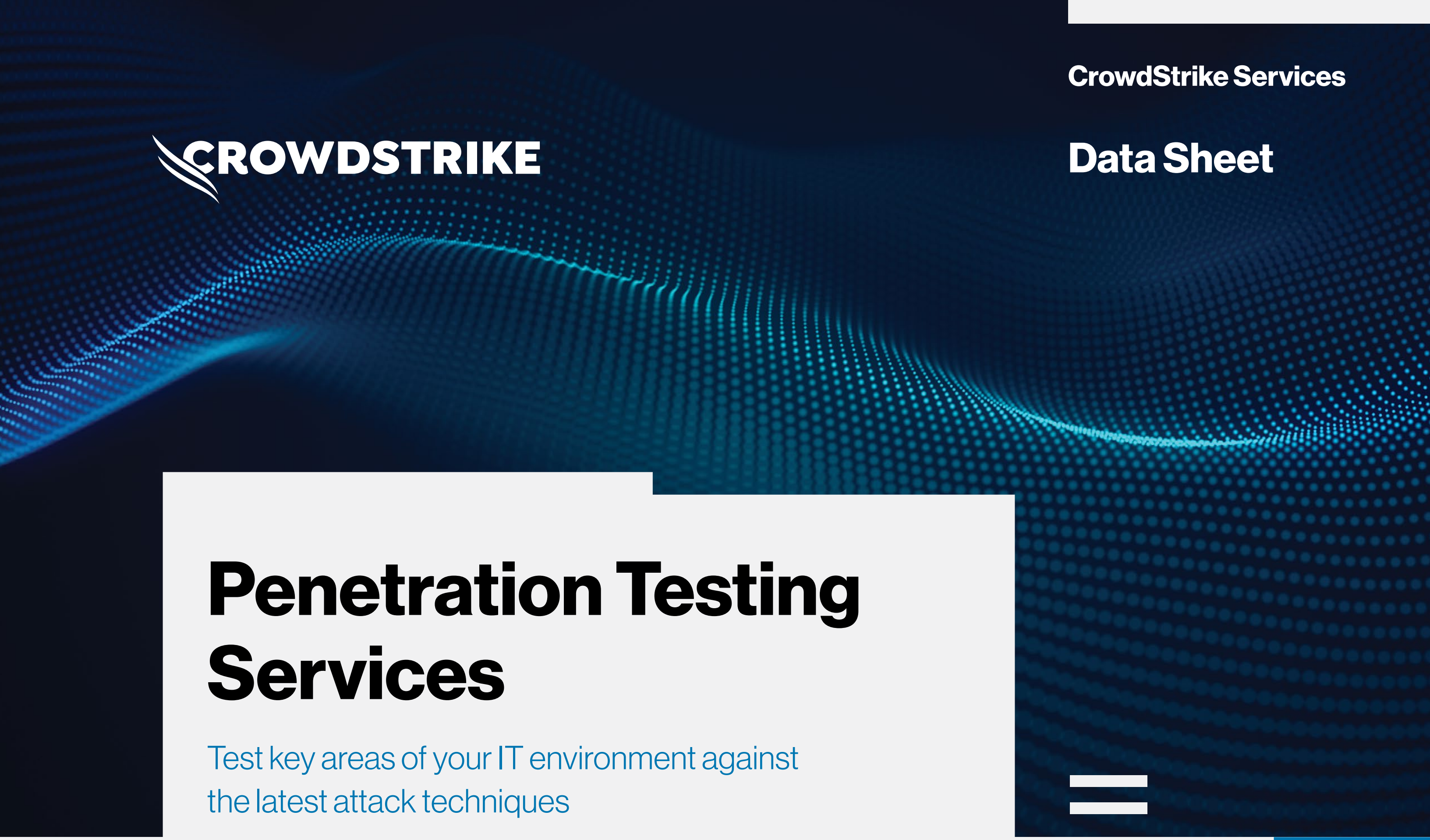

CrowdStrike Services

Data Sheet

Penetration Testing Services

Test key areas of your IT environment against the latest attack techniques

Testing for sophisticated attacks can be daunting

Testing the different components of your IT environment is a continuous and often daunting task that can include applications, networks, firewalls, wireless, mobile, insider threats and more — the list goes on. At the same time, understanding the latest attack techniques — and testing and assessing your defenses against those types of attacks — is critical to improving your cybersecurity posture.

To stop today's sophisticated attacks, identifying vulnerabilities requires more than simply running a scan of your IT environment. Identifying an existing vulnerability is only the first step — you gain a much deeper insight into your environment when you understand how attackers could exploit that vulnerability and test how far they might be able to penetrate into your network and systems.

Mimic advanced attacks to test your defenses

To truly protect your environment, you need to know which adversaries are more likely to target your organization so you can mimic their advanced tactics to better test your defenses.

CrowdStrike Penetration Testing Services simulates real-world attacks on different components of your IT environment to test the detection and response capabilities of your people, processes and technology in order to identify where vulnerabilities exist.

Key benefits

Identify and mitigate vulnerabilities throughout components of your IT environment, reducing the attack surface for today's advanced threats

Gain an objective perspective, exposing blind spots and gaining visibility into security gaps that could be missed by your internal IT teams due to lack of expertise or unfamiliarity with the latest threats

Test the investments you have made in your cybersecurity tools and technology to determine if any vulnerabilities or gaps exist and whether they can stop a sophisticated attack on your organization

Prioritize your security budgets where they are needed most, saving money over the long term by preventing wasteful expenditures on issues related to the broader security landscape

Key service features

CrowdStrike delivers penetration testing services to test components of your IT environment against today's sophisticated attack techniques and tactics.

There are several types of penetration tests that are designed to meet the specific goals and threat profile of an organization. Below are some of the most common types of penetration tests delivered by CrowdStrike Services.

Internal red team exercise	External network penetration testing
Assesses your organization's internal systems to determine how an attacker could move laterally throughout your network. The test includes system enumeration, exploitation, privilege escalation, lateral movement and objectives.	Assesses your internet-facing systems to determine if there are exploitable vulnerabilities that expose data or unauthorized access to the outside world. The test includes system identification, enumeration, vulnerability discovery and exploitation.
Web application penetration testing	**Mobile application penetration testing**
Evaluates and uncovers serious vulnerabilities in your web applications — using a three-phase process of reconnaissance, discovery and exploitation — to identify vulnerabilities that can lead to unauthorized access to sensitive data through your web applications.	Evaluates and uncovers serious vulnerabilities in your mobile applications by simulating real-world attacks from threat actors to gain unauthorized access to sensitive personal data, tamper with your mobile application or compromise the integrity of the system.
Wireless network penetration testing	**Insider threat penetration testing**
Identifies the risks and vulnerabilities associated with your wireless network. The team assesses weaknesses such as deauthentication attacks, misconfigurations, session reuse and unauthorized wireless devices.	Identifies the risks and vulnerabilities that can expose your sensitive internal resources and assets to those without authorization. The team assesses areas of escalation and bypass to identify vulnerabilities and configuration weaknesses in permissions, services and network configurations.

About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Technical Assessments, Training and 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.

Why choose CrowdStrike?

Real-world expertise

The CrowdStrike team has unrivaled expertise and skills drawn from vast, deep experience in incident response, forensics and red team engagements to create attacks using real-world threat actor tools that expose vulnerabilities within your environment.

Advanced threat intelligence

CrowdStrike uses the most advanced threat intelligence to understand the tactics, techniques and procedures (TTPs) that adversaries will use to penetrate your environment and disrupt your business operations.

Going beyond vulnerability scanning

CrowdStrike engagements deliver more than just a simple vulnerability scan. These tests are designed to penetrate deep into your networks, exploit your vulnerabilities, and identify where security gaps exist and how to close them.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com