Dekalb County School District

AllyCare for Microsoft 365

Statement of Work

SOW Delivery Date: 6/26/2026

SOW Expiration Date: 8/25/2026

Submitted By: Monica Davis

(P) (404) 316-3565

mdavis@blueally.com

Table of Contents

1.0 Introduction

Statement of Work

This Statement of Work (SOW) is effective as of June 26, 2026, between Dekalb County School District (Client) and BlueAlly Technology Solutions, LLC (Service Provider). The parties agree as follows.

Client:	Dekalb County School District
Client Contact:	Dr. Kermit Belcher
Project Name:	AllyCare for Microsoft 365
Statement of Work ID:	BA2026105663-1
Statement of Work Investment Summary:	$241,086
Statement of Work Date:	June 26, 2026
Statement of Work Expiry Date: (if not executed by all Parties)	August 25, 2026
Service Provider Contact:	Monica Davis

2.0 Solution Description

2.1 AllyCare Guardian

The AllyCare Guardian solution provides continuous security hardening, monitoring, and breach detection for Microsoft 365 tenants. The service builds on Microsoft 365 E5/G5/A5 licensing to maximize available security features, reduce redundancy, and ensure proactive compliance alignment. AllyCare Guardian is delivered as a recurring service focused on reviewing, implementing, and updating workloads across the Microsoft ecosystem while incorporating MAD365 for advanced breach detection and monitoring.

Table 1: Scoping Worksheet

Item	Core System / Service Component	Scope Parameters
1	Microsoft 365 Tenant Workloads	Entra ID, Purview, Defender for Cloud Apps, Defender for Endpoints, Exchange Online, Intune (MAM), OneDrive, SharePoint, Teams
2	Security Review & Hardening Cycle	Initial assessment followed by ongoing quarterly reviews
3	MAD365 Identity Breach Protection	Log ingestion, anomaly detection, and engineer-led analysis
4	Security Policy Implementation	Conditional Access, Multi-Factor Authentication (MFA), Data Loss Prevention (DLP), Retention, Anti-Spam/Phishing/Malware policies
5	Monitoring & Alerting	Periodic monitoring, high-risk escalation to Client, remote technical support

Services Provided

Service Provider will employ the BlueAlly solution delivery methodology as the framework to deliver AllyCare Guardian. Project phases are described below:

Project Initiation

- Conduct kickoff meeting and review scope
- Request and validate system access

- Develop project plan/schedule

Discovery and Assessment

- Perform initial assessment of Microsoft 365 tenant security posture
- Review Entra ID, Purview, Defender, Exchange, Intune (MAM), OneDrive/SharePoint, Teams
- Deliver findings and prioritized timeline

Implementation and Hardening

- Implement agreed-upon security changes in working sessions
- Apply MFA, Conditional Access, DLP, Safe Links/Attachments, and retention policies
- Provide support immediately following implementation

MAD365 Breach Detection and Monitoring

- Weekly review of Microsoft Defender for Cloud Apps logs
- Anomaly detection: impossible travel, anonymous IPs, failed logins, suspicious activity
- Engineer review and escalation of high-risk issues

Ongoing Review and Optimization

- Quarterly reviews and compliance alignment
- Continuous updates for new Microsoft security features
- Recommendations for additional controls and configuration improvements

Deliverables

- Security Assessment Report
- Prioritized Implementation Plan
- Quarterly Security Review Reports
- MAD365 Alerts
- Configuration and Policy Documentation

2.2 AllyCare Support

The AllyCare Support solution provides Level 1 and Level 2 assistance for Microsoft 365 workloads, ensuring consistent end-user support, troubleshooting, and escalation management. The service consolidates ticket intake, triage, and resolution through Service Provider's secure support portal and certified Microsoft 365 engineers.
When Microsoft intervention is required, Service Provider manages the escalation process end-to-end, providing a single point of contact for your Microsoft 365 support needs.
Key benefits include:

- Centralized case management and visibility through the ticketing portal
- Direct access to certified Microsoft 365 engineers for faster resolution
- Streamlined Microsoft escalation management under your support entitlements

Table 2: Scoping Worksheet

Item	Core System / Service Component	Scope Parameters
1	Microsoft 365 Core Workloads	Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams
2	Security & Compliance	Microsoft Purview, Defender for Cloud Apps, Defender for Endpoints, Defender for Identities, Defender for Office 365, Entra ID, Intune

Item	Core System / Service Component	Scope Parameters
3	Productivity & Platform Support	Microsoft 365 Apps, Power Platform (Power Apps, Power Automate, Power BI, Power Pages)
4	L1/L2 Troubleshooting	Incident triage, diagnosis, and resolution across supported workloads
5	Escalation Management	Microsoft case creation, tracking, and resolution coordination

Services Provided

Service Provider will employ the BlueAlly service delivery methodology to deliver AllyCare Support.

