SecureShield365

TERMS OF SERVICE

SERVICES AGREEMENT TERMS AS OF JANUARY 17, 2022

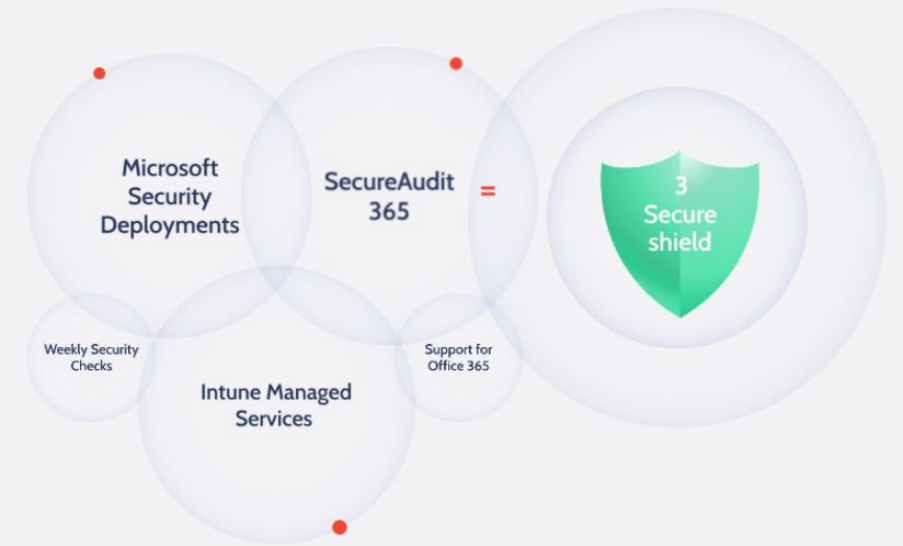
NOTE: THIS TERMS OF SERVICE INCLUDES ALL POSSIBLE CONFIGURATION OPTIONS – SEE EXECUTED PRICING SHEET FOR ACTUAL SELECTIONS IN SCOPE.

CONFIDENTIAL
PATRIOT CONSULTING TECHNOLOGY GROUP, LLC
17192 Murphy Avenue, #14067, Irvine, CA 92623
Direct: 1-844-560-4630 I PatriotConsultingTech.com

Table of Contents

Introducing SecureShield365 by Patriot Consulting

SecureShield365 is managed service for Microsoft 365 customers. Imagine hiring an employee who has deployed Microsoft 365 over 300 times. That would be an expensive expert right? SecureShield365 provides this experience for half the cost of a full-time employee.



- **Intune Deployment Services (Platinum Tier),** is a full deployment of Microsoft Intune to the following platforms: Windows 10 or later, iOS/iPadOS, MAC OS, and Android.
  Patriot will deploy a baseline Intune implementation including security guidance for Windows 10, Apple iOS/iPad OS, MAC OS, and Android devices. This includes Compliance, Configuration, and Azure AD Conditional Access Policies.
- **SecureAudit 365**, a managed audit and configuration service to discover and harden configuration in Microsoft 365.
  This service includes 6 hours remediation assistance per quarter to implement our security recommendations while offering insight these changes may have on end-user productivity. In addition, you will receive a monthly update of significant configuration changes that could impact end-user security or productivity.
- **Quarterly Security Health Checks,** performed by a Microsoft Certified Security Expert. Patriot will provide a deliverable each quarter containing any incidents that require attention or action. See Appendix C for more information.
- **Level 3 Support for Microsoft 365 Defender and Intune,** delivered by Microsoft Office 365 Certified Experts. Patriot will provide a helpdesk ticketing solution to track requests to completion. Intune and M365 support are shared hours in the Level 3 support for M365 line item in the pricing sheet.
  See Appendix A and B for more information on in scope supported services.
- **Microsoft 365 Deployment as a Service. (Optional Add-on, See Pricing Sheet if selected)**
  Patriot will deploy M365 Defender services at any time clients decides and is licensed for it. This includes Microsoft Defender for Office, Defender for Endpoint, Defender for Identity, and Microsoft Defender for Cloud Apps, or a custom plan (if specified in the Deployment Section).

Intune Managed Services

The key to a successful Intune design and deployment is to define the intended use and required features of the solution clearly. Gathering the business and technical requirements of the solution and applying Patriot' Intune Managed Services design standards, Client has identified the following business goals as part of this project:

- Utilize Patriot to design, plan and deploy Microsoft Intune Managed Services to increase operational efficiency and protect corporate data
- Stay current with the Intune service with a trusted Microsoft Partner

Intune Service Catalog

The Patriot Intune Service provides baseline configuration for features by platform and general:

See Appendix "A" Service Catalog and Appendix "B" Microsoft 365 Support Catalog

Intune Technical Objectives

Patriot has identified the following as technical objectives and makes assumptions for this Service Agreement (SA):

