CROWDSTRIKE

Unlock Proactive Exposure Management:

5 Key Elements and Why Traditional Approaches Fail

Proactively reduce risk with unified, AI-powered vulnerability prioritization and complete attack surface visibility

Presented by:

TD SYNNEX Public Sector | DLT™

CrowdStrike eBook

Defending the Modern Enterprise

Modern organizations face unprecedented challenges in securing a rapidly expanding attack surface. With a growing number of cloud, bring your own device (BYOD), IoT/OT and software-as-a-service (SaaS) assets to protect, many security teams grapple with how to solve modern problems using legacy tools and processes.

The first step to a strong defense is understanding your assets and threat landscape — and that's where many fall short. Organizations often attempt to defend their growing attack surface with multiple point products, but this creates coverage gaps for adversaries to exploit. Merely knowing what they need to protect is a challenge for most security teams.

Meanwhile, adversaries are getting smarter, bolder and faster. The average breakout time for eCrime intrusion activity dropped to just 62 minutes in 2023, and the fastest observed time was only 2 minutes and 7 seconds, according to the CrowdStrike 2024 Global Threat Report. Those targeting your organization grew faster and more capable last year. Did you?

Understanding your assets, exposures and adversary context requires a modern approach that traditional vulnerability management, IT asset management and external attack surface management solutions lack. The growing field of exposure management takes a more comprehensive approach to protecting endpoints, servers and cloud workloads from modern attacks.

This ebook unlocks the benefits of exposure management and explains how it outpaces traditional vulnerability management solutions.

The average breakout time for eCrime intrusion activity was just 62 minutes in 2023, and the fastest observed time was only 2 minutes and 7 seconds.

Source: CrowdStrike 2024 Global Threat Report

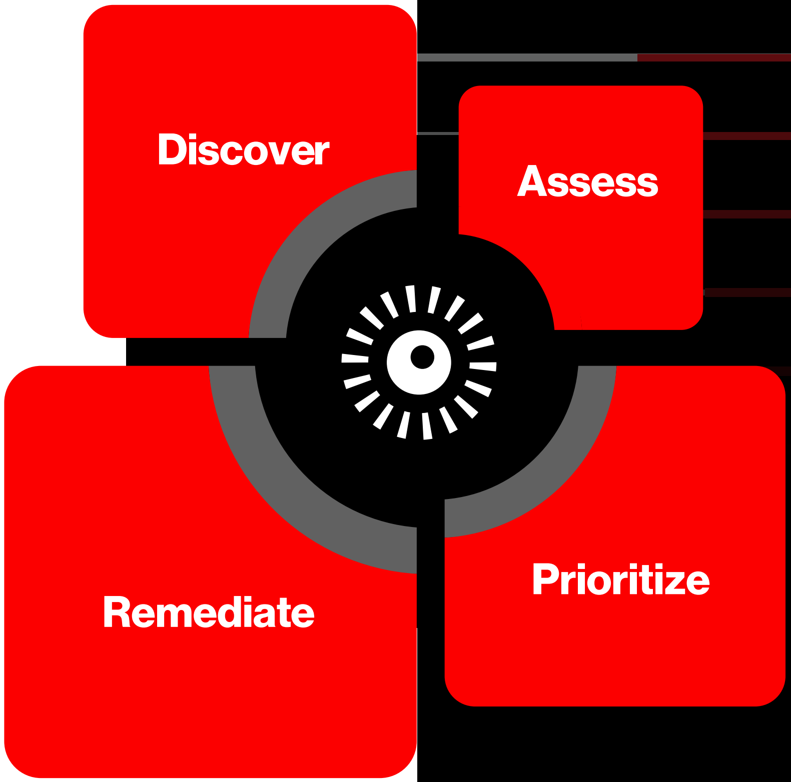
What Is Exposure Management?

Exposure management is a proactive approach to cybersecurity that takes a broader view of managing risks to prevent cyberattacks. It provides a more comprehensive picture of your digital assets and risk while helping to streamline management and remediation workflows.

This approach considers the expanding types of attack surface, including external-facing assets and cloud infrastructure. To detect assets that may put organizations at risk, exposure management alerts to multiple vulnerability types, including common vulnerabilities and exposures (CVEs) and non-CVE vulnerabilities and misconfigurations.

Four aspects of exposure management

- **Asset discovery:** Identify and inventory all internal and external assets, along with their business criticality.
- **Risk assessment:** Use adversary context and attack path analysis to quickly see how each asset is exposed and how exposures can be exploited.
- **Prioritization:** Leverage AI across internal and external exposures to prioritize vulnerabilities based on risk level to your organization.
- **Remediation and mitigation:** Use compensating controls such as killing running processes, closing ports and blocking removable media devices to remediate threats.