Project Initiation

- Conduct a kickoff meeting and review the service scope
- Validate access and Client Enrollment Package (CEP)
- Establish ticketing, escalation, and change management workflows
-

Incident Intake and Triage

- Intake support requests via portal, email, or phone
- Categorize, prioritize, and assign cases
- Perform initial troubleshooting using established knowledge base/runbooks

L1/L2 Troubleshooting and Resolution

- Resolve common end-user and workload issues (Exchange, Teams, OneDrive, SharePoint)
- Provide support for Purview alerts, Defender incidents, and Intune/Entra ID configuration errors
- Escalate complex or unresolved issues to Microsoft as required

Escalation and Vendor Coordination

- Open and manage support cases with Microsoft under Client entitlements
- Track escalation progress and maintain communication until resolution

Ongoing Support Operations

- Provide end-user updates and ticket status visibility
- Implement workarounds to restore service quickly where possible
- Document resolutions and update the knowledge base

Deliverables

- Kickoff and Service Setup Documentation
- Secure Support Portal Access (Client enrollment, knowledge transfer, and portal knowledge transfer)
- Case Resolution Summaries (ticket documentation and root cause analysis (RCA) notes)
- Escalation Reports (status and outcome of vendor-managed cases)
- Knowledge Base Updates (runbooks and standard fixes maintained by Service Provider)

SLA Response Guide

The following is Service Provider's SLA Response Guide:

- Note: Service Provider maintains its own SLAs separately from those kept by Microsoft
- P1 tickets are the only tickets considered "emergency" and will receive a 24x7x365 response
- P1 tickets must be called in to receive an emergency response

- All portal tickets are handled as P2-P4, which are handled during normal business hours (8:00 am – 5:00 pm Central time)

Service Provider Targeted Response Times

Priority	Response SLA (Bus Hours)	Response SLA (After Hours)	Description	Business Impact
P1: CRITICAL	1 Hour	2 Hours	Microsoft 365 service outage or security incident preventing user access with no workaround.	Organization-wide or critical business functions unavailable.
P2: HIGH	4 Hours	Next business day	Degradation of a core Microsoft 365 service affecting multiple users or departments.	Business operations significantly impacted but not fully halted.
P3: MEDIUM	24 Hours	Next business day	Issue affecting individual users or non-critical Microsoft 365 functionality.	Limited impact to daily operations.
P4: LOW	48 Hours	Next business day	Informational requests, minor issues, or advisory support related to Microsoft 365.	No material business impact.

Access and Permissions

Service Provider may require remote access to Client's Microsoft 365 tenant. Remote access can be established by Granular Delegated Admin Privileges (GDAP) (recommended) or a local account in your tenant with the appropriate roles assigned. Service Provider will coordinate establishing access to your tenant during the onboarding process.

2.3 AllyCare Assist

The AllyCare Assist solution offers organizations a flexible yearly retainer program, providing access to a dedicated block of consulting and engineering hours for Microsoft cloud and on-premises systems. Hours can be applied toward reactive support or strategic initiatives, eliminating the need for separate project contracts.

Designed to adapt to evolving IT needs, AllyCare Assist ensures that expert help is always available — whether deploying new Microsoft 365 capabilities, optimizing Azure workloads, securing hybrid environments, or maintaining on-premises infrastructure.

Key benefits include:

- Flexible allocation of yearly hours across Microsoft 365, Azure, and Windows Server workloads
- Access to strategic advisory services such as roadmap planning, licensing guidance, and adoption strategies
- Hybrid expertise spanning cloud and on-premises platforms
- Predictable IT spend through a fixed yearly cost

Table 3: Scoping Worksheet

Item	Core System / Service Component	Scope Parameters
1	Microsoft 365 & Azure Workloads	Exchange Online, Teams, SharePoint, OneDrive, Azure networking, firewalls, security
2	Hybrid & On-Premises Support	Windows Server, Active Directory, Entra ID synchronization
3	Flexible Hour Allocation	Yearly retainer block for proactive or reactive tasks
4	Strategic Advisory	Roadmap planning, licensing reviews, adoption strategies, cost optimization
5	Common Use Cases	Tenant health checks, migration planning, DLP/security assessments, licensing reviews

Services Provided

Service Provider will employ the BlueAlly service delivery methodology to deliver AllyCare Assist.

