyber adversaries are faster, stealthier, and more sophisticated than ever. Rather than relying on traditional malware, they increasingly exploit valid credentials, misconfigured cloud services, and legitimate tools to move laterally across your environment, targeting multiple domains in one coordinated campaign. These cross-domain attacks bypass isolated defenses by slipping through the gaps between siloed systems and teams, often blending in with normal business activity and evading detection until it's too late and damage has been done.

To defend against these threats, organizations must evolve from reactive, siloed security to a unified approach built for speed, visibility, and coordination across domains. This starts with understanding where you stand today. This checklist is designed to help you assess your organization's exposure to cross-domain attack risk. By answering these targeted questions, you'll uncover critical requirements, spot potential blind spots, and identify where your defenses may need to evolve. Use it as a strategic tool to evaluate your current posture and take the next step toward a modern, unified security model that outpaces adversaries.

Adversary Spotlight: SCATTERED SPIDER Is Back with a Vengeance

A known eCrime actor is resurging with high-profile attacks on the retail sector, leveraging help desk social engineering, SaaS exploitation, and attempts to access VMware ESXi infrastructure. In recent intrusions, SCATTERED SPIDER deployed the DragonForce Linux ransomware variant, exploiting gaps in identity and cloud security.

Stopping attacks like these requires full-spectrum protection.

Are you prepared to stop cross-domain adversaries like SCATTERED SPIDER? Use this checklist to find out.

General Readiness

Modern adversaries exploit the gaps between siloed tools and teams to move undetected across your environment. Ensuring foundational readiness — such as unified visibility, integrated workflows, and rapid response capabilities — is essential to defend against fast-moving, cross-domain threats. A cohesive security architecture lays the groundwork for effective detection and containment before attackers can escalate their access.

- ☐ Do you have broad, correlated visibility across your endpoint, identity, cloud, and SaaS environments?
- ☐ Do your security tools integrate detections and accelerate response across domains?
- ☐ Can your SOC consistently respond to threats before the average eCrime breakout time of 48 minutes?
- ☐ Do you regularly conduct simulation testing or red teaming to assess cross-domain defense effectiveness?
- ☐ Are your security teams empowered to collaborate across all silos with shared workflows and threat context?
- ☐ Is your environment equipped to support a unified threat model that includes cloud, identity, and endpoint signals?

Identity Protection

Compromised credentials are now the top method for adversary access and the gateway to escalating privilege and traversing your environment. Identity-based attacks are stealthy, malware-free, and hard to detect without contextual awareness. Real-time identity protection is essential to uncover misuse, privilege abuse, and hybrid lateral movement between cloud and on-premises systems.

- ☐ Do you have systems in place to detect identity anomalies like off-hours access, unusual login patterns, and impossible travel?
- ☐ Are you able to identify hybrid lateral movement across identity providers (e.g., on-premises AD to Azure or Okta)?
- ☐ Can your tools detect and block privilege escalation attempts based on compromised or suspicious identities?
- ☐ Do you continuously assess user risk by correlating credentials with device trust and behavior analytics?
- ☐ Is identity telemetry integrated with your endpoint and cloud systems for a unified picture of adversary activity?
- ☐ Are SaaS and cloud access patterns governed by conditional access or behavioral-based identity risk signals?

Cloud and SaaS Security

Cloud environments and SaaS applications expand your attack surface and introduce new blind spots, especially when security controls are inconsistent. Adversaries exploit misconfigurations, abuse cloud-native tools, and remove forensic logs to maintain stealth. Protecting your cloud infrastructure and SaaS stack requires runtime visibility, access control correlation, and unified policy enforcement across all platforms.

- ☐ Are misconfigurations, vulnerabilities, and policy violations in your cloud environments automatically detected and prioritized?
- ☐ Can you track and respond to role changes, access anomalies, and escalation attempts within your cloud control plane?
- ☐ Are your SaaS apps continuously monitored for exposure risks, including unsanctioned data sharing or shadow IT usage?
- ☐ Can you detect adversary attempts to remove or tamper with cloud logging and telemetry?
- ☐ Are you enforcing consistent access controls and visibility across IaaS, PaaS, and SaaS environments?
- ☐ Do you correlate user activity, application behavior, and asset context in real time across cloud workloads?

Endpoint Security

Endpoints remain a critical attack vector for adversaries and a pivot point in cross-domain campaigns. Adversaries use legitimate tools, remote monitoring and management (RMM) software, and hands-on-keyboard tactics to gain footholds and remain undetected. Advanced endpoint protection must go beyond malware signatures to deliver AI-powered behavioral analysis and real-time response to disrupt attackers before they move laterally.