- Optimize or Support Intune configuration, compliance, application offerings and conditional access baselines for client supported platforms (Windows 10, iOS/iPadOS, Mac OS, Android) (For Gold and Platinum Plans) (See Appendix "A" Intune Support Catalog)

- Implement Intune configuration, compliance, application offerings and conditional access baselines for client supported platforms (Windows 10, iOS/iPadOS, Mac OS, Android) (See Appendix "D" Intune Deployment Scope (Platinum Plan)

Intune Detailed On-Boarding Scope

Patriot will be responsible for the following tasks associated with this project (for Gold and Platinum Plans)

On-Boarding Management

- Facilitate Kickoff Meeting and Status Meetings
- Conduct Issues and Risk Management
- Provide Agenda and Meeting Notes
- Track Client and Patriot Deliverables
- Schedule Patriot engineering and support resources via ticket management system
- See Appendix D for Deployment Scope (For Platinum Service Plans)
- Create a SharePoint Team Collaboration site that will contain:
    - Real Time Document Repository
    - Real Time Active Project Schedule
    - Real Time Active Meeting Notes and Status Updates
    - Deliverables

Intune Support

- Intune Professional Services for the supported configurations (see Pricing table for number of hours)
    - Hours can be used to configure and test new configurations/policies
    - General support for supported device & related security configurations
    - Change Request log for all updates
    - Tier 1 and 2 support is excluded from this Service Agreement
        - Client helpdesk will make effort and escalate, as needed, to an internal subject matter expert who will act at the point of contact for Patriot. If this person is unable to resolve the issue, then the point of contact can escalate to Patriot (Tier 3). The engineer that responds from Patriot will be a Tier 3 skilled engineer.
    - Tier 3 Support (next business day SLA). All Tier 3 support requests should be submitted in the Patriot provided ticketing system. Upon the executed agreement, the ticketing system will be introduced to the client and access will be granted.
    - Intune configurations or features that require additional planning, design, and testing will require a Change Request
        - These will require a high level of involvement of client technical staff and are client defined milestones/deadlines.
        - Patriot will be responsible for informing Client of this prior to completing any related work.

        - A change request and cost of effort would be developed and presented to the client for agreement.
        - A Patriot Project Management Resource and Architect will be assigned to that scope of work with an agreed change request.
    - Professional Services cannot be used for production rollouts in this agreement, unless purchased as part of the Platinum or an Add-On Package.
        - Professional Services will provide guidance and support for tested features, configuration, and policies
- Quarterly Roadmap Updates
    - New features/Settings
    - As Built documentation can be provided quarterly upon written request

Intune Assumptions

The following assumptions were made in the creation of this Service Agreement. Should any of these assumptions prove to be incorrect, Patriot reserves the right to modify the scope or schedule of work as defined in this Service Agreement.

- Client will provide Patriot administrative access to the existing Intune tenant to provide support and perform the deployment, as required
- Anything not specifically listed in the Scope section is considered out of scope.
- Client will be responsible for Intune Enrollment beyond the Pilot Group (limited to 10 endpoints of each supported platform)
- Client will provide Patriot with authorization to contact application vendor directly when Patriot is tasked with doing application deployment.
- The requirements, design goals, and other information provided by the Client to Patriot is accurate and complete and forms the foundation upon which this SA is based.
- The SA start and completion dates are to be determined upon receipt of Purchase Order and signed acceptance of this SA.
- Work will be done independently but in close coordination and communication with the Client. Unless otherwise agreed upon in writing, work will not be done via shared screen sessions such as Teams, as it will materially impact the level of effort quoted.
- This Service Agreement assumes that the existing environment meets all Intune prerequisites. Any work required to meet these defined prerequisites is not included in this Service Agreement.
- The Intune service agreement will only cover supported operating systems and browsers
- The client's network environment is capable of meeting the Intune network configuration requirements
- Unless specified otherwise in this Service Agreement or agreed to in writing by the parties, services shall be performed during Normal Business Hours. Client may be responsible for any additional labor costs associated with Services performed outside Normal Business Hours, which are above and beyond the scope of this Service Agreement
- Should issues occur that cannot be resolved by Patriot with due care and diligence, a support ticket may need to be opened with Microsoft. Patriot will open and work the ticket using the customer's existing support contract with Microsoft. If no support contract exists, then Patriot will open a support case using Patriot's Partner agreement with Microsoft.
- Patriot will be provided timely access to various resources necessary to complete the project including documentation, systems, accounts, applications, code, personnel, and other artifacts that are directly related to the Service Agreement.
- Microsoft Azure, Intune and Office 365 are Microsoft services and Client will secure all subscriptions with Microsoft. Patriot is providing consulting services and this Agreement does not cover the cost of subscriptions or any other software licensing unless expressly defined in the project cost.

