CRITICALSTART®

SOLUTION BRIEF

Protect against user account attacks

Managed Detection & Response Services
Microsoft Security Consulting Services

Harness the value of Microsoft 365 Defender to protect against user account attacks

Adversaries have multiple attack vectors to steal, harvest and misuse user account credentials. This diversity of attack lines severely limits how endpoint-oriented response actions can fully disrupt an active misuse of a stolen user credential across authentication sources and cloud applications.

Organizations need a solution that extends their cyber defender team's ability to investigate each and every alert. Even missing one successful credential attack can lead to data compromise.

KEY SOLUTION BENEFITS

Prevent identities from being compromised

Organizational barriers are blurring the lines between who is in and out of your network. Personal devices and remote work mean that data is no longer centralized behind traditional network security. Microsoft Security Consulting workshops help you understand how identity can be a fundamental pillar of your end-to-end security program.

Minimize risk and reduce exposure from email threats

Email phishing is one of the fastest growing attack vectors to harvest user credentials. Successful attacks expose your organization to data breaches through standard user account access methods. Critical Start MDR services provide email threat detection, investigation and remediation options for user submitted email phishing.

Detect and disrupt attacks during the attack chain

People prevent attacks, not tools. MDR services extend your security defenses across your domain—from endpoint, to email, to user credentials, to cloud apps. Our experts provide guidance and enable you to protect it all as every single activity is monitored to prevent a breach.

Improve security posture

Your goal is to stay ahead of advanced threats. Our Microsoft experts help you understand your environment and map a deployment strategy. With Microsoft 365 Defender and the leader in MDR, you have access to integrated threat protection that speeds up investigation and response beyond the endpoint. We continuously work with you to fine-tune your deployment as new risks are identified.

Increase productivity

We do the heavy lifting for you so your team can focus on what matters. Our team investigates escalated alerts and incidents and curates out-of-the box Microsoft detections and Indicators of Compromise (**IOCs**). Our team can respond on your behalf, and we work with your team until remediation is complete. A named Customer Success Manager (**CSM**) ensures you are receiving the tools and support for continuous security improvement.

Our Approach

Getting identity and threat protection right is a critical part of deploying Microsoft 365 Defender. At Critical Start, the experts on our Microsoft Security Consulting team help you identify risk in your environment, gain insights into your application landscape and improve your security posture.

Managed Detection and Response (**MDR**) services provide **24x7x365** cross-domain threat protection. We empower you with capabilities that go beyond the endpoint to detect user attacks against authentication sources, applications, and attempts at credential harvesting.

KEY SOLUTION FEATURES

Microsoft Workshops
Learn more about the features and benefits of the Microsoft 365 Defender suite and how to integrate its robust security controls into your environment to protect user identities.

Microsoft experts at your service
Our Microsoft-certified security staff has deep experience with Microsoft tools and uses Microsoft Security Best Practices. Team members are Microsoft Certified: Security Operations Analyst Associates.

Microsoft Outlook "Report Message" integration
Our MDR services not only detect but can also take response actions to disrupt user account attacks. An integration with Microsoft Outlook "Report Message" allows us to further support you with investigation and response for employee-submitted emails that are suspected phishing attacks.

Direct-action responses
Minutes count. While other MDR providers may only give recommended actions for the user to take, Critical Start has natively integrated our web interface and MOBILE**SOC**® mobile application with Microsoft 365 Defender APIs to create a single interface to perform manual and automated response actions. False positives are automatically resolved with our **Cyber Operations Risk & Response™ platform**. True positives are escalated to our security analysts for further investigation and response.

Reduce dwell time with triage on the go
An industry-leading first, MobileSOC, an iOS and Android application, lets you contain breaches right from your phone. It features 100% transparency, with full alert detail and a timeline of all actions taken.

What Critical Start has done with its MDR service for Microsoft 365 Defender is a game changer for my team. It's turned a 2am problem into a 9am problem. Our analysts now have the capability to disrupt and contain an attack with the click of a button as soon as the attack occurs. They then can go back to assess the scope and restore later.

-SECURITY OPERATIONS MANAGER, FINANCIAL SERVICES
MICROSOFT SENTINEL, MICROSOFT DEFENDER FOR ENDPOINT, MICROSOFT 365 DEFENDER USER

KEY USE CASES

Brute Force Attacks – Adversaries will attempt to break in via brute force attacks with weak passwords. Our platform automates the alert investigations process and elevates legitimate threats to the Critical Start Risk & Security Operations Center (**RSOC**) analyst team for follow-up. Response actions leverage manual and automated steps to stop brute force attacks, including disabling a user account, forcing a logout and expiring sessions, and enforcing password changes.

Email Phishing – Critical Start detects multiple steps in credential harvesting attacks from Microsoft Defender for Office, such as real phishing emails and malicious links. We provide course of response action to disrupt the chain and flag user accounts as potentially compromised.

Attacks Against Cloud Applications – We leverage Microsoft Entra ID and Defender for Cloud Apps to detect suspicious login behavior and identify compromised accounts.

Security Awareness Training to Defend against Phishing Attacks: Critical Start adds additional email phishing analysis in combination with Microsoft's native capabilities, further supporting security awareness training by enabling a positive feedback loop informing employees of the outcome of the reported email.

Microsoft Intelligent Security Association

Microsoft

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

CRITICALSTART®

For more information about Critical Start services and solutions for Microsoft Security, schedule a demo at:
www.criticalstart.com/contact/request-a-demo/