Where Legacy Vulnerability Management Falls Short

Since the turn of the century, security teams have used vulnerability management tools to detect and address CVEs. But in today's complex business environment, these outdated technologies leave security teams with many unanswered questions:

What are the attack paths associated with exposed assets?
Legacy vulnerability management tools make it hard to identify which exposed assets adversaries are likely to exploit for compromise and lateral movement. For example, one compromised endpoint could connect into cloud infrastructure, giving the adversary only two steps to reach a critical asset. But would you know if they did?

How are adversaries using this exposure in the wild?
To effectively prioritize risk remediation efforts, you must be able to see which exposures are actively being used by adversaries in the wild. This includes seeing if there's an exploit kit available, if the exploit kit is being used, which adversaries are using it, which industries are under attack and other critical information. Legacy vulnerability management tools lack this context.

What does this risk score really mean?
Risk scores typically rely on commodity sources of intelligence, leaving many organizations wondering how real the risk is for their organization. Instead, risk scores should be based on deep, real-world telemetry sourced from front-line adversary intelligence across endpoint, identity and cloud to deliver more relevant insights.

Am I able to continuously find new exposures?
Legacy vulnerability management is based on complex scanning technology that impacts network performance, leading to intermittent vulnerability and risk information. That's not good enough. Since exposures happen in real time, organizations need a way to continuously find new exposures and the risks associated with them to effectively prevent breaches.

See why IDC named CrowdStrike a Leader in the IDC MarketScape: Worldwide Risk-Based Vulnerability Management Platforms 2023 Vendor Assessment

Five Key Elements Behind Why Traditional Approaches Fail

Exposure management builds on legacy vulnerability management technology, serving as the next frontier for how organizations can more effectively reduce cyber risk.

1. It provides more comprehensive attack surface visibility across endpoints, servers and cloud workloads. You can't secure what you can't see. Exposure management delivers complete, near-real-time visibility from the inside out and outside in with deep context into areas where legacy vulnerability management tools can't reach, including external-facing assets and exposures, logins, applications and accounts.

2. It finds weaknesses, including internet exposures, potential attack paths and misconfigurations. Exposure management shuts down adversary opportunities by looking beyond vulnerabilities to identify risk from novel attack techniques.

3. It prioritizes risk to make remediation efforts most impactful. Stop looking for a needle in a needle stack. Exposure management uses AI and machine learning to cut through the noise and prioritize remediation efforts that will have the greatest impact on your organization.

4. It brings adversary-driven threat intelligence to the forefront. The better you know the adversary, the better you can defend against them. Exposure management infuses adversary-driven threat intelligence to help you clearly understand the risks associated with your exposures so you can prioritize and mitigate them.

5. It facilitates remediation — not just notification. To reduce risk, you must take action. Exposure management delivers tightly integrated remediation actions and the ability to integrate third-party tools to quickly mitigate cyber risk across your entire attack surface.

While exposure management is an approach that requires people, processes and technology, investing in an exposure management tool is half the battle, as it will get you to your goal faster to build a proactive security posture. Let's explore the CrowdStrike approach to exposure management.

The CrowdStrike Approach to Exposure Management

CrowdStrike now offers an incredibly powerful and popular exposure management tool delivered as part of the unified, AI-native Falcon platform.

The CrowdStrike Falcon® Exposure Management module reduces cyber risk by enabling you to prioritize and proactively remediate vulnerabilities that could lead to a breach. The tool combines CrowdStrike's industry-leading threat intelligence with AI-based vulnerability telemetry from the Falcon platform to help you predict attack paths and prioritize risk mitigation actions to stop breaches before they happen.

Complete attack surface visibility: Reduce risk with real-time visibility of all internal assets, external assets and unknown exposures without complex scanning infrastructure.

AI-powered risk prioritization: Proactively stop breaches with analytics-based vulnerability prioritization and predictive attack path mapping sourced from front-line adversary insights.

Consolidate point products with a unified platform: Cut complexity and costs by consolidating risk-based vulnerability management (RBVM), IT asset management (ITAM), external attack surface management (EASM), and continuous attack surface management (CASM) tools with an integrated platform, delivered from a single lightweight agent.

With Falcon Exposure Management, you no longer have to boil the ocean and patch every system. Reduce noise by 95% on average compared to legacy vulnerability management tools with a modern tool built for today's complex business environment and threat landscape.

The AI Advantage

How does CrowdStrike turn thousands of vulnerabilities into the handful you should care about? The answer lies in AI. While other vendors rely on third-party data to power their exposure management offerings, CrowdStrike uses predictive ExPRT.AI prioritization models, trained on world-class threat intelligence and Falcon detection data, to surface the vulnerabilities that are most likely to be exploited — so you can focus your resources on what matters most.