- General uptime, availability and guaranteed functionality for these services is controlled by Microsoft and Patriot cannot be held responsible for any service outages or impaired functionality experienced by the Client on the Microsoft hosted platform.
- The project scope does not include efforts to remediate GPOs that may conflict with Intune policies.
- The Testing & Validation phases will be capped at 30 days per phase to ensure that the on-boarding can be completed in a timely manner. The Client will have up to 30 days per phase to pilot the solution, request support and report errors or issues for remediation. The time period for resolution of errors or issues may extend beyond the 30-day window Patriot will provide assistance until those errors are resolved within the confines of what Microsoft and the Intune product will support; however, the Client will perform all required testing and report all errors or issues within that 30-day window.
- The cancellation of 2 or more scheduled working sessions, by the client, with less than 24-hour notice, will result in a $500 cancellation fee per occurrence beginning with the 3rd cancellation
- All meetings will be remote and scheduled in advance. This consulting engagement does not include on-call or emergency support services
- Client has an existing Microsoft 365 Tenant with Domain Names registered in tenant
- End-user training and communications are not included in this Service Agreement
- Troubleshooting pre-existing issues relating to underlying systems such as networking, hardware, and storage are not included in scope
- Patriot will not be held responsible or liable for security breaches that occur. This includes, but is not limited to, application vulnerabilities, malicious activity, or attacks on client network.
- Devices participating in the pilot will need to enroll with Intune
- Remote wipe will only be used on test devices with no data, user devices will not be tested for remote wipe. Patriot is not responsible for lost data due to remote wipe functionally being tested on pilot devices
- Intune automatic enrollment requires an Active Directory premium subscription
- The SA scope does not include efforts to create new packages to remove pre-existing software from devices
- Client will assign Patriot Consulting Technology Group LLC as Claiming Partner of Record for a period of one year for the workload(s) covered in this statement of work

SecureAudit 365

More than 225 million people are now using the Microsoft 365 platform, making it an attractive target for cyber criminals. A single compromise can result in cyber criminals gaining access to your organization's most critical data. In some cases, we have seen ransomware lead to disruptive work stoppages, costing over $1 million per day in lost revenue.

Through years of research, Patriot has painstakingly assembled an inventory of over 850 configuration settings in Microsoft 365, along with the impact caused when changing these settings. Most customers are unaware that the default settings are weak and put them at risk of cyber-attack. Microsoft's own Secure Score service measures only 100 of the possible 850+ settings, and records that the global average score is just 37.

Some of our most diligent customers have attempted to harden the tenants on their own, but even their best attempts of using Secure Score will only result in 100 of the 850+ settings being analyzed, and they are also unaware of the potential negative impact any one of the settings may have on end-user experience.

What is Secure Audit 365?

To help Company Name harden its Microsoft 365 configuration against cyber-attack, Patriot Consulting Technology Group ("Patriot") offers ***SecureAudit 365***, a managed audit and configuration service to discover and harden configuration in Microsoft 365. This service includes configuration assistance to implement our security recommendations while offering insight these changes may have on end-user productivity. In addition, you will receive a monthly update of significant configuration changes that could impact end-user security or productivity.

How does it work?

Your Microsoft 365 settings will be compared against our exclusive database of recommended settings, with a custom implementation plan to achieve optimal results. We will schedule a configuration review with your internal teams where we educate them on the possible impact to end-user productivity. Finally, we schedule a maintenance window for our team to work alongside your team to implement the recommendations in a friendly knowledge sharing session through screen sharing.

What if my configuration changes?

Change happens. Your own internal administrators may make authorized or unauthorized changes over time. Microsoft adds 120 new settings on average every year. Because any of these configuration changes could impact user productivity or weaken security posture, Patriot will audit once per quarter and provide an updated governance document of any new or changed settings. And since you will receive a monthly report of any significant change, saving you an estimated 8 to 12 hours of research every month.

PATRIOT CONSULTING

SA365 Scope of Work

Within the Microsoft 365 tenant and depending on your license there are over 850 settings that can affect Company Name's security posture. As part of the SecureAudit 365 service Patriot captures and documents all the settings that are relevant within your M365 tenant for all features available to your end users. This Governance document will include detailed recommendations to improve your Microsoft 365 tenant's security posture.

This engagement provides Company Name with insight and recommendation for their Microsoft 365 tenant and settings, including:

- An Executive Summary of key findings and recommendations
- A Governance Document providing a single trusted source of M365 settings.
  This is a Microsoft Excel document with the default value of every setting in Microsoft 365 compared to your current setting, and Patriot's recommendation for each setting.
- Following the presentation of the Executive Summary, Patriot will provide up to 6 hours per quarter of configuration assistance to implement the recommendations.
- Each Client is entitled to one Microsoft 365 Incident Response for up to 1 account per year as part of this contract. Please note Appendix A for details and limitations.

SA365 Monthly Feature & Security Update

-

On average Microsoft makes 75 to 125 announcements every month, and 120 new settings are added to Office 365 every year. Patriot provides a monthly report including our analysis of major announcements and changes. This is designed to help you avoid disruptive changes and help you take advantage of new features or settings that may improve user experience.