Hour Allocation and Intake

- Allocate yearly hours per Client's priorities
- Submit requests via the support portal
- Prioritize and schedule requests based on availability and agreed timelines

Ongoing Service Operations

- Track consumed hours and provide usage visibility
- Allow purchase of additional hours at the contracted rate
- Deliver periodic updates and recommendations

Deliverables

- Kickoff and Service Setup Documentation
- Service Portal Access: enrollment, knowledge transfer, and request process knowledge transfer
- Assessment Reports: tenant health, licensing, or cost optimization as requested
- Configuration and Advisory Outputs: documentation of tasks completed under retainer hours
- Yearly Usage Summary: hours consumed, tasks completed

3.0 Period of Performance

The Period of Performance is twelve (12) months from the date of Project Kickoff. Working sessions are scheduled in one (1)-hour blocks. Remote delivery is assumed unless otherwise agreed.

4.0 Responsibilities and Assumptions

4.1 Service Provider Responsibilities

- Lead kickoff, discovery, implementation, and quarterly review activities
- Provide security assessment, design, and implementation support
- Monitor MAD365 logs and escalate high-risk events
- Deliver quarterly reporting and recommendations
- Maintain project documentation and communicate updates

4.2 Client Responsibilities

- Assign stakeholders and establish a single point of contact (SPOC)

- Provide required system access and documentation
- Participate in working sessions and approve deliverables
- Maintain licensing and ensure environmental readiness

4.3 Assumptions

- Client must hold Microsoft 365 E5/G5/A5 licensing to leverage all features
- Client Subject Matter Experts (SMEs) and stakeholders are available for workshops and reviews
- Client provides secure remote access and Identity and Access Management (IAM) permissions to Service Provider engineers
- Additional functionality outside scope requires a Change Order

4.4 Out-of-Scope Services

This guide outlines the services provided. Any services not explicitly detailed within this guide are considered beyond the scope of this service. Requests falling outside the scope may necessitate adjustments to the existing contract, denial of service, or additional billing on an hourly basis. Before any billing for services outside the agreed scope, Client approval is mandatory.
The following services are out of scope and require a separate engagement or contract modification:

- Network infrastructure redesign
- Custom development or third-party security platform integration
- Support for non-Microsoft cloud platforms

5.0 Working Hours and Services Criteria

5.1 Designated Place of Work

Service Provider's designated place of work will be remote. Meetings with Client will be held via web conference.

6.0 Change Management Process

In the event unforeseen factors change this services scope of work and/or impact the term and cost of Service Provider provided services, Client and Service Provider may mutually revise the Agreement and Service Provider shall provide Client with an estimate of the impact of such revisions to the fees, payment terms, completion schedule, and other applicable provisions of the Agreement. If the parties mutually agree to such changes, a written description of the agreed-upon change ("Change Order") shall be prepared, incorporating such changes to the Agreement, and shall be signed by both parties. The terms of a Change Order prevail over those of the Agreement.

7.0 Engagement Terms and Conditions

7.1 Engagement Contacts

	Service Provider Contact	Client Engagement Contact
Contact name	Monica Davis	Dr. Kermit Belcher
E-mail address	mdavis@blueally.com	Kermit_Belcher@dekalbschoolsga.org
Phone number	(404) 316-3565	(678) 676-1188
Mailing address	3475 Piedmont Road NE, Suite 900 Atlanta, GA 30305	2652 Lawrenceville Highway Decatur, GA 30033

7.2 Project Pricing and Invoicing

This quote is a fixed-price quote. Invoicing will be performed monthly at the beginning of the contract period or upfront.

Description	Monthly Fee	Annual Fee
AllyCare Guardian (3,000-5,999 users)	$7,978	$95,736
AllyCare Support (3,000-5,999 users) (January 1, 2027 – August 31, 2027)	$4,267	$34,136
AllyCare Assist (451 hrs total)	$8,926	$107,112
Total Cost	**$21,171**	**$236,984**

AllyCare Support requires a one-time setup/onboarding fee of $4,102 which will be billed up front.

