



Effective December 05, 2025. These Service Descriptions supersede and replace all prior versions.

## **Schedule of Services**

### **MANAGED SERVICES**

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

### **■ Unlimited Remote Support - 12x5**

#### **Unlimited Remote User / Application / Device Support**

- Live Answer US-Based Staff
- Mon-Fri 7:30am to 8:00pm Eastern

#### **Emergency Afterhours Support**

- Mon-Fri (8:00pm to 10:00pm Eastern)
- Sat-Sun (8:00am to 10:00pm Eastern)

#### **Vendor Liaison**

- Coordination and escalation with ISP
- Coordination and escalation with IT vendors (copiers, phones, etc.)

## Microsoft 365 Tenant Management

### Microsoft 365 Tenant Management

- Security Baseline And Standards
- Microsoft Entra ID
- Conditional Access Policies
- Multi-Factor Authentication Enrollment
- OneDrive / SharePoint / Teams
- Endpoint Manager / Intune
- Mobile Device/Application Management
- Defender for Office
- Defender for Endpoint
- Office Message Encryption
- Auditing, Monitoring, and Alerting
- Cloud Backup and Recovery

## Security Services

### Huntress - Managed Endpoint Detection and Response

- **24/7 Threat Operations:** Our ThreatOps team is the backbone of the Huntress platform. Through the combination of automated detection and around-the-clock threat analysts, even the most advanced threat actors won't stand a chance against your defenses.
- **Persistent Footholds:** At the core of The Huntress Managed Security Platform is our ability to identify malicious footholds. Huntress monitors for these footholds, and when found, delivers actionable recommendations and instructions for removal.
- **Ransomware Canaries:** Like the old canary in the coal mine, our Ransomware Canaries enable faster and earlier detection of potential ransomware incidents.
- **Managed Antivirus:** By providing centralized management and visibility, Managed AV enables you to reclaim and amplify existing investments in Microsoft Defender and open up more options to strengthen your security stack.
- **External Recon:** External Recon gives you visibility into external attack surfaces by monitoring for potential exposures caused by open ports connected to remote desktop services, shadow IT and more.

### Huntress - Managed Detection and Response for Microsoft 365

Huntress Managed Detection and Response (MDR) for M365 secures your Microsoft 365 users and applications by leveraging our 24/7 ThreatOps to detect and respond to suspicious user activity, permission changes, and anomalous access behavior.

MDR for M365 protects you 24/7 with no gaps or lags in coverage during the peak seasons, off hours, or holidays.

- **24/7 Threat Operations:** Threats can happen at all hours but attackers target off hours and holidays to catch their targets unaware. Huntress 24/7 ThreatOps team of security experts are always reviewing incidents, removing false positives, investigating incidents and providing remediation directions. No more vague alerts.
- **Suspicious Login Identification:** Threat actors accessing an account leave anomalous behavior indicators, for example, a series of sustained failed logins before success, which is a valuable leading pointer to potential compromise.
- **Suspicious Mail Forwarding Configuration:** Threat actors can use compromised user accounts for several malicious purposes, the main ones being the ability to forward users emails out to an external, malicious account and to Obfuscate Email.
- **Access Activity:** Threat actors will often need access to systems not available or unused by the accounts they have compromised. Novel or unauthorized access to applications, files, or data can be a key indicator of a compromised account.
- **Privilege Escalation:** Threat actors will often need to change, add or alter the permissions for the compromised account or others.
- **Account Isolation:** When an account is compromised and accessed by a threat actor, its access must be shut down immediately. Account Isolation allows ThreatOps to disable an account and log them out from all applications or devices.
- **Malicious Inbox Rule Removal:** Malicious inbox rules remain a threat actor's tool of choice for data exfiltration. Malicious Inbox Rule Removal enables ThreatOps to remove the offending inbox rule without impacting other important business email configurations.

## KnowBe4 - Security Awareness Training

- **Pre-built training Content:** With KnowBe4's pre-built training content, you're able to provide your organization with a multitude of resources and training on a variety of security awareness topics. This content is available in multiple formats including videos, interactive modules, and quizzes. It can also be customized to meet the specific needs of each organization.
- **Phishing Simulation Templates:** KnowBe4 offers a range of phishing simulation templates that mimic real-world phishing attacks. These templates can be customized to fit the specific needs of your organization. They can also include a range of different scenarios and attack types.
- **Reporting and Analytics:** KnowBe4's platform includes robust reporting and analytics tools. These tools provide organizations with detailed insights into the effectiveness of their security awareness training program. Track employee progress, identify areas where additional training is needed, and measure the overall effectiveness of the program.

**Automated Campaigns:** Access KnowBe4's automated campaigns! These campaigns enable advanced scheduling to ensure that employees receive regular training. This allows your team to stay engaged and maintain their level of security awareness so that they're always ready.

## ID Agent - Dark Web ID Monitoring

Get valuable intelligence you need to close security gaps with accurate data about your company's Dark Web credential compromise threats. Get additional protection from unpleasant surprises with credential monitoring for your supply chain and for the personal email addresses of your executive and administrative users, reducing the risk from cybercriminals gaining access to a privileged account. Dark Web ID delves into every corner of the Dark Web, including:

- Hidden chat rooms
- Unindexed sites
- Private websites
- P2P (peer-to-peer) networks
- IRC (internet relay chat) channels
- Social media platforms
- Black market sites
- 640,000+ botnets

## ■ Infrastructure Management

### **Infrastructure Security Management**

- Firewall Monitoring and Alerting
- Unified Threat Management
- VPN Management
- Switch and VLAN Management
- Guest WIFI Management
- Power and UPS Monitoring

Hardware Provided for Office Locations

- Firewall / Router
- Switches
- Wireless Access Points
- UPS Battery Backups
- Power State Monitors

### **Huntress - SIEM**

- The huntress human-led SOC has an eye on your environment and logs 24/7 to detect, investigate and hunt. Making you secure and compliant.

## ■ Implementation Services

**The specific implementation activities will be defined in the applicable Order and may include:**

- New Client Onboarding
- Microsoft 365 Security Baseline Deployment
- Microsoft 365 Core Feature Enablement
  - Entra ID
  - Intune
  - Defender for Office
  - Defender for Endpoint/Business
  - Conditional Access
  - Teams
  - OneDrive
  - Standard SharePoint Communication Site
- Migration of data, mail, or identity systems

\*\*Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.

**THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY  
TIME WITHOUT NOTICE.**