Patriot offers an interactive webinar to explain the changes and updates announced by Microsoft. Attendees can submit questions to tap into Patriot's expertise. Notifications will continue for the Service Duration outlined in the pricing section.

SA365 Quarterly Audit Update

Each quarter (every 90 days) Patriot will update the initial Audit Report to include any new settings that Patriot has found added to your tenant by Microsoft. Annually, Patriot will perform a full Audit of all settings, both new and existing.

SA365 Deliverables

Deliverable Name	Description
Executive Summary of Key Findings & Recommendations	A detailed report of recommendations designed to improve the security of Company Name's Microsoft 365 tenant, users and data
Governance/Settings Matrix	A matrix detailing all the relevant settings within Company Name's Microsoft 365 tenant comparing default, current, and recommended settings (relevant settings are based on the M365 license(s) owned)
Configuration Assistance	Each quarter Patriot will provide up to 6 hours per quarter of configuration assistance, guidance or coaching related to the findings and recommendations report or the monthly Cloud Advisory report for the life of this contract.
Monthly feature & security updates	A "Cloud Advisory Report" summarizing new security and productivity features in Microsoft 365 each month and our recommendation on how to take advantage of them.
Quarterly Audit Update	Each quarter (every 90 days) Patriot will update the initial Audit Report to include any new settings that Patriot has found added to your tenant by Microsoft. Annually, Patriot will perform a full Audit of all settings, both new and existing.
Incident Response	Each Client is entitled to one Microsoft 365 Incident Response for up to 1 account per year as part of this contract. ***Please note Appendix E for details and limitations.***

SA365 Assumptions

This proposal assumes the following:

- This governance and hardening audit is limited to Microsoft 365 tenant settings and excludes Windows 10 Desktop security settings and on-premises Advanced Threat Analytics settings.
- Governance meeting is a remote meeting initiated and scheduled by Patriot and Client.
- Monthly feature & security updates report is a report emailed to Client on a monthly basis. Client to provide a list of individuals who will receive the report. Patriot will review the report via a live (and recorded) video stream.
- Patriot does not guarantee that its services will prevent security breaches. Patriot is not responsible for breaches that occur through no fault of Patriot, including, but not limited to, inherent application vulnerabilities, malicious activity, or attacks on the Client's network. Patriot shall only be responsible and liable for security breaches that occur as a result of Patriot's gross negligence or willful misconduct.
- Client will assign Patriot Consulting with Global Administrative rights in the Microsoft 365 tenant to collect all the required information for the duration of the Audit phase of this agreement. Patriot recommends the use of Azure AD Privileged Identity Management (PIM) so the account can be elevated to privileged while the audit is taking place and reduced to non-privileged after the audit is complete. Patriot can configure PIM at no additional cost for Client. Additionally, if Client does not own PIM licensing Patriot will offer to credit this contract up to $84 to offset cost of an Azure AD Premium P2 license.
- Configuration or remediation services are limited to the recommendations in the Governance and Hardening document or the monthly Cloud Advisory Report. This proposal is not intended to deploy new services or capabilities.
- All resources provided for this statement of work are subject to availability. In the event that there are project delays caused by the Client, consisting of a total of 1 or more weeks, and the resources are no longer available, Patriot can provide resources with equivalent skills.
- The cancellation of 2 or more scheduled working sessions, by the Client, with less than 24-hour notice, will result in a $500 cancellation fee per occurrence beginning with the 3rd cancellation.
- The 6 hours of configuration assistance for guidance or coaching related to the findings and recommendations or monthly Cloud Advisory report are optional and must be used during the quarter in which they are issued. The hours do not roll-over each quarter. Unused hours are non-refundable.
- Client will assign Patriot Consulting Technology Group LLC as Claiming Partner of Record for a period of no less than one year for the workloads covered in this statement of work.
- The Service Agreement (SA) will require a high degree of involvement with Client IT staff. The success of the Service will require a substantial commitment in time and focus to execute the SA in a timely and satisfactory manner. The specific details will be delivered at the end of the Design & Planning phase by Patriot. It is Patriot's goal to provide a well-planned but flexible approach where new information, ideas and requirements can be incorporated into the solution, as needed by providing on going Professional Services under agreed terms.
- Client will be responsible for required network changes and providing adequate resources that meet the requirements of the Service Agreement. Client will need to perform timely and diligent application validation and testing to ensure that the Service features can be completed within the time frame and budget estimated herein. Client acknowledges that general uptime, availability, and guaranteed functionality for Microsoft hosted platform is controlled by Microsoft, and Patriot

cannot be held responsible for any service outages or impaired functionality experienced by the platform.

