CROWDSTRIKE

CrowdStrike Services

Data Sheet

Endpoint Recovery Services

Rapid recovery from advanced persistent threats and attacks with zero business interruption

A race against the clock

When a breach occurs, quick remediation and recovery are critical to minimize the impact on your business. Advanced persistent threats can quickly break out across your network, infecting your endpoints, laterally moving across your systems and disrupting your business operations.

These very sophisticated, sustained cyberattacks often establish multiple points of undetected persistence in your network to infect your systems with malware or steal sensitive data over a prolonged period of time. These attacks are carefully planned and designed to infiltrate your organization, evade existing security measures and fly under the radar. Most importantly, if coordinated and effective countermeasures are not taken to remove all points of persistence, the attacker will continue to reinfect systems after initial remediation, causing further delays and interruptions to business recovery.

The need for speed to recovery

Once a breach has occurred, the timeliness and accuracy of the decisions made by your security teams will make or break your ability to recover from the attack and resume normal business practices with minimal impact. Today's sophisticated attacks can go unnoticed with the wrong technology, and even after detection, they can cause confusion within your environment as unequipped and inexperienced security teams race against the clock to stop these types of destructive malware.

CrowdStrike® Endpoint Recovery Services delivers the right combination of technology, intelligence and expertise to assist you with the detection, analysis and remediation of known security incidents and enable rapid recovery with minimal business interruption. CrowdStrike's solution can be deployed within hours of a breach, so you can get back to business faster and be confident that your attackers will not reappear.

Key benefits

Stops attacks immediately: Deploy the CrowdStrike Falcon® platform quickly to eradicate threat actors and prevent further attempts to compromise your environment.

Recovers environments rapidly: Quickly identify and mass-remediate malicious artifacts and persistence vectors to prevent re-exposure, with an average time to remediation of 72 to 96 hours.

Minimizes business disruption: Restore business operations efficiently and effectively without having to reimage or reissue devices.

Reduces cost to recover: Reduce the average recovery time from weeks or months to days, with zero interruptions so you can get back to business right away.

Provides continued support: After the recovery phase (typically the first 72 to 96 hours), CrowdStrike Services continues to monitor and remediate security threats.

Key phases of a recovery engagement

CrowdStrike Endpoint Recovery Services is available in 30-day increments to enable the fast recovery of endpoints across your network. For the term of your engagement, CrowdStrike monitors your environment using the global security expertise of the CrowdStrike® Falcon OverWatch™ team to prevent any new or recurring attacks.

Prevention

- Within the first 24 hours of an engagement, the rapid deployment and configuration of the Falcon platform and sensors begin, with powerful prevention policies to immediately stop the execution and lateral movement of active attacks.

Recovery

- Over the next 72 to 96 hours, the CrowdStrike Services team leverages the Falcon platform to analyze attacks and actively remediate and remove any memory-resident malware, persistence and other active attack components.
- The Services team makes recommendations based on the security events identified within the Falcon console. Combining attack intelligence and the analyzed data points, the team provides insight into the probable cause, attack technique and/or vulnerability to enable recovery and prevent further occurrences.
- The focus of the engagement is fast and efficient recovery of endpoints with no business disruption and excludes full forensic investigation.

Monitoring

- In the post-recovery period and for the remainder of your service engagement, CrowdStrike continues to monitor your environment for any re-emergence of the previous incident and detects and remediates any new incidents or attempts to breach your network.
- The OverWatch threat hunting team monitors for attack techniques designed to bypass even the best security technology and communicates directly with the recovery team when attacker behavior is observed and remediation is required.

Reporting

- At the conclusion of the service engagement, the recovery team provides a final report (executive summary and technical description) that outlines observations, analysis and recovery actions taken during the engagement.

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?

CrowdStrike is an industry leader in endpoint protection and incident response, delivering the right combination of technology, intelligence and expertise to rapidly detect breaches, investigate attacks, eject adversaries and remediate your endpoints so you can recover from an attack with minimal disruption.

Leading technology platform: The cloud-native Falcon platform deploys within hours to quickly detect and investigate an attack, ejecting the adversaries from your environment.

Intelligence-led remediation: CrowdStrike's global threat intelligence leverages the latest indicators of attack (IOAs) and indicators of compromise (IOCs) to detect even the most sophisticated and advanced persistent threats that might be operating undetected within your environment.

Cybersecurity expertise: CrowdStrike security analysts bring years of experience and expertise, interacting directly with your infected endpoints to remove any residual artifacts and persistence mechanisms, thereby preventing reinfection without the need to reimage your machines.

Rapid recovery: With CrowdStrike's market-leading endpoint technology, global threat intelligence capabilities and unrivaled security expertise, you get back to business faster as you recover your environment from the most sophisticated attacks and advanced persistent threats.

Learn more
www.crowdstrike.com/services

Email
services@crowdstrike.com