- ☐ Are your endpoints protected against fileless and malware-free intrusions using behavioral and contextual detection?
- ☐ Can your endpoint solution detect and block unauthorized RMM tools or misuse of legitimate admin software?
- ☐ Are your response mechanisms set up to respond in real time, kill processes, and remove malicious files without user disruption?
- ☐ Are endpoint detections automatically enriched with identity and cloud telemetry to reveal multi-domain risk?
- ☐ Can you detect hands-on-keyboard activity that mimics legitimate operations and evades traditional defenses?
- ☐ Are you using AI-powered indicators of attack (IOAs) to uncover stealthy adversary behavior early in the attack lifecycle?

Data Protection

In the age of GenAI and hybrid work, sensitive data moves faster — and is more exposed — than ever before. Insider threats, accidental leaks, and malicious actors all target sensitive information as it flows across devices, cloud apps, and AI systems. Modern data protection must detect misuse in real time, understand data context, and stop exfiltration before it becomes a breach.

- ☐ Do you have real-time visibility into sensitive data movement across endpoints, cloud services, SaaS apps, and GenAI tools, without needing separate agents?
- ☐ Can you classify sensitive data consistently across both endpoint and cloud environments using one classification engine?
- ☐ Are you able to detect and block unauthorized data movement, even if the content is encrypted, renamed, or obfuscated?
- ☐ Can you detect insider-driven exfiltration attempts based on behavioral anomalies, like mass downloads or unexpected access patterns?
- ☐ Can your system prevent data from leaking into personal or unauthorized GenAI tools, while allowing safe use of corporate AI platforms?
- ☐ Is sensitive data movement treated as a high-fidelity signal that integrates directly with incident response workflows?
- ☐ Can your cloud data protection solution detect and monitor sensitive data flowing to unauthorized destinations at runtime?

Threat Hunting and Incident Response

Detecting and disrupting cross-domain attacks requires more than passive defenses — it requires significant experience and demands active, intelligence-led hunting. Adversaries adapt rapidly, using tactics, techniques, and procedures (TTPs) that blend into legitimate activity and stretch across endpoint, identity, and cloud. Proactive threat hunting and automated incident response are critical to outpace attackers, uncover stealthy movement, and reduce dwell time from hours to minutes.

- ☐ Do you proactively hunt for stealthy adversary behavior using TTPs, not just known indicators of compromise (IOCs)?
- ☐ Can your threat hunters correlate endpoint, identity, and cloud telemetry to reveal the full scope of an intrusion?
- ☐ Are your teams equipped with real-time access to adversary intelligence and behavioral threat models?
- ☐ Do you have continuous 24/7 monitoring, with either in-house or managed threat hunting support?
- ☐ Are your incident investigations streamlined with integrated tools that reduce triage and containment time?
- ☐ Are security orchestration, automation, and response (SOAR) playbooks, automated threat disruption, and “click-to-hunt” capabilities embedded in your response stack?

What's Your Readiness?

Review your answers to see how you're stacking up against the threat of cross-domain attacks:

Mostly Yes:

Strong readiness.

You have broad coverage across key domains.

Focus on optimizing workflows, automating response, and proactively hunting threats.

Mix of Yes and No:

Moderate readiness.

You're on the right track, but critical gaps remain — especially in cross-domain visibility or real-time response. Strengthen integrations and prioritize areas marked “No.”

Mostly No:

At risk.

Your environment may be vulnerable to modern threats. Focus on eliminating silos, replacing outdated tools, and gaining unified visibility across endpoint, identity, and cloud.

Cross-domain attacks are designed to exploit fragmentation between tools, teams, and signals. This checklist is your starting point to uncover where those gaps may exist in your current environment. By honestly assessing your readiness across key security domains including endpoint, identity, cloud, data, and response, you gain clarity on where you're strong and where you're vulnerable.

No matter your current readiness, the path forward is clear: Unify visibility, accelerate detection and response, and adopt a platform approach that moves just as fast as the adversary — or even faster. The AI-native CrowdStrike Falcon® platform delivers exactly what you need to stop breaches by seamlessly connecting data, intelligence, and action across the entire attack surface.

Stay Protected from Cross-Domain Attacks

Once you've assessed your organization's readiness, take action to strengthen your defenses and stay ahead of today's fastest, stealthiest adversaries.

- Download CrowdStrike's [Combating Cross-Domain Attacks eBook](#) to learn more about how a unified approach to endpoint, identity, and threat hunting can close security gaps and stop breaches before they escalate.
- Join a [Hands-on Workshop](#) to experience how CrowdStrike's Falcon platform unifies detection and response across domains in a real-world, interactive environment.
- Read this year's [CrowdStrike Global Threat Report](#) to learn about the latest trends in adversary behavior, breakout speeds, and how today's most advanced threats are evolving.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: <https://www.crowdstrike.com/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