- Patriot will be responsible for all Intune work outlined and included in this Service Agreement. The Service Onboarding period is expected to take 2 to 3 weeks depending on Client availability and scheduling for validation and planned enrollments with end users. Anything not specifically listed in the onboarding tasks list is considered out of scope and shall require a Change Request to this SA or a new Project SOW will be executed between the parties.
- Patriot's services do not guarantee any outcome or result. Further, Patriot's services are based on the information provided to Patriot by Client and the information available at the time that the services are performed. Patriot is not responsible for any omissions, inaccuracies, or other issues with the services that are the result of changes in the information provided by or from Microsoft or any other third parties, or any other relevant information.
- Deliverables created from this project will be deleted from Patriot's systems 180 days following project termination. Legal agreements will be retained for 3 years and then deleted from Patriot's systems.

Microsoft 365 Defender Deployment Services

Patriot will deploy the following Microsoft 365 Defender services:

- **Microsoft Defender for Identity**

Defender for Identity (DFI) is an Intrusion Detection Solution (IDS) for on-premises Active Directory. It uses both behavioral-based IDS combined with signature-based IDS to detect breaches that have already occurred or are in progress. Many of these threats are exclusively detected by DFI that no other security product can detect because of how Active Directory traffic is encrypted by domain controllers. This product requires very little footprint, no server infrastructure as everything is hosted in Azure.
To learn more click (here)

- Patriot to provide guidance on how to run the Capacity Planning tool for DFI
- Client to run the Capacity Planning tool (Tool runs for 24 hours minimum)
- Patriot to show DFI features and configuration options
- Patriot to assist with capacity planning report to verify domain controller meets minimum system requirements
- Client to ensure the domain controllers meet minimum size requirements and pre-requisites
- Patriot to assist client with deploying the DFI agent to 1 domain controller
- Client to deploy the DFI agent to all remaining domain controllers
- Patriot to provide guidance on performing a test DNS Zone Transfer against on-premises domain controllers to verify that alert is registered in DFI

- **Microsoft Defender for Cloud Apps**

"Microsoft Defender for Cloud Apps is the swiss-army knife of cloud security. It is like a firewall for SaaS applications. There are over 20 use cases that this product solves. To learn more click (here)"

  - Patriot to show available Microsoft Defender for Cloud Apps configuration options and discuss client custom use cases
  - Patriot to assist client with configuring Defender for Cloud Apps
  - Patriot to assist client with testing to confirm that policies are configured and working properly
  - Patriot to assist client with updating policies to block when suspicious activity is found (assuming client change management approves this change).

- **Microsoft Defender for Endpoint**

Microsoft Defender for Endpoint is the #1 Top Endpoint Detection and Response solution that includes dozens of additional capabilities such as 3rd party software vulnerability assessment correlating to the Common Vulnerability Exposure (CVE) database. To learn more click (here)

  - Patriot to assist with configuring Microsoft Defender for Endpoint Portal options
  - If client is using Intune to manage their Windows 10 PCs, Patriot will assist client with configuring Intune to deploy the MDFE agent and then assigning to a test group in Intune.
  - Patriot to assist client with deploying the MDFE agent to all computers via Intune (If Intune is used for Windows PC management).
  - Patriot to assist client with deploying MDFE to Servers (Patriot will use the train the trainer method where we demonstrate the method and client's Level 2 Administrators will complete deployment under Patriot supervision).

- **Microsoft Defender for Office 365**

Defender for Office 365 includes sandbox detonation of email attachments, and hyperlink redirection to inspect for phishing emails. Also protects against malware and phishing links in Office on the Web, SharePoint Online, Teams, and OneDrive for Business. To learn more click (here)

  - Patriot to have consulting conversations around and plan for enabling Microsoft Defender for Office 365 features, including Safe Links, Safe Attachments and Anti-Phishing policies.
  - Patriot to assist client with configuring policies based on planning meeting and assign to test users
  - Client testing:
    - Send a test link and attachment to see if Safe Links and Safe Attachments are configured as desired
  - Client to communicate to end-users expected changes prior to global policy assignment
  - Patriot to assist client with assigning policies globally

Appendix "A" Intune Support Catalog

Windows 10 Service Catalog

Intune Feature/Description	Details	Supported
Join Type	Azure AD Joined	X
Intune Enrollment	Autopilot: Admin-Based	X
Intune Enrollment	Autopilot: User-Driven	X
Intune Enrollment	Autopilot: Whiteglove / pre-provisioning	X
Intune Enrollment	Manual Enrollment: Company Portal	X
Intune Enrollment	Registered: Azure Creds/BYOD	X
Configuration Profile	Device Configuration Profile	X
Compliance Policy	Device Compliance Policy	X
Conditional Access Policy	Device Conditional Access Policy	X
Application	MSI	X
Application	Win 32	X
Application	Built-In	X
Application	Microsoft Store for Business	X
WUfB Pilot	Pilot	X
WUfB Production	Production	X
Windows Hello for Business	Authentication/Identity (Cloud Only)	X
Default Dynamic Security Groups	Standardized Dynamic Security Groups	X
Group Policies Analytics	Analyzes on premises GPO to determine if it is supported in the cloud tenant	X
Endpoint Analytics	Device Analytics captured	X

