Effective October 29, 2026. 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.

Managed User (Workforce+ User)

Includes:

- IT Support, Identity and Access Management, Onboarding and Offboarding, Backup and Continuity, Strategy and Planning, and the user-level parts of Security Management
- Cloud backup of the user's email, files, calendar, and contacts
- Email security gateway with email incident response (link and attachment protection, impersonation and account compromise detection, quarantine handling)
- Security awareness training and phishing simulations
- Password and privileged access management, including dark web credential monitoring

Managed Service Account

Includes: Email security gateway and cloud backup for the account, plus the account governance in Identity and Access Management.

Managed Device

Includes:

- The Device Management component and the device-level parts of Security Management
- Remote monitoring and management or MDM, including patching and configuration
- Endpoint protection with XDR
- Automated software deployment, provisioning, and onboarding tools
- Remote access tooling for support

Managed Server (Cloud & Server Management)

Includes:

- Health and performance monitoring, maintenance, patching, and alert remediation so the server performs for its purpose
- Endpoint protection with XDR
- Backup agent, backup scheduling to the customer's defined scope, and backup health monitoring
- Directory services health monitoring, virtualization host management, and certificate renewal coordination where applicable
- Support for the server environment that hosts line-of-business applications, including assisting with application upgrades

Managed Mobile Device

Includes:

- MDM enrollment, configuration, and management for iOS and Android
- Compliance policy enforcement, remote lock, and remote wipe
- Application management and deployment
- Device inventory and lifecycle tracking

Managed Site (Location Management)

Includes:

- Initial on-site survey to onboard the location, assess existing infrastructure, and set up remote management
- Management of the network stack: firewalls, switches, and wireless access points
- Network design and segmentation, including isolation of guest, IoT, and sensitive traffic
- Intrusion prevention and threat service configuration and tuning
- Network and ISP monitoring, and first outreach to the ISP during an outage

© Scott & Scott, LLP

- Basic configuration changes (for example port VLAN assignments, simple DHCP updates)
- Routine firmware and security patching of network equipment
- Hardware failure diagnostics and manufacturer RMA coordination
- Remote access VPN, site-to-site VPN, and SD-WAN management and monitoring (initial configuration is billed separately)
- Wireless management and optimization
- Remote support for other technology at the location when it runs on our supported platforms: phone systems the customer buys directly from a voice provider we support, video surveillance and door access control systems, and audio systems and displays, that we installed or approved

ADD-ON SERVICES

Managed Access Point

Includes: Ongoing management, monitoring, and support of each access point.

Managed Conference Room

Includes: Monitoring, configuration oversight, firmware management, and remote support for conference room AV and conferencing systems, including the remote management licensing those systems need.

Location Maintenance

Includes:

- Recurring visits to each enrolled location on an agreed cadence (for example monthly or quarterly), or an agreed number of visits per month
- Physical inspection of network equipment, racks, and network closets
- Cable management and labeling cleanup within existing infrastructure
- Minor fixes during the visit (reseating cables, power cycling, small configuration changes)
- Help with small open issues from remote support that can be handled during the visit
- Conference room AV and peripheral checks
- A location health report after each visit with findings and recommended follow-ups
- Coordination with building management, landlords, and ISPs for access and vendor visits

24/7 Managed Detection and Response (MDR)

Includes:

© Scott & Scott, LLP

- 24/7/365 monitoring of enrolled endpoints
- Alert triage and investigation covering scope, impact, and technique
- Active response: threats are contained and removed, not just reported
- Root cause analysis and incident case reporting
- Endpoint telemetry, with optional integration of network, cloud, identity, email, and business application sources
- Coordination with Lerner for follow-up, ticketing, and user communication
- Detection tuning and enrollment changes as devices are added or retired

Tenant Protection (Franchisee Security Add-On)

Includes:

- **Email security gateway:** API-connected layer on top of native Google Workspace or Microsoft 365 filtering that scans inbound, outbound, and internal mail for phishing, business email compromise, impersonation, and malicious links and attachments. Policy configuration and tuning, time-of-click link protection, attachment sandboxing, account compromise alerts, and quarantine release through the support desk.
- **Email and productivity backup:** backup of mail, files, shared drives, calendars, and contacts in Google Workspace or Microsoft 365 beyond native retention, kept per the plan's retention. Restores on request, scoped to an email, file, folder, user, or point in time. Monitoring for failed or skipped jobs.
- **Security awareness training and phishing:** enrollment synced to the directory, recurring short courses, scheduled phishing simulations with click and report tracking, automatic follow-up training for users who click, and human risk reporting reviewed at account check-ins.

Vulnerability Management

Includes: Two separate services. Endpoint: an agent on each enrolled computer collects vulnerability data. Facility: a probe installed on the network at a location scans the traffic and devices on that network. Both include ongoing scanning, findings reporting, and remediation guidance.

Security Program Advisory

May include: Security risk assessments, security policy development beyond standard Workforce+ policies, Zero Trust Network Access deployment and management, secure remote and contractor access, scoped and time-limited third-party access controls, device posture checks for remote and contractor endpoints, and privileged remote access controls and monitoring.

Advanced Compliance

May include: Readiness assessment and gap analysis, control mapping and documentation, help gathering evidence for audit preparation, ongoing compliance monitoring and control

© Scott & Scott, LLP

maintenance, framework-specific policy development, support for the customer's team in developing extended policies (change management, vendor risk, data retention, encryption standards), and coordination with the customer's auditors.

Endpoint Backup

Includes: Backup agent installation, scheduling, and backup health monitoring.

Additional Backup Accounts

Definition: Backup and email protection for mailboxes kept in the tenant that are neither Managed Users nor Managed Service Accounts, most commonly former employees whose mailboxes the customer wants to retain. Because protection is applied to the whole domain, these accounts carry cost until the customer removes them. This is a legacy add-on a few customers are still billed for. Going forward, retained accounts are billed as Managed Users or Managed Service Accounts until deleted.

Block Hours (Remote Managed Services)

**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.

© Scott & Scott, LLP