

FALCON SURFACE: EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)

The industry's most complete EASM technology stops breaches by minimizing risk from exposed assets

The digital footprint of organizations is expanding at an unprecedented rate. The move to the cloud, Internet of Things (IoT), digital transformation, connected supply chain partners and related trends have led to an explosion of internet-facing assets, cloud workloads, websites, user credentials, S3 buckets, SSL certificates, IoT, operational technology (OT), rogue IT devices and more. Now, a majority of digital assets are located outside the traditional enterprise infrastructure — falling outside the immediate control of IT teams.

Every asset that is connected to the internet represents a potential risk of an exposure that could lead to a data breach. Adversaries continue to refine reconnaissance methods to discover and exploit internet-facing assets, many that are rife with vulnerabilities. Their techniques to find these vulnerabilities can often outpace an organization's ability to discover and enforce good security hygiene on a digital asset. The unfortunate truth is that the adversary often has a better sense of the organizational risk exposure of their target than the target itself does.

CrowdStrike Falcon® Surface pinpoints unknown, exposed internet-facing assets so security teams can secure their ever-evolving digital perimeter. It enables them to detect, prioritize and manage all exposed internet-facing assets that are centralized or remote across on-premises environments and subsidiary, cloud and third-party vendors with a zero-touch approach.

Falcon Surface's intelligent internet mapping and association technology continuously indexes the entire internet and automatically maps companies' known and unknown assets, discovering exposures, risks and misconfigurations within and beyond their official network ranges. All exposed assets are automatically classified, analyzed and prioritized according to contextualized risk score. Falcon Surface also generates quick-to-implement, actionable remediation steps.

KEY BENEFITS

See what others miss, 24/7: Unmatched real-time discovery produces high-fidelity data augmented by the world's richest adversary intelligence

Prioritize risks with business context: Focus on what matters with context based on industry, CVE score, geolocation, attack history, asset type and manual edits

Get guided remediation: Respond to vulnerabilities in real time with quick-to-implement, guided and actionable remediation steps

Be future-proof: Extend protection from the outside-in to the inside-out spanning vulnerability management, IT hygiene, CNAPP and the holistic CrowdStrike Falcon® platform

FALCON SURFACE: EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)

SHUT DOWN SECURITY GAPS WITH AN OUTSIDE-IN VIEW OF THE ENTERPRISE ATTACK SURFACE

Falcon Surface offers continuous visibility into an organization's exposed assets, enabling security teams to stay on top of any changes with an always up-to-date asset inventory. It uses a proprietary real-time 24/7 engine to scan the entire internet, across the globe, enabling organizations to see how their attack surface looks from an adversary's country-centric view. Its mappers index over 7 billion exposed assets globally each year, with 140 million identified each week.

- Mapping an entire ecosystem is based solely on domain addresses — including third-party vendors, subsidiaries and cloud environments. It is non-intrusive and identifies a variety of asset types, including endpoints, nodes, servers, IoT devices, OT and more.
- Artificial intelligence (AI)-enabled association engines correlate an asset to its source regardless of “official” ownership or not, through multiple identifiers like certificates, subdomains or other means. In addition, the platform can match an organization to its industry, a key component to contextualizing the highest priority risks for network security.
- The detailed discovery path allows for reviewing the association to vulnerable exposed assets and understanding its history and context.

PRIORITIZE ATTACK SURFACE RISKS WITH INDUSTRY-LEADING ADVERSARY INTELLIGENCE AND AI-POWERED INSIGHTS

CrowdStrike's industry-leading threat intelligence and AI-powered attack surface insights help you find the most critical exposures based on risk and business context to determine what needs to be addressed first. Falcon Surface provides each customer with an automated prioritization metric designed for the organization's specific needs, considering its industry, CVE score, geolocation, attack history, asset type and customer's manual edits. Falcon Surface streamlines alerts and action with built-in integrations that enable teams to activate playbooks, push data into workflows and quickly resolve issues using Slack, ServiceNow, Jira and other systems.

The module's automatic risk prioritization is based on:

- Business context: geolocation, industry, cyberattack history and more
- Asset type
- CVE scores
- Manual edits

Exposures and security issues are flagged and prioritized dynamically so security and IT teams know what to tackle first at any time.

ALIGN SECURITY AND IT TEAMS WITH ACTIONABLE REMEDIATION STEPS

For every identified risk, such as application end-of-life (EOL) versions, Falcon Surface automatically generates quick-to-implement, actionable remediation steps for IT and security teams to apply for real-time vulnerability mitigation. With its surgical yet clear remediation steps, it optimizes teams' productivity, increases efficiency and reduces exposure time. Neither special skills nor knowledge are required — just follow the steps.

COMMON USE CASES

Discover unknown digital assets

Manage your attack surface

Secure your cloud development journey

Track subsidiaries security

Monitor supply chain and third-party risks

Assess merger and acquisition (M&A) security risks

Reduce cyber insurance premiums

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/>

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

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

© 2022 CrowdStrike, Inc. All rights reserved.