PATRIOT CONSULTING

SECURESHIELD 365

MICROSOFT SECURITY DEPLOYMENTS	INTUNE SECURE AUDIT	WEEKLY SECURITY CHECKS	SUPPORT HOURS FOR OFFICE 365

WHY PATRIOT?

WE ARE *THE* MICROSOFT ELITE SECURITY PARTNER

MSFT Priority Managed Partner
(1 of 25 in USA)

Top 3 in United States
98% Customer Satisfaction

Microsoft
Solutions Partner
Security

Specialist
Threat Protection
Identity and Access Management
Information Protection and Governance

1,500+ Projects since 2015
4+ million seats deployed (in 2023)
270+ Clients (in 2023)

Patriot’s Mission Statement

Empowering clients to manage cyber security risk by securely deploying Microsoft cloud technology

Our Core Values

Ethics

Urgency

Passion

A Commitment to Excellence

WHAT IS SECURESHIELD 365?

- SecureShield 365 is managed service for Microsoft 365
- Ongoing security configuration and risk management
- Governance and Remediation based on CIS, SOC2, NIST, ISO 27001, PCI and HITRUST.
- Includes deployment and ongoing management of Intune, M365 Defender and Compliance solutions

DEPLOYMENT SERVICES

Rapidly deploy Microsoft Security, Compliance, Identity, Intune and Purview

SECUREAUDIT 365

Managed Security Configuration

What is SECURESHIELD 365

INTUNE MANAGED SERVICES

Ongoing Intune Design, Planning, Configuration and Deployment

SECURITY HEALTH CHECKS

For Entra & Defender

MANAGED DETECTION AND RESPONSE

24/7/365
Security Operations

UNLIMITED LEVEL 3 SUPPORT

For *Intune, Entra, Purview & Defender*

SECUREAUDIT 365

AUDIT OF 940+ Settings IN M365 & Azure

24 Hours of Remediation

MONTHLY REPORTS

- New Settings
- Webinars & Training

PowerBI Reporting

ClientName	SettingID	Type	Grouping	Recommendation
Patriot Consulting Technology	625	Critical	3rd Party application access	Limit group owners who can consent to apps accessing data. (Setting #625)
Patriot Consulting Technology	417	Critical	Defender for Cloud Apps	Configure and Deploy Microsoft Cloud Access Security Broker (CASB) that operates on mul cyberthreats across all your cloud services. -- OR -- Resolve MDCA Alerts or limit alert funct
Patriot Consulting Technology	405	Critical	Defender for Identity	Configure and deploy Defender for Identity, a cloud-based security solution that leverages identities, and malicious insider actions directed at your organization. (Setting #405 - #414)
Patriot Consulting Technology	925	Critical	Device Access and Management	Deploy Windows LAPS, a free tool from Microsoft to randomize and then rotate local admin Infrastructure, consider using LAPS for Active Directory. (Setting #925)
Patriot Consulting Technology	16	Critical	Device Access and Management	If this is set to NO, AND if there is no CA Policy to require MFA for Device Registration or In (Setting #16) i) Also, if MFA settings allow push notification without code matching, or if phone verificat
Patriot Consulting Technology	926	Critical	Device Access and Management	Intune connectors are a very important part of your organization; they keep data flowing t
Patriot Consulting Technology	84	Critical	Exchange	Customize 'MyBaseOptions' management role in OWA policy to remove the automatic ema outbound spam rule against auto-forwarded messages. (Setting #84)
Patriot Consulting Technology	342	Critical	Exchange	Disable or Restrict access to remote PowerShell for Exchange Online (except Admins). By de
Patriot Consulting Technology	628	Critical	Exchange Online Protection	Disable Auto-Forwarding mode in Outbound Spam Policy or with a transport rule. (Setting #
Patriot Consulting Technology	624	High Security	3rd Party application access	Consider using preview settings to allow Pre Approved permissions levels to automatically b
Patriot Consulting Technology	146	High Security	3rd Party application access	Disable the Office store so users do not install 3rd party plug-ins to Outlook w/o requiring
Patriot Consulting Technology	623	High Security	3rd Party application access	Prevent users from consenting to apps accessing company data on their behalf and requir permissions to be allowed. (Setting #623, #624)
Patriot Consulting Technology	358	High Security	Admins	Reduce the total # of Global Admins (you have ##), Microsoft recommends 5 or less. (Setting
Patriot Consulting Technology	669	High Security	Admins	Remove Synced accounts Admin Permissions and begin mastering all Admin roles in Entra https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-micros
Patriot Consulting Technology	618	High Security	Admins	Review current alerts in the Microsoft 365 Admin Center. (Setting #618)
Patriot Consulting Technology	31	High Security	Authentication	Consider using Identity Protection to deploy MFA, which has a built-in 14-day grace perio
Patriot Consulting Technology	630	High Security	Authentication	If you aren't going to customize the individual threat policies, Microsoft suggests that you
Patriot Consulting Technology	140	High Security	Authentication	Recommend locking down the MFA verification methods to only use Number Matching, Ver (Setting #140)
Patriot Consulting Technology	777	High Security	Authentication	Recommend that the auto unblocked be set to at least 15 minutes or more. (Setting #777

