

Taegis MDR Proactive Response Actions

Accelerate Response With Decisive Actions to Stop Threats

Discovering a threat is only one step in staying ahead of threat actors. There has to be an ability to respond, and in those moments, time is critical to keep adversaries from inflicting damage. Certain pivotal actions performed immediately, such as blocking a host or disabling a user, can accelerate response time.

Secureworks® Taegis™ MDR customers can take advantage of multiple Proactive Response Actions that allow our Security Analysts to perform these kinds of immediate actions to mitigate detected threats. Customers have the option to allow Secureworks to take these predetermined actions without contacting the customer. This can be crucial for customers who have limited team availability, operate on a non-standard schedule, or are out of office for a period of time.

Why Proactive Response Actions are Helpful

An effective security solution should help ease the burden that determining response puts on a customer’s security resources. Proactive Response Actions remove the question of how to approve and apply individual response actions, instead formulating a proactive plan before an incident is detected. Taegis MDR customers can select which Proactive Response Actions to enable, clearing the way for Secureworks Security Analysts to apply their expertise and take decisive action on the customer’s behalf. And there’s flexibility built right in: Customers can opt out of or change any previously determined Proactive Response Action plan at any time.

Available Proactive Response Actions

Red Cloak agent isolate	Microsoft Defender ATP isolate	Entra ID disable user	AWS disable user login
Red Cloak agent undo isolate	Microsoft Defender ATP undo isolate	Entra ID enable user	AWS enable user access key
Taegis agent isolate	Carbon Black Cloud isolate	Entra ID force password reset	AWS disable user access key
Taegis agent undo isolate	Carbon Black Cloud undo isolate	Taegis NDR block	AWS disable user MFA device
CrowdStrike Falcon endpoint isolate	SentinelOne endpoint isolate	Taegis NDR unblock	
CrowdStrike Falcon endpoint undo isolate	SentinelOne endpoint undo isolate	AWS enable user login	

Contact your Secureworks sales representative today to learn how Taegis cybersecurity solutions can help you **secure your mission**.

About Secureworks

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis™, an AI-native security analytics platform built on more than 20 years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.



For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com