HUNTRESS

Huntress Managed Detection and Response for Microsoft 365

Proactive Cyber Defense for Microsoft 365

Catch Cyber Attacks and Defend Your Microsoft 365 Users

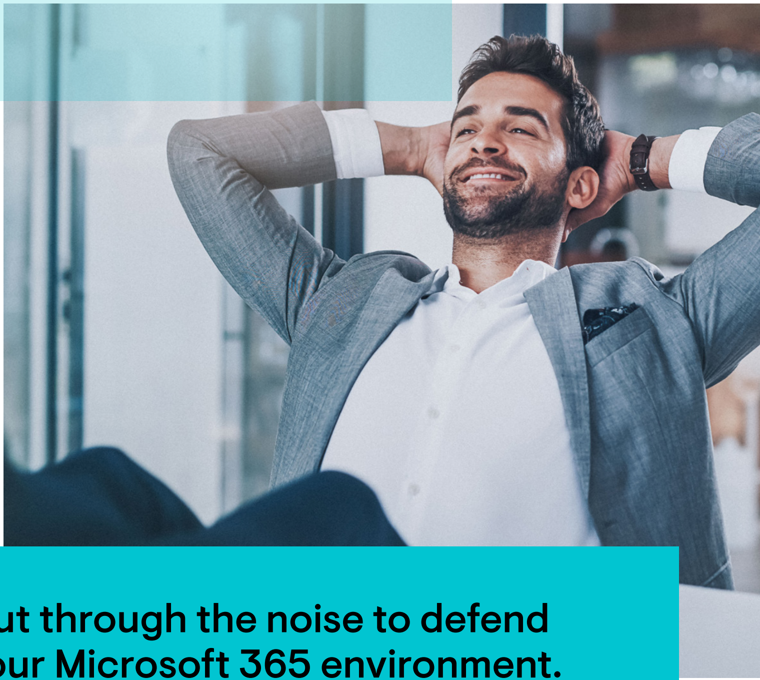
With modern cloud-based application services, a single stolen credential or compromised account can be used to launch a crippling cyber-attack. Detecting suspicious logins or activity like new mail forward configurations can identify an emerging intrusion. Use Huntress Managed Detection and Response (MDR) for Microsoft 365 to have Huntress' 24/7 Security Operations Center (SOC) detect and respond to these and other early signs of an attack to shut down hackers fast.

Give Your Microsoft 365 Environment the 24/7 Protection It Deserves

Huntress MDR for Microsoft 365 secures your Microsoft 365 users and applications by leveraging the Huntress 24/7 SOC Team to detect and respond to suspicious user activity, permission changes and anomalous access behavior. MDR for Microsoft 365 protects you 24/7 with no gaps or lags in coverage during the peak seasons, off hours or holidays.

Real-time Cyber Defense Backed by Human Experts

MDR for Microsoft 365 integrates seamlessly with AzureAD and collects and combines user, tenant and application data enriched with additional organic and external threat feeds. Together, this data is utilized by the Huntress SOC Team to detect, analyze and report on suspicious behaviors or dangerous threats and provide remediation options.



Cut through the noise to defend your Microsoft 365 environment.

DETECT THREATS FASTER

Identify threat actor behavior faster and more accurately by detecting early entry and persistence activities.

RESPOND AND REMEDIATE QUICKER

The Huntress SOC Team analyzes incidents 24/7, removing false positives and providing remediation steps.

BE MORE EFFICIENT

Huntress MDR for Microsoft 365 works quickly and efficiently so you see what truly matters; real threats and the recommended steps for remediation.

HUMAN-POWERED PEACE OF MIND

Our 24/7 human-intelligence-powered detection and response solution saves you time and money, so you can focus on your core business.

Features and Threats Detected

SUSPICIOUS LOGIN IDENTIFICATION

Threat actors accessing an account leave anomalous behavior indicators, for example, a series of sustained failed logins before success and impossible or improbable travel between logins, all valuable leading pointers to potential compromise.

SUSPICIOUS MAIL FORWARDING CONFIGURATION

Threat actors can use compromised user accounts for several malicious purposes, including reading emails in a user's inbox, forwarding emails to external recipients and sending phishing emails.

ACCESS ACTIVITY MONITORING

Threat actors will often need access to systems and services not available or unused by compromised accounts. Novel or unauthorized access to applications, files or data can be a key indicator of a compromised account.

PRIVILEGE ESCALATION AND EXPLOITATION TRIGGERS

Threat actors often need to change, add or alter the permissions for the compromised account or others. Permission changes can include high-level or sweeping privileges, additional mailbox access, creating new accounts, new groups and others.

HUNTRESS 24/7 SOC

Threats can happen at all hours, but attackers target off hours and holidays to catch their targets unaware. Huntress' 24/7 SOC Team of security experts always reviews incidents, removes false positives, investigates incidents and provides remediation directions. No more vague alerts.

ACCOUNT ISOLATION

When a threat actor compromises and accesses an account, the account must be restricted immediately. Account Isolation enables the Huntress SOC to log out of the account from all applications and devices, including disabling the account from further environment access.

MALICIOUS INBOX RULE REMOVAL

Malicious inbox rules remain a threat actor's tool of choice for data exfiltration. Malicious Inbox Rule Removal enables the Huntress SOC to remove the offending inbox rule without impacting other important business email configurations.

> **“With Huntress, we can call the end user and say, ‘someone was in your mailbox, and they're doing these suspicious actions. But don't worry, we changed your password, revoked all sessions, and required MFA re-enrollment.’ Definitely a nice show of value for us.”**

Chris Brannon
Director of Technology | L7 Solutions

Need better defense for your Microsoft 365 environment? **Huntress is how.**

Learn more about what Huntress MDR for Microsoft 365 can offer.

HUNTRESS.COM