Patriot Academy

Defender Experts Security Defender

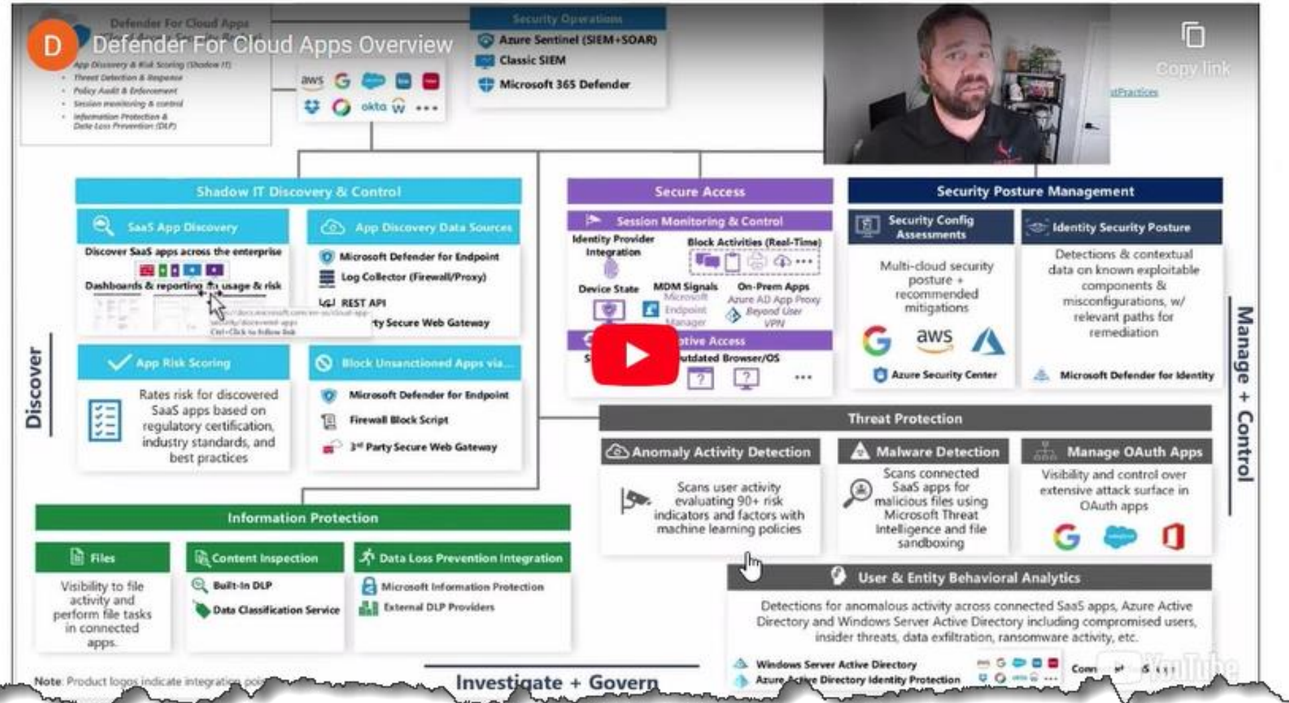
- Defender
  - Portal Security Permissions
- Defender for Cloud Apps
  - Advanced Hunting
  - Conditional Access App Control
- Defender for Endpoint
  - Advanced Hunting
  - Attack Surface Reduction (ASR)
  - Operations Guide
- Defender for Identity
  - Advanced Hunting
  - GMSA Setup
- Defender for Office
  - Advanced Hunting
  - Transport Rule Examples

Defender for Cloud Apps

Features
Benefits

Defender for Cloud Apps

Defender for Cloud Apps is a comprehensive security solution designed to protect cloud-based applications and data across various platforms, including Microsoft 365, Azure, and other Software-as-a-Service (SaaS) applications. With its advanced threat detection and response capabilities, Defender for Cloud Apps helps organizations safeguard their cloud environments and mitigate risks associated with cloud app-related threats.

