

Compromise Assessment

Hunt for threat activity across your endpoint, cloud, and SaaS environments

Modern enterprises operate across hybrid environments — and adversaries are exploiting inadequate monitoring, weak security controls, and the growing complexity of today's IT ecosystems to evade detection and advance their objectives. Even organizations with advanced cybersecurity defenses may struggle to identify and mitigate threats, particularly as adversaries evolve their tradecraft. This challenge is especially evident in emerging technologies, such as SaaS and cloud, where security controls are often less mature. Moreover, threat actors increasingly pivot across multiple domains, leveraging gaps in security coverage to achieve their objectives and cause significant damage.

The consequences are familiar and frequent, according to public reporting: ongoing attacks compromising systems in under-monitored, almost-decommissioned, and recently acquired environments. These attacks often lead to massive data loss, long outages, intense disruption to business operations, expensive and distracting breach notification responsibilities, and costly (or even impossible) recovery and restoration operations. To effectively defend against these threats, organizations must have comprehensive visibility into both historical incidents and real-time activity across their entire cyber estate. Understanding past attacks and monitoring current threats are critical to strengthening security posture and ensuring resilience.

Threats to organizations today target multiple domains, rendering single-domain approaches wholly inadequate.

In 2024, there was a 26% increase in cloud intrusions compared to the previous year. SaaS applications were frequently targeted for credential theft and lateral movement, particularly Microsoft 365 (SharePoint and Outlook), which was accessed in 22% and 17% of cloud intrusions, respectively.¹

Key benefits

- **Uncover hidden threats:** Detect adversary activity across multiple domains by analyzing logs, system telemetry, and unauthorized changes coupled with indicators of attack (IOAs) and suspicious behaviors.
- **Minimize dwell time:** Break the attack lifecycle and prevent adversaries from executing on their objectives.
- **Reduce uncertainty:** Strengthen security investments with data-driven insights from a comprehensive threat hunt.
- **Proactively identify critical weaknesses:** Uncover critical vulnerabilities and high-risk practices that expose your organization to potential threats.

¹ [CrowdStrike 2025 Global Threat Report](#)

The Solution: Cross-Domain Compromise Assessment

CrowdStrike's cross-domain Compromise Assessment provides a comprehensive threat hunt to identify both ongoing and historical threat actor activity across multiple environments. This assessment covers endpoints (workstations, servers, and virtual machines), cloud platforms (AWS, Azure, Google Cloud, Oracle Cloud), identity platforms (Active Directory, Entra ID, Okta), network traffic analysis, and more than 60 SaaS platforms. Additionally, CrowdStrike identifies critical security issues that increase the risk of compromise, including the most serious misconfigurations, vulnerabilities, and security practices, to provide organizations with the insights needed to fortify their defenses against evolving threats.

The Compromise Assessment leverages the CrowdStrike Services team's years of experience in responding to intrusions by the most advanced adversaries, together with the comprehensive CrowdStrike Falcon® platform, industry-leading cyber threat intelligence, and 24/7 monitoring powered by CrowdStrike Falcon® Adversary OverWatch™. These forces combine to deliver the industry's most comprehensive assessment of your organization's IT environment, answering the critical question: "Has my organization been breached?"

CrowdStrike goes beyond traditional indicator-based, endpoint-only detections to deliver a compromise assessment based on both expert analysis of historical forensic evidence and real-time threat detection and hunting using the most advanced detection and response capabilities in endpoint, identity, SaaS, cloud, and network security.

Key capabilities

- **A highly skilled team:** The CrowdStrike Services team has unrivaled expertise and skills, having recruited the top experts from within the world of cybersecurity, incident response, forensics, and operations to conduct compromise assessments. The team has unique experience with the tradecraft and tactics, techniques, and procedures (TTPs) used by today's most skilled adversaries.
- **A comprehensive approach:** The assessment combines expert analysis of historical forensic evidence and real-time threat detection and hunting, allowing CrowdStrike to enumerate environments for suspicious activity across multiple domains, including endpoint, identity platforms, network, cloud, and SaaS.
- **The industry's leading tools:** The Falcon platform allows immediate, real-time visibility into your environment — using CrowdStrike Falcon® Insight XDR for Microsoft Windows, macOS, and Linux, CrowdStrike Falcon® Shield for SaaS security, CrowdStrike Falcon® Identity Protection, CrowdStrike Falcon® Exposure Management, and CrowdStrike Falcon® Cloud Security — to identify potential compromises and allow you to work on eliminating them. This offers a significant advantage over standard compromise assessments, which use classic forensics-based approaches that scan only for indicators of compromise (IOCs).

Why choose CrowdStrike?

- **Comprehensive defense platform:** CrowdStrike's unparalleled breadth and depth in the Falcon platform delivers real-time threat detection, proactive risk mitigation, and seamless workload protection across endpoint, cloud, identity, and SaaS.
- **Unmatched threat intelligence:** CrowdStrike's deep threat intelligence informs defensive security capabilities across every facet of cyber defense, drawn from proprietary channels and billions of monitored assets.
- **Unrivaled incident response:** With years of experience responding to the most advanced multi-domain breaches, CrowdStrike offers targeted proactive recommendations to minimize impact and strengthen resilience against future attacks.

- **A strong foundation for proven technologies:** The platform also includes Falcon Forensics Collector — a cross-platform, non-persistent, single-run tool to collect and aggregate data from more than 45 forensically significant artifacts on each endpoint — and Falcon Network Monitoring using the Corelight Open NDR Platform.
- **24/7 monitoring with Falcon Adversary OverWatch:** During the assessment, organizations benefit from the support of Falcon Adversary OverWatch threat hunting, which constantly monitors telemetry across multiple platforms and customers, identifying emerging threat techniques before they've been detected even by modern technology.

Learn More →

About CrowdStrike

CrowdStrike Services delivers Incident Response, Red Teaming, and Technical and Strategic Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: **We stop breaches.**

Learn more: www.crowdstrike.com/services/

Email: services@crowdstrike.com