7.3 Terms and Termination

The term of this SOW begins on the SOW execution date and ends upon Client's acceptance of engagement. Service Provider will provide a Certificate of Acceptance document or email to Client for signature to acknowledge the completion of the contract in writing. Client will return the signed acceptance document or an email stating acceptance within ten (10) business days of receipt. If Client fails to respond or notify Service Provider of discrepancies, then Service Provider will perceive the non-response as acceptance.

7.4 Microsoft Partner of Record

Client agrees to designate BlueAlly as its Partner of Record with Microsoft for the following:

- ✓ Azure Subscriptions – those used as part of this project
- ✓ Microsoft/Office 365 – those workloads that are part of this project
- ✓ Intune

Disclosure to Client: Microsoft may pay Service Provider incentives for helping to implement and support Azure, Office 365 and EMS. This does not change Client's licensing, support, and pricing agreements with Microsoft.

7.5 Terms and Conditions of Engagement

Client agrees to purchase from Service Provider those services specified in the SOW attached hereto. In addition to the terms and conditions set forth in the SOW, Client agrees that all services provided by Service Provider to Client will be subject to the following terms and conditions:

1. Billing. Payment for services rendered by Service Provider shall be billed and invoiced by Service Provider on a periodic basis. Client agrees to pay all invoiced amounts within thirty (30) days of the date of invoice. All out-of-pocket expenses incurred by Service Provider in the performance of

services to Client shall be billed as incurred. Client shall pay all such expenses as promptly as practicable after receipt thereof. All taxes incurred by Client, resulting from the performance by Service Provider of the services specified in the SOW, shall be the responsibility of Client.

2. No Solicitation. During the term of the services provided by Service Provider to Client and for a period of twelve (12) months thereafter, Client shall refrain from soliciting for hire any current or future Service Provider employee, provided that nothing shall prevent Client from general solicitation for hire of employees through public advertisement.

3. Termination. Client may terminate the transactions contemplated by the SOW and this agreement upon the material breach or non-performance by Service Provider of the terms and conditions set forth in the SOW or this agreement, provided that Service Provider fails to cure such breach or non-performance within thirty (30) days of Service Provider's receipt of notice thereof. Service Provider may terminate the transactions contemplated by the SOW and this agreement upon the material breach by Client of the terms and conditions set forth in the SOW or this Agreement, or the failure by Client to pay any amounts due or to become due under the terms hereof or thereof. Client shall remain liable for payment of all fees and expenses incurred by Client up to the date of termination.

4. Limitation of Liability. Client's sole and exclusive remedy for all claims, damages, losses, costs, fees, expenses, or similar items arising from the transactions contemplated by the SOW, including the provision of services by Service Provider, shall be limited to termination by Client of the services set forth in the SOW in accordance with the terms set forth above. In no event shall Service Provider be liable for any incidental, consequential, or punitive damages, including any damages resulting from the loss of data or its use, lost profits, or claims asserted against Client by a third-party. Service Provider DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

5. Access. Client shall afford Service Provider access to such Client technical matter, data, information, operating supplies, and computer system(s), as may be reasonably required by Service Provider to perform the services set forth in the SOW (including, providing Service Provider with a primary point of contact).

6. Service Provider Personnel. Service Provider retains sole discretion to assign such Service Provider personnel as it deems necessary or appropriate to perform the services set forth in the SOW. Service Provider will provide Client with a primary point of contact for inquiries regarding the services.

7. Confidentiality. Any information (whether written or oral) designated as confidential at any time by either party shall be held in strict confidence by the receiving party and may be used by the receiving party only for the purposes set forth in the SOW and the terms of this agreement. Except as required by law, no confidential information, including the terms of this agreement and the SOW, shall be disclosed by either party without the prior written consent of the party designating the information as confidential. Confidential information shall not include any information, that is in or becomes part of the public domain through no fault of the recipient, is already known to the recipient, has been developed independently, or is received from a third party without similar restriction and without breach of this or a similar agreement. Nothing contained in this agreement or the SOW shall prevent Service Provider from publicizing its business relationship with Client or the nature of the services it provided to Client.

8. Interpretation. In the event of a conflict between the terms and provisions of this agreement and the SOW, any purchase order or other document authorizing the work or services covered by this agreement and the SOW, the provisions of this agreement, and the SOW shall govern.

8.0 Acceptance and Authorization

The terms and conditions of the Statement of Work apply in full to the services and products provided under this Statement of Work.