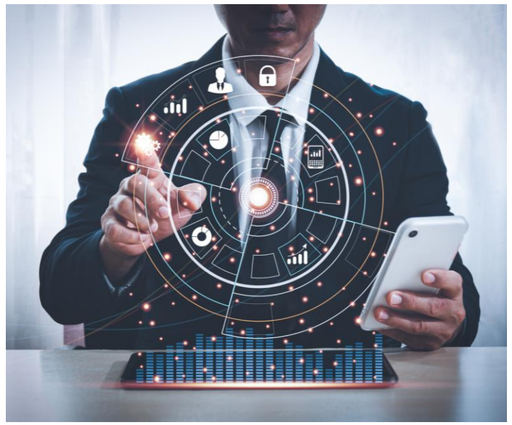


SECURITY HEALTH CHECKS

INCLUDED

- 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 included User risk, Active Incidents, Security Score
- Review Message Center updates for Action
- Deliverable will be sent to client quarterly containing a summary of findings and recommendations



2023

Patriot Consulting

INTUNE MANAGED SERVICES

Intune Managed services take the strain off your resources when it comes to deploying, managing and protecting Windows 10, iOS/iPadOS, Android, MacOS endpoints and applications.

NET NEW DEPLOYMENTS

EXISTING INTUNE DEPLOYMENTS

- For those who already utilize Intune
- Receive a complete audit of your existing configuration
- Monthly configuration updates based on new Intune features and changes.
- Included Hours per month for Professional Services for supported configurations
- Roadmap updates allow you to get ahead of coming changes and helps you make decisions that could impact the end user
- As built documentation describing any updates and changes to tenant

NET NEW INTUNE DEPLOYMENTS

- For brand new deployments
- Provides a baseline deployment of Intune based on Patriot best practices
- Monthly configuration updates based on new Intune features and changes
- Roadmap updates allow you to get ahead of coming changes and helps you make decisions that could impact the end user
- Included Hours per month for Professional Services for supported configurations
- As built Design and Planning document that details the specifics of the deployment and any updates made as new features and changes occur

PLATFORMS

Windows 10
macOS
iOS & Android

MICROSOFT DEFENDER DEPLOYMENT SERVICES

DEFENDER FOR ENDPOINT

A COMPLETE ENDPOINT SECURITY SOLUTION

- Agentless and Cloud powered so it is always up to date
- Unparalleled optics and built on the industry's deepest threat intelligence
- Automated Security
- that goes from alert to remediation in minutes at scale

DEFENDER FOR IDENTITY

MANAGE IDENITITY RISKS

- Identify and Resolve Vulnerabilities and help eliminate on prem vulnerabilities.
- Assess threats efficiently
- focus on real threats and help security teams prioritize information.

DEFENDER FOR OFFICE

INTEGRATED THREAT PROTECTION FOR OFFICE 365

- Native Protection for Office 365 that boost productivity and lowers total cost of ownership
- Industry leading AI and automation that improves sec ops efficiency through automated workflows
- Comprehensive approach that helps protect your organization from attacks across kill chain

DEFENDER FOR CLOUD APPS

APPLICATION SECURITY

- Discover and manage your apps to streamline cloud access security with native integration
- Govern access to apps and resources that can uncover shadow IT
- Evaluate your cloud apps against compliance standards to prevent leaks & limit access to regulated data

MXDR365

www.MXDR365.com

Patriot's 24x7x365 Managed Extended Detection & Response Service built upon Microsoft Sentinel

Ransomware attacks grew over 100% over the past year, and the tactics are becoming more sophisticated. No organization is immune

MXDR protects you from these new threats by being a complete service from assessment to enablement

How does MXDR365 Protect Your Organization?

Our 24/7/365 managed security operations center (SoC) services include:

- Advanced Detection
- Advanced Investigation
- Advanced hunting
- Automated and AI and Machine trained Intelligent response
- Remediation across all Microsoft Products (M365 and Azure) using Microsoft Sentinel

ONBOARD INTEGRATE MONITOR HUNT RESPOND REPORT

ORGANIZATIONS LACK BUDGET OR IN-HOUSE SECURITY RESOURCES TO MANAGE ALERTS OR ARE SEEKING DEEPER DETECTION EXPERTISE

LACK OF EXPERTISE

Does your IT Team have deep security investigation experience to detect and respond to attacks? Can they do it 24/7?