Falcon Exposure Management reduces noise by 95% on average compared to legacy vulnerability management tools.

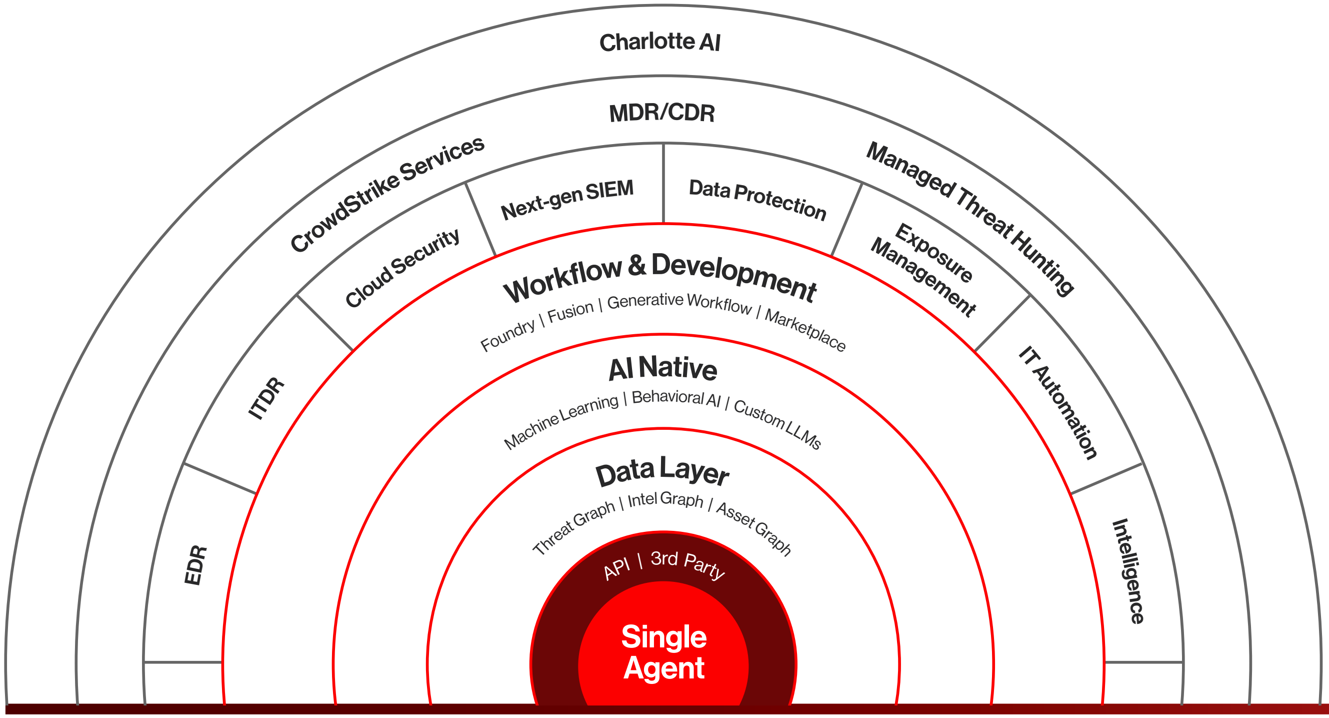
Source: These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.

Consolidate Point Products with the CrowdStrike Falcon Platform

Organizations are embracing cybersecurity consolidation to reduce cost and complexity, while improving security outcomes. The field of exposure management is no exception.

Identifying and addressing vulnerabilities requires a unified platform approach that brings together real-time security and IT data with threat intelligence, extended detection and response (XDR) telemetry, and AI-powered exploit prioritization.

By delivering Falcon Exposure Management as a tightly integrated capability built on the Falcon platform, organizations can consolidate vulnerability management point products, eliminate additional agents and unify protection against adversary intrusion.



Outpace Adversaries, Prevent Breaches

If you're only thinking about vulnerability management, you're not thinking big enough.

As adversaries weaponize vulnerabilities with greater speed, organizations must also accelerate their ability to identify security gaps and proactively manage their risk exposure before a breach occurs. Exposure management extends the capabilities of vulnerability management to help organizations reduce cyber risk across the entire attack surface.

Next Steps

- Schedule a Falcon Exposure Management demo
- Register for hands-on workshop: Empowering Proactive Protection with CrowdStrike Falcon Exposure Management
- See Falcon Exposure Management in action
- Read the IDC MarketScape: Worldwide Risk-Based Vulnerability Management Platforms 2023 Vendor Assessment

CROWDSTRIKE

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.

Follow us: Blog | X | LinkedIn | Facebook | Instagram
Learn more: https://www.crowdstrike.com/

Presented by:

TD SYNNEX Public Sector | DLT