IN WITNESS WHEREOF, the parties hereto each acting with proper authority have executed this Statement of Work, under seal.

	BlueAlly Technology Solutions, LLC	**Dekalb County School District**
Signature		
Name	Jason Schroeder	
Title	SVP, Services	
Date		

Appendix A: AllyCare Guardian

The following table details the minimal security workloads covered by AllyCare Guardian. As Microsoft adds workloads and functionality, the additions will be incorporated.

Overall Tenant Security Checklist:

Tasks / Effort	Platform
Review Entra ID Reporting	Entra ID
Turn on User Risk Policies	Entra ID
Turn on User Sign-in Policies	Entra ID
Restrict user consent to applications	Entra ID
Do not allow users to grant consent to unmanaged/unreliable applications	Entra ID
Restrict logins by IP / Geo-Location	Entra ID
Enable self-service password reset	Entra ID
Enforce MFA for Admins	Entra ID
Set up Entra ID Break Glass Accounts	Entra ID
Implement Privileged Identity Management for Just-in-Time access	Entra ID
Remove dormant accounts from sensitive groups	Entra ID
Use limited administrative roles	Entra ID
Implement Custom Banned Passwords List and Lockout thresholds	Entra ID
Secure Applications Access using Conditional Access Rules	Entra ID
Ensure all users can complete multi-factor authentication for secure access	Entra ID
Configure Named Locations to allow bypass of conditional access policies	Entra ID
Block Legacy Authentication	Entra ID
Do not expire passwords	Entra ID
Enable password hash sync if hybrid	Entra ID
Configure General Anti-Spam Policies	Compliance & Security
Configure Safe Links	Compliance & Security
Configure Safe Attachments Delivery in block mode	Compliance & Security
Configure DLP (Data Loss Prevention) Rules and notifications	Compliance & Security
Configure Retention Policies	Compliance & Security
Configure General Anti-Phishing Policies	Compliance & Security
Configure user/domain impersonation	Compliance & Security
Configure Impersonation Safety Tips	Compliance & Security
Configure General Anti-Malware Policies	Compliance & Security
Create customized DLP policies for personal data	Compliance & Security
Create DLP Policies for Company Sensitive Information	Compliance & Security
Create DLP Policies for Personally Identifiable Information	Compliance & Security
Configure Sensitivity Labels	Compliance & Security
Apply sensitivity labels to protect sensitive or critical data	Compliance & Security
Configure Microsoft Information Protection Scanner for on-premises file classifications	Compliance & Security
Review Security Recommendations for Azure and remediate	Compliance & Security
Ensure that Auto-labeling data classification policies are set up and used	Compliance & Security
Configure supported app connectors	MDCA
Configure Conditional Access App Controls for apps for session control	MDCA
Enable Entra ID Identity Protection Integration	MDCA
Enable Defender for Identities Integration	MDCA
Configure Unsanctioned Apps to block access using Defender for Endpoints	MDCA
Discover Risky and Non-Compliant Shadow IT Applications	MDCA
Detect anomalous behavior	MDCA
Set automated notifications for new and trending cloud applications in Client organization	MDCA
Notify upon Detection of New OAuth Application	MDCA