ALERT FATIGUE

Security solutions such as Microsoft Defender for Endpoint or Sentinel identify thousands of issues and alerts daily—most of which are not threats to the organization. Trying to keep up with the volume can be exhausting.

BUDGET LIMITATIONS & Staffing Challenges

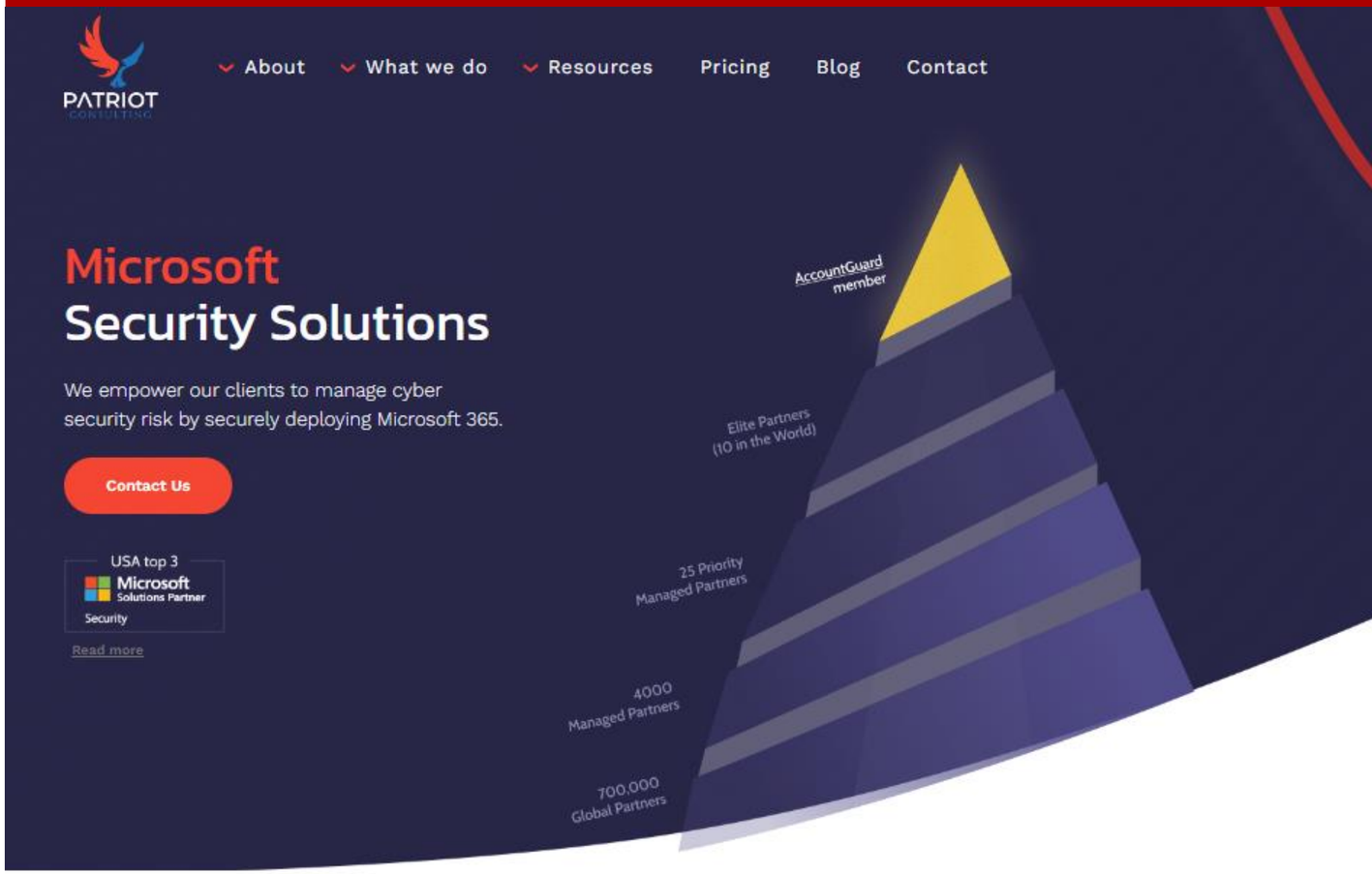
The cost to staff a 24/7 SOC is expensive – 3 x 8 hour shifts of Tier1 and Tier2 analysts. Finding the talent is hard! 3 million unfilled security jobs creates a supply shortage. The challenge of retaining top talent is equally difficult!

GET IN TOUCH

We are always here to help

Irvine, CA

1-844-560-4630

secure365@patriotconsultingtech.com

www.patriotconsultingtech.com