Apple iOS/iPadOS

Intune Feature/Description	Details	Supported
Join Type	Registered	X
Intune Enrollment	Org-owned ABM/ADE	X
Intune Enrollment	Manual Enrollment	X
Configuration Profile	Device Configuration Profile	X
Compliance Policy 1	Device Compliance Policy	X
Conditional Access Policy	Device Conditional Access Policy	X
Application 1	VPP Tokens	X
Application 2	iOS Store Apps	X
Application 3	Built-in	X
Default Dynamic Security Groups	Standardized Dynamic Security Groups	X
App Protection Policy	Personally Owned Devices	X
App Protection Policy	Corporate Owned Devices	X

MAC OS

Intune Feature/Description	Details	Supported
Join Type	Registered	X
Intune Enrollment	Org-owned ABM/ADE	X
Intune Enrollment	Manual Enrollment	X
Intune Enrollment	Registered	X
Configuration Profile	Device Configuration Profile	X
Compliance	Device Compliance Policy	X
Conditional Access	Conditional Access Policy	X
Application 1	MS 365 Apps for the enterprise	X
Application 2	Line of Business Application	X
Default Dynamic Security Groups	Standardized Dynamic Security Groups	X
App Protection Policy BYOD	Personally Owned Devices	X
App Protection Policy MDM	Corporate Owned Devices	X

Android

Intune Feature/Description	Details	Supported
Join Type	Registered	X
Intune Enrollment	Enterprise for Work Profile	X
Intune Enrollment	Enterprise (Corp owned) with Work Profile	X
Intune Enrollment	Enterprise (fully managed)	X
Configuration Profile:	Device Configuration Profile	X
Compliance Policy	Device Compliance Policy	X
Conditional Access	Device Conditional Access Policy	X
Application 1	Android Store Apps	X
Application 2	Android System Apps	X
Application 3	Android Built-in apps	X
Application 4	Line of Business Application	X
Default Dynamic Security Groups	Standardized Dynamic Security Groups	X
App Protection Policy BYOD	Personally Owned Devices	X
App Protection Policy MDM	Corporate Owned Devices	X

Appendix "B" Microsoft 365 Support Catalog

Defender for Endpoint Service Catalog
- Onboarding new clients using existing Intune (Installing Defender for Endpoint on iOS, Android, macOS or Windows 10/11)
- Quarterly Security Health Check (see Appendix C)

MCAS Service Catalog
- Custom Session Control for SaaS Apps
- Custom Alerts and Policies
- Tuning Alerts
- Quarterly Security Health Check (see Appendix C)

Microsoft Defender for Identity Service Catalog
- Onboarding (Installing Lightweight Agent on Domain Controllers)
- Quarterly Security Health Check (see Appendix C)

Microsoft Defender for Office 365
- Quarterly Security Health Check (see Appendix C)

Appendix "C" Quarterly Security Health Checks

Quarterly Security Health Check Tasks

- Review Microsoft 365 Incidents at Security.microsoft.com for Actionable Response
- Check Automated Investigations for Pending Actions
- Review User Reported Phishing Submissions
- Review Spoofed Users and take action as required
- Review Spoofed Domains and Impersonated Domains and take action as required
- Review Office 365 Alerts
- Review Security and Compliance Reporting
- Review Microsoft Security Center Reports including User Risk, Active Incidents, Security Score
- Review Message Center Updates for Action
- A deliverable will be sent to client quarterly containing a summary of findings and recommendations

Appendix "D" Intune Deployment Scope (Platinum Plan)

Patriot will be responsible for the following tasks associated with this project:

Intune Project Management

- Facilitate Kickoff Meeting and Status Meetings
- Conduct Issues and Risk Management
- Provide Agenda and Meeting Notes
- Document Project Plan
- Track Client and Patriot Project Deliverables
- Schedule Design meetings and facilitate architecture review and acceptance
- Schedule Patriot engineering and support resources
- Create a SharePoint Team Collaboration site that will contain:
    - Real Time Document Repository
    - Real Time Active Project Schedule
    - Real Time Active Meeting Notes and Status Updates
    - Project Deliverables

Phase 1 –Planning/Build (Estimated 4 to 5 weeks)

- Prerequisites
    - Access to Client environment, including the following administrative roles to Intune and Azure tenant
        - Intune Admin
        - Security Admin
        - Global Reader
    - Availability of all required stakeholders and IT personnel
    - Intune subscription procured
    - Azure AD Premium subscription procured
- Patriot to host design & planning meetings with client to complete discovery. Patriot will then complete the build for testing each platform that meets the stated objectives.
    - Discover/Review Identity Provider
    - Discover/Review MDT/Config Mgr. Infrastructure (envisioning/guidance only)
    - Discover/Review AAD Connect
    - Identify security, and password requirements
    - Discover/Review Certificate requirements
    - Identify application deployment requirements (up to 3 apps)
    - Identify Wi-Fi policy requirements
        - Assistance for Basic Wi-Fi is supported
        - Guidance for Enterprise Wi-Fi is supported
            - Assistance for this scope requires a change request
    - Identify compliance requirements
    - Identify conditional access scenarios
    - Identify client provided devices for testing

