CROWDSTRIKE

ENDPOINT RECOVERY SERVICES

Minimize business disruption and recovery costs from widespread attacks with real-time response

A RACE AGAINST THE CLOCK

Today's sophisticated, widespread ransomware and malware attacks infect hundreds and sometimes thousands of endpoint systems. Traditional recovery methods of reimaging, rebuilding and replacing so many endpoints is simply too time-consuming, too inefficient and too costly to be effective. This approach places your business at serious risk of downtime and business interruption, substantially increasing the overall cost of an attack.

THE NEED FOR SPEED IN RECOVERY

When a breach occurs, time is of the essence. The speed to remediation and recovery is critical for minimizing the impact to your business operations. You need to engage a recovery team that can respond quickly, in real time, to contain the threat and recover your endpoints with speed and precision.

CrowdStrike® Endpoint Recovery Services delivers the right combination of endpoint protection technology, threat intelligence and incident response expertise to help you quickly identify and contain the threat, eject the adversary from your network, and recover and mass-remediate your endpoints with minimal disruption to your users — so you can get back to business faster.

CrowdStrike's intelligence-led, rapid recovery approach uses the power of the CrowdStrike Falcon® platform and the Falcon Real Time Response (RTR) capabilities of the Falcon sensor to remotely remove malicious artifacts and persistence mechanisms from your endpoints and restore your environment to an operational state.

KEY BENEFITS

- CONTAIN THREATS QUICKLY
- RECOVER ENDPOINTS WITH SPEED AND PRECISION
- AVOID BUSINESS INTERRUPTION
- REDUCE RECOVERY COSTS

KEY SERVICE FEATURES

CrowdStrike Endpoint Recovery Services is available in 30-day increments to enable the rapid recovery and mass remediation of endpoint systems across your network. For the term of your engagement, CrowdStrike monitors your environment using the global security expertise of the CrowdStrike Falcon OverWatch™ threat hunting team to identify any hands-on-keyboard activity and other attempts by the threat actor to breach your network.

PREVENT FURTHER SPREAD OF ATTACK

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

RECOVER SYSTEMS IN REAL TIME WITH MINIMAL DISRUPTION

The CrowdStrike endpoint recovery team immediately leverages the Falcon platform to analyze the attack and actively remediate and remove any memory-resident malware, persistence mechanisms and other active attack components.

The recovery team makes recommendations based on the security events identified within the Falcon console. Combining attack intelligence and analyzed data points within the Falcon console, the team provides insight into the probable cause, attack technique and vulnerability used to exploit the environment. With a detailed understanding of the attack vectors, the recovery team uses the RTR capabilities of the Falcon sensor to remotely access impacted endpoints to perform detailed analysis and required remediation actions, including (but not limited to):

- List current network connections and configuration
- Explore the file system and delete infected files
- List running processes, extract process memory and kill malicious processes
- Extract event logs, query system registries and restore registry entries
- Identify and remove scheduled tasks
- Execute scripts for additional custom/mass remediation tasks

Using RTR, the recovery team can rapidly and effectively remediate 1, 100, 1,000 or 10,000s of impacted systems within the environment with minimal user disruption and no business downtime.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon® platform — including next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

Learn more at www.crowdstrike.com/services/
Email: services@crowdstrike.com

© 2021 CrowdStrike, Inc. All rights reserved.

WHY CHOOSE CROWDSTRIKE?

Superior technology platform: The Falcon platform is easily deployed and quickly detects active threat activity that other solutions have missed.

Intelligence-led approach: Identify detailed threat activity using high-fidelity behavioral indicators of attack using the threat intelligence capabilities of the Falcon platform.

Response in real time: Recover hundreds or thousands of endpoints in your environment using the Real Time Response capabilities of the Falcon platform.