

Managed ITDR from Huntress and Wizard Computer Services, Inc.

Identity is the New Endpoint

In today's cloud-first world, hackers no longer just "break in"—they log in. As traditional perimeters fade, your digital identities have become the primary target for sophisticated attacks that bypass standard security measures. Partnering with **Huntress Managed ITDR** (Identity Threat Detection & Response) provides a 24/7 team actively watching your Microsoft 365 and Google Workspace identities - investigating suspicious behavior and stopping BEC and account takeovers before they turn into fraud, data loss, or reputational damage.

What Is Managed ITDR (and Why It Matters)

Managed ITDR is the most effective way to secure your organization's credentials and session tokens:

- **Continuous Monitoring:** Our team of relentless identity experts monitors your Microsoft 365 and GWS environments 24/7 to identify and mitigate threats.
- **Rapid Detection & Response:** We provide swift responses to suspicious activities, such as session hijacking and malicious OAuth applications, that often bypass 2FA/MFA.
- **Human-Verified Alerts:** Every alert you receive is actionable and verified by a human expert, ensuring a low false-positive rate and very low noise.

Instead of discovering a breach days or weeks too late, Managed ITDR stops it while it's happening.

Why Businesses Rely on Managed ITDR

- **Stop Account Takeovers:** We combat credential theft and Adversary-in-the-Middle (AiTM) attacks to protect your most critical assets.
- **Combat Shadow Workflows:** We neutralize malicious inbox and forwarding rules to protect your business from pervasive business email compromise (BEC) attempts.
- **Uncover Rogue Apps:** Our team proactively detects and remediates potentially malicious OAuth applications lurking in your environment.
- **Industry-Leading Speed:** With a **3-minute mean-time-to-respond (MTTR)**, we stop hackers in their tracks before they can cause damage.

What Makes This Solution Different

- **Beyond Simple Logs:** While other tools might just flag an anomaly, Huntress identifies location-based and VPN anomalies to ensure only authorized users have access.
- **Elite Expertise:** Our solution is built to address the evolving landscape of session hijacking and credential-stealing malware—tactics that automated tools often miss.
- **Proven Results:** 98% of users say Managed ITDR has reduced their time to detect and respond to identity threats.

Who It's Built For

Managed ITDR is a vital fit for:

- **Organizations Using Microsoft 365 or GWS:** Any business relying on cloud productivity tools that needs to secure its digital identities.
- **Remote & Hybrid Workforces:** Companies that need to monitor for VPN anomalies and location-based threats.
- **Regulated Industries:** Businesses that must prevent data breaches and unauthorized access to maintain compliance.
- **Any business** that wants to lock down its identity assets and keep cybercriminals out.

Let's Keep Your Business Moving

Ask about activating **Huntress Managed ITDR** for your business today.

Contact Us

Website	www.wizardcpu.com
Email	info@wizardcpu.com
Phone Number	781-341-2222

In partnership with HUNTRESS