- Identify settings for Windows 10 automatic enrollment
- Identify/Review VPN requirements
- Identify Windows Update for Business requirements
- Identify Windows Hello for Business requirements (Azure AD Only)
- **Build** (Scoped to Client provided non-production endpoints and users for validation and testing)

    - Windows 10
        - Create/Validate MDM Authority
        - Create security groups for testing
        - Assign license (if needed)
        - Create Device Compliance policies (up to 2)
        - Create Device Configuration profiles (up to 3)
        - Create applications deployments / offerings (up to 3)
        - Configure Hybrid Azure AD Join
        - Configure Autopilot Profiles (up to 2)
        - Create Conditional Access policies referencing Compliance (up to 2)
        - Configure Windows Update for Business Policy (up to 2)
        - Configure Windows Hello for Business (Azure Ad Joined Only)
    - iOS/iPadOS
        - Create/Validate Apple Push Notification Cert
        - Provide guidance for Apple Business Manager (ABM) Integration
        - Provide guidance for Location token (VPP) integration
        - Create/Validate ABM enrollment profiles (up to 2)
        - Create Application Protection Policy (up to 2)
        - Create Device Compliance policies (up to 2)
        - Create Device Configuration profiles (up to 2)
    - Android
        - Configure Google for Enterprise
        - Create Application Protection Policy (up to 2)
        - Create Device Compliance policies (up to 2)
        - Create Device Configuration profiles (up to 2)
    - Misc.
        - Brand tenant (Azure AD tenant and Office 365 Company Portal)
        - Enrollment restrictions (up to 2)
        - Provide guidance on application offerings/publishing in the Company Portal App

Phase 2 – Stabilize (Validation/Testing) (Estimated 4 to 5 weeks)

- Patriot and Client will complete validation and testing of the Intune configurations prior to the production deployment on up to 5 non-production pilot devices, per platform
  - Test Azure and Hybrid Azure AD join
  - Test platform enrollments
  - Test Autopilot profiles for Azure AD joined devices
  - Test Autopilot profiles for Hybrid Azure AD Joined devices
  - Test Compliance, Configurations, Resource, and Applications deployments/offerings
  - Test wipe/reset scenarios for in scope platforms
  - Test Intune App Protection policies (iOS/iPadOS and Android)
    - Test Application Protection Policy Selective Wipe
- Deliverables
  - Intune Design, Planning, and deployment document

Phase 3 – Deploy (4 to 5 weeks)

- Patriot and Client will complete deployment of the Intune configurations on up to 5 production users and devices, per platform
- A controlled deployment can be used in the production deployment. Patriot recommends that Azure AD Join, Hybrid Azure AD Join and Intune Windows automatic enrollment be excluded from the controlled validation. These actions are transparent to the endpoint and user objects and will not impact production.
- Deliverables
  - Intune "As-Built" document
    - This deliverable will be considered accepted if no objections are received within 5 business days. If objections are received, then the deliverable will be considered complete within 5 days after Patriot submits the document containing the corrections.

Success Criteria

The Intune Deployment will end, and the Intune Support will begin, when Phase 3 has completed.

Appendix "E" Incident Response

In order to qualify for this service Client must have Microsoft's Always-On Multi-Factor Authentication (MFA) turned on for **all** employees within their organization. If Microsoft MFA is not turned on for all employees Client is not entitled to this service as part of this Agreement. Client may choose to purchase Incident Response services from Patriot under a separate agreement.

Incident Response (IR) will attempt to answer the following questions:

- Based on available audit logs obtained, when did the attacker gain access to the account
- What was the attacker's origin IP addresses and what location and country is this associated with
- What actions did the attacker take
- Based on these actions, Patriot's opinion of the attacker's motivation
- A review of the response that the IT Department has taken with recommendations for improvement
- Confirmation whether the attacker's activity has ceased

IR Deliverables

The output of the Incident Response engagement will include a detailed account of the findings and recommendations of the incident in Microsoft Word format, along with an export of all audit logs obtained.

- Screen Shot of Initial Phishing Email (if applicable)
- Security and Compliance Center Log Analysis Findings
- Azure Sign-In Log Analysis Findings
- Additional Security Product Log Analysis (ATP URL Trace, MCAS, WDATP, Azure ATP, when licensed)
- Inbox Rule forwarding and SMTP Forwarding Discovery
- Mailbox Audit Log Search Analysis Findings
- Mailbox Audit Log Session ID Correlation
- Attacker Known IP addresses
- Correlation of Attacker IP addresses with other user account sign-in activity
- Attacker Known ClientInfoString
- Correlation of ClientInfoStringwith other user account sign-in activity
- Attacker First Known Logon Date
- Attacker Last Known Logon Date
- Screen Shot of Message Tracking Logs
- What emails were sent from the victim's mailbox during the time the attacker had access to the mailbox? Do any of these look suspicious?
- What emails were sent to the victim's mailbox just before the attacker's first successful logon? Do any indicate perhaps how the attacker gained access? (credential phishing emails)?
- Attacker's Entry Point (Do we know how the attacker gained access?)
- Is the Victim's identity found on the dark web?
- Attacker's activity Timeline (Based on the audit logs, what was the attacker's timeline?)
- Last Known Password Change Date (When was the victims' password last changed?

Client Responsibilities for Incident Response

- Client or its designated partners shall perform the following:
- Client will create a Global Administrator Account in their Microsoft 365 Tenant.
- Client should communicate any known symptoms that led to believe an account was compromised
- Client should communicate any remediation activities performed on the account being investigated

Incident Response Assumptions

This proposal assumes the following:

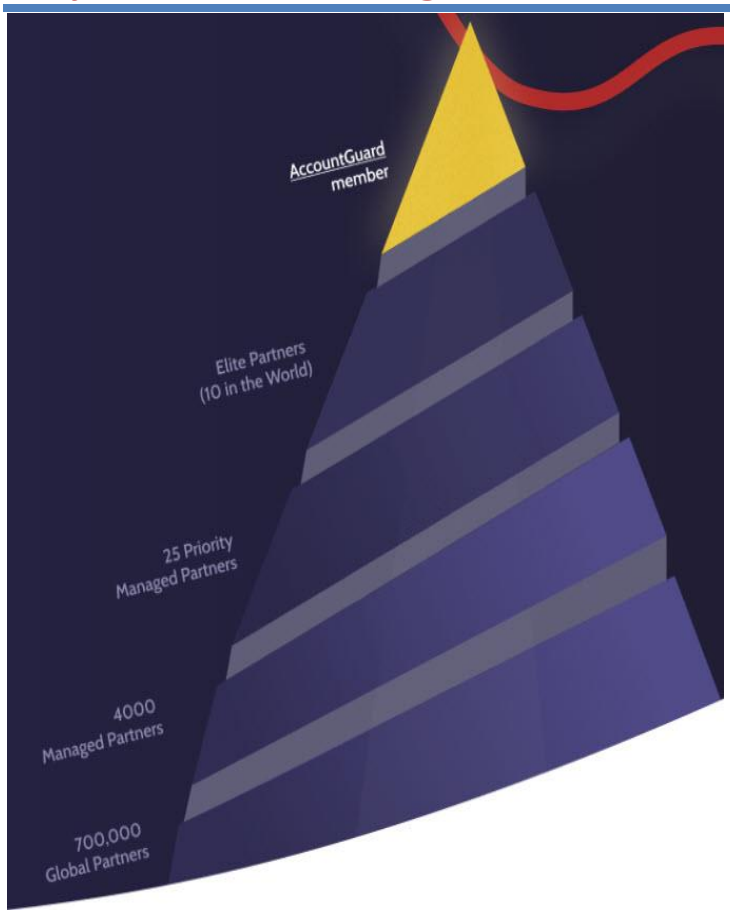
- In the course of its investigation, Patriot may need to create an "E5 Trial License" to gain enhanced visibility into the incident. Client will not be charged and will not be under any obligation to purchase these services.
- Incident response analysis is limited to a single security incident. If additional security incidents are discovered, then Patriot will present a change request to client for additional time. A security incident is defined as an unauthorized user gaining access to a single user account.

About Patriot

Microsoft Solutions Partner
Security
Specialist
Identity and Access Management

Patriot Consulting Technology Group is a Microsoft Partner with offices across the U.S.A Patriot Consulting focuses 100% exclusively on Office 365 Migrations and has migrated over 300 companies and hundreds of thousands of users to Office 365. Patriot Consulting has earned multiple Gold competencies. **Patriot was the only Microsoft Security Partner hand-picked to provide cybersecurity consulting for the US 2020 Elections[1], and is now providing cybersecurity consulting for 31 democracies worldwide. [2]**

Why Patriot Consulting?



- **Our Process is Fast**. We follow a successful project methodology process
- **Client Experience**: We average 98% Client Satisfaction
- **Security at the Top.** Patriot is one of the most trusted names in Microsoft Security. Patriot's CEO is a Microsoft Most Valuable Professional (MVP) in Security.[3]
- **Expertise.** Microsoft selected Patriot for the Microsoft's Elite Partner Program (only the top Microsoft Partners in the world are chosen).

[1] https://blogs.microsoft.com/on-the-issues/2020/06/18/accountguard-security-2020-elections-yubico/
[2] https://blogs.microsoft.com/on-the-issues/2021/03/09/accountguard-expansion-high-risk-defending-democracy/
[3] https://mvp.microsoft.com/en-us/PublicProfile/5003929?fullName=Joe%20Stocker

PATRIOT CONSULTING