Tasks / Effort	Platform
Create a Custom Activity Policy to Discover Suspicious Usage Patterns	MDCA
Email Notifications	MDCA
Microsoft Defender for Endpoints Integration	MDCA
User Enrichment Integration with Entra ID	MDCA
Automatically scan new files for sensitivity labels and content inspection warnings	MDCA
Azure Security Monitoring	MDCA
Install Defender for Endpoints on Servers	MDE
Enable Entra ID Identity Protection Integration	MDE
Enable Tamper Protection	MDE
Configure Device Groups	MDE
Web Content Filtering	MDE
Automatically Resolve Alerts	MDE
Configure Auto-remediation levels	MDE
Use MDE to enforce security configuration settings from MEM	MDE
Automated Investigation	MDE
Live Response	MDE
Live Response for Servers	MDE
Enable EDR in block mode	MDE
Allow of block file	MDE
Show user details	MDE
Office 365 Threat Intelligence connection	MDE
Microsoft Defender for Cloud Apps Integration	MDE
Microsoft Intune connection	MDE
Device discovery	MDE
Email Notifications	MDE
Implement Outbound Spam Policy	Exchange Online
Implement DMARC for outbound mail	Exchange Online
Enable Client Rules Forwarding Block	Exchange Online
Set action to take on high-confidence spam detection	Exchange Online
Ensure that no sender domain allowed for an anti-spam policy	Exchange Online
Spam retention in Quarantine (recommended is 30 days)	Exchange Online
Block users who reached the message limit (300 per day)	Exchange Online
Set up a Sender Policy Framework to prevent spoofing	Exchange Online
Implement BIMI with a logo	Exchange Online
Configure Message Records Management Tags and Policies (for archiving)	Exchange Online
Allow Mailbox Delegation Only When Authorized	Exchange Online
Do Not Override FROM Address Enforcement	Exchange Online
Implement connection filter	Exchange Online
Do not allow Exchange Online calendar details to be shared with external users	Exchange Online
Enable Mailbox Intelligence	Exchange Online
Move messages that are detected as impersonated users by mailbox intelligence	Exchange Online
Quarantine messages that are detected from impersonated domains	Exchange Online
Quarantine messages that are detected from impersonated users	Exchange Online
Set action to take on phishing detection	Exchange Online
Set the email bulk complaint level (BCL) threshold to be 6 or lower	Exchange Online
Configure Application Protection Policies for unmanaged devices	Intune
Configure Application Configuration Policies for unmanaged devices	Intune
Review and Configure OneDrive and SharePoint Sharing configuration	OneDrive/SharePoint
Review Security configuration for OneDrive and SharePoint	OneDrive/SharePoint
Block unmanaged devices from running desktop apps	OneDrive/SharePoint
Block Apps that don't use modern authentication	OneDrive/SharePoint
Enable versioning for document libraries	OneDrive/SharePoint
Configure External Sharing Links to Expire	OneDrive/SharePoint

Tasks / Effort	Platform
Sign out inactive users in SharePoint Online	OneDrive/SharePoint
Allow syncing only on computers joined to specific domains	OneDrive/SharePoint
Review the ADFS environment for security	On-premises
Entra ID Password Protection on on-premises domain controller	On-premises
Configure Microsoft Defender for Identities (formerly Azure ATP)	On-premises
Configure secondary Entra ID Connect server in staging	On-premises
Configure which users are allowed to present in Teams meetings	Teams
Require lobbies to be set up for Teams meetings	Teams
Restrict anonymous users from joining meetings	Teams
Limit external participants from having control in a Teams meeting	Teams
Restrict anonymous users from joining Teams meetings	Teams
Restrict dial-in users from bypassing a meeting lobby	Teams
Only invited users should be automatically admitted to Teams meetings	Teams

Defender for Endpoints (client-specific) checklist:

Tasks / Effort	Platform
Turn on Firewall in macOS	MDE
Turn on Microsoft Defender Antivirus PUA protection in block mode on macOS	MDE
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	MDE
Block Win32 API calls from Office macros	MDE
Block execution of potentially obfuscated scripts	MDE
Block Office applications from injecting code into other processes	MDE
Block executable content from email client and webmail	MDE
Block persistence through WMI event subscription	MDE
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	MDE
Block Office applications from creating executable content	MDE
Block Office communication application from creating child processes	MDE
Block Adobe Reader from creating child processes	MDE
Block all Office applications from creating child processes	MDE
Block process creations originating from PSExec and WMI commands	MDE
Block untrusted and unsigned processes that run from USB	MDE
Block JavaScript or VBScript from launching downloaded executable content	MDE
Block abuse of exploited vulnerable signed drivers	MDE
Enable 'Network Protection'	MDE
Set User Account Control (UAC) to automatically deny elevation requests	MDE
Disable Solicited Remote Assistance	MDE
Disable 'Allow Basic authentication' for WinRM Service	MDE
Disable 'Allow Basic authentication' for WinRM Client	MDE
Set LAN Manager authentication level to 'Send NTLMv2 response only. Refuse LM & NTLM'	MDE
Set default behavior for 'AutoRun' to 'Enabled: Do not execute any autorun commands'	MDE
Enable 'Require additional authentication at startup'	MDE
Disable 'Enumerate administrator accounts on elevation'	MDE
Enable 'Local Security Authority (LSA) protection'	MDE
Turn on Microsoft Defender Application Guard managed mode	MDE
Turn on Microsoft Defender Credential Guard	MDE
Enable scanning of removable drives during a full scan	MDE
Disable Anonymous enumeration of shares	MDE
Disable 'Autoplay' for all drives	MDE
Fix unquoted service path for Windows services	MDE
Enable FileVault Disk Encryption in macOS	MDE
Set account lockout threshold to 5 or lower in macOS	MDE
Secure Home Folders in macOS	MDE
Set minimum password length to 15 or more characters in macOS	MDE

Tasks / Effort	Platform
Set 'Account lockout threshold' to 1-10 invalid login attempts	MDE
Disable JavaScript on Adobe DC	MDE
Ensure the screensaver is set to start in 20 minutes or less in macOS	MDE
Set the screen to lock when screensaver starts in macOS	MDE
Set 'Maximum password age' to '90 or fewer days, but not 0' in macOS	MDE
Set 'Enforce password history' to '24 or more password(s)' in macOS	MDE
Disable JavaScript on Adobe Reader DC	MDE
Disable Flash on Adobe Reader DC	MDE
Enable 'Hide Option to Enable or Disable Updates'	MDE
Disable 'Continue running background apps when Google Chrome is closed'	MDE
Block outdated ActiveX controls for Internet Explorer	MDE
Disable running or installing downloaded software with an invalid signature	MDE
Set 'Interactive logon: Machine inactivity limit' to '1-900 seconds'	MDE
Enable Local Admin password management	MDE
Disable 'Installation and configuration of Network Bridge on your DNS domain network'	MDE
Enable 'Microsoft network client: Digitally sign communications (always)'	MDE
Disable the local storage of passwords and credentials	MDE
Disable IP source routing	MDE
Set IPv6 source routing to the highest protection	MDE
Disable 'Autoplay for non-volume devices'	MDE
Set 'Minimum PIN length for startup' to '6 or more characters'	MDE
Enable 'Apply UAC restrictions to local accounts on network logons'	MDE
Prohibit the use of Internet Connection Sharing on DNS domain network	MDE
Set 'Minimum password age' to '1 or more day(s)'	MDE
Set 'Enforce password history' to '24 or more password(s)'	MDE
Set 'Minimum password length' to '14 or more characters'	MDE
Disable 'Password Manager'	MDE
Set user authentication for remote connections by using Network Level Authentication to 'Enabled'	MDE
Disable merging of local Microsoft Defender Firewall connection rules with group policy firewall rules for the Public profile	MDE
Disable merging of local Microsoft Defender Firewall rules with group policy firewall rules for the Public profile	MDE
Enable Automatic Updates	MDE
Enable Gatekeeper in macOS	MDE
Secure Microsoft Defender firewall private profile	MDE
Secure Microsoft Defender Firewall domain profile	MDE
Secure Microsoft Defender Firewall public profile	MDE
Fix Microsoft Defender for Endpoint sensor data collection in macOS	MDE
Enable 'Block third party cookies'	MDE
Enable 'Require domain users to elevate when setting a network's location'	MDE
Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile	MDE
Disable Microsoft Defender Firewall notifications when programs are blocked for Private profile	MDE
Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile	MDE
Encrypt all BitLocker-supported drives	MDE
Update Microsoft Defender for Endpoint core components	MDE
Fix Microsoft Defender for Endpoint impaired communications in macOS	MDE
Fix Microsoft Defender for Endpoint impaired communications	MDE
Fix Microsoft Defender for Endpoint sensor data collection	MDE
Update Microsoft Defender Antivirus definitions in macOS	MDE
Turn on Microsoft Defender for Endpoint sensor	MDE
Enable EDR in block mode	MDE
Change service account to avoid cached password in Windows registry	MDE
Change service executable path to a common protected location	MDE
Disable SMBv1 client driver	MDE

Tasks / Effort	Platform
Turn on Tamper Protection	MDE
Use advanced protection against ransomware	MDE
Disable 'Configure Offer Remote Assistance'	MDE
Set controlled folder access to enabled or audit mode	MDE
Set 'Maximum password age' to '60 or fewer days, but not 0'	MDE
Update Microsoft Defender Antivirus definitions	MDE
Turn on real-time protection	MDE
Turn on PUA protection in block mode	MDE
Ensure BitLocker drive compatibility	MDE
Fix Windows Defender Antivirus cloud service connectivity	MDE
Turn on Microsoft Defender Antivirus	MDE
Resume BitLocker protection on all drives	MDE
Enable Microsoft Defender Antivirus real-time behavior monitoring	MDE
Enable Microsoft Defender Antivirus scanning of downloaded files and attachments	MDE
Turn on Microsoft Defender Antivirus real-time protection in