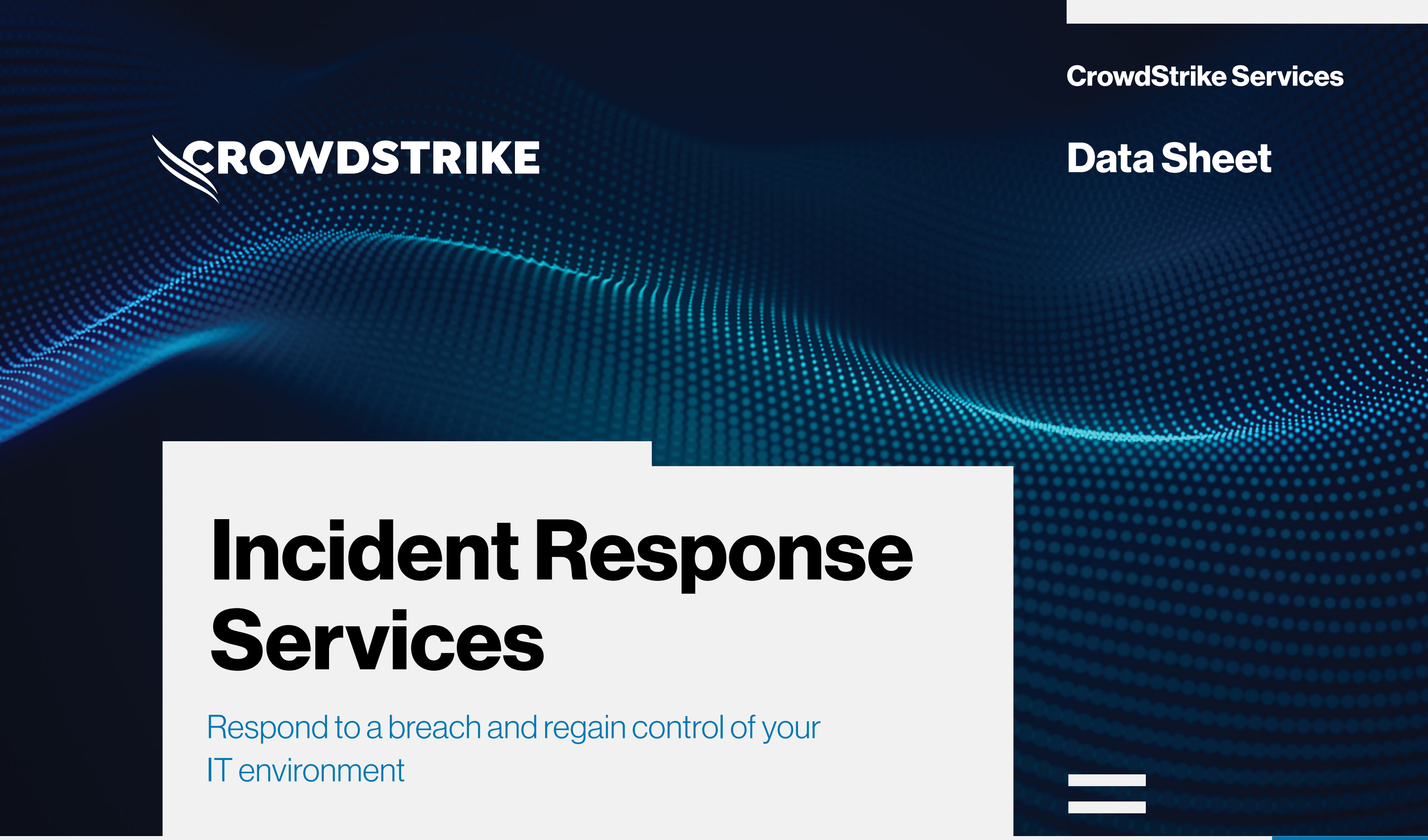

CROWDSTRIKE

CrowdStrike Services

Data Sheet

Incident Response Services

Respond to a breach and regain control of your IT environment

Cybersecurity incidents can be devastating

There are countless reports in the media highlighting the damaging effects a cyber incident can have on an organization. The reality is any organization (large or small) is likely to encounter a cyber incident at some point in time.

The way you respond to an attack can be the difference between stopping a breach before an adversary can complete their mission and failing to stop a breach, resulting in significant business interruption to operations and severe financial consequences.

When a breach occurs, time is of the essence

IT security leaders need to respond quickly to security incidents to stop breaches from disrupting their business and get back to normal operations faster.

Organizations under attack need the support of an experienced, fast and precise incident response (IR) team that has the right technology to gain visibility into the attack and gather the forensic evidence needed to understand what happened and which systems were compromised.

CrowdStrike® **Incident Response Services** delivers immediate threat visibility and active threat containment to eject adversaries from your network and recover your systems with speed and precision. CrowdStrike's accelerated forensic analysis reduces investigation time and provides the insight needed to quickly recover systems in real time with the aid of the CrowdStrike Falcon® platform.

Key benefits

Gain immediate visibility into the full threat context to contain the incident and stop a cyber breach

Accelerate the investigation and recover in real time to reduce the cost of the attack

Avoid costly downtime and minimize business disruption

Recover with speed and precision to get back to normal business operations faster

Key service features

CrowdStrike Incident Response Services brings the expertise of front-line responders, investigators, hunters and recovery specialists armed with the full power of the CrowdStrike Falcon platform to investigate a breach and recover from an incident with speed and precision. CrowdStrike experts use an intelligence-led rapid recovery approach that includes the following:

- **Rapid technology deployment** of the cloud-based Falcon platform and sensors
- **Immediate threat visibility** that enables CrowdStrike experts to quickly understand the full threat context and navigate the fastest path to business recovery
- **Active threat containment** using blocking and prevention policies to stop the spread of the attack to other systems on the network
- **Accelerated forensic analysis** to collect relevant artifacts from select subsets of infected systems and conduct triage analysis of the tradecraft being used in the attack
- **Real-time response and recovery**, armed with the intelligence of knowing what actions a threat actor executed, to surgically undo and remove the threat to recover systems with speed and precision
- **Enterprise remediation** to reduce the number of systems requiring full remediation (reimage or rebuild) to a manageable number
- **Monitoring and threat hunting** to monitor the environment for hands-on-keyboard activity and stop any reinfection that may occur
- **Managed detection and response** by the CrowdStrike Falcon® Complete team to stop future attacks

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?

People

CrowdStrike cybersecurity consultants bring decades of experience and have responded to many high-profile incident response cases.

Process

CrowdStrike intelligence-led rapid recovery approach reduces recovery time by as much as 5X and business interruption costs by as much as 10X over other IR firms.

Technology

CrowdStrike IR engagements are enabled by the full power of the CrowdStrike Falcon platform to deliver immediate visibility and rapid response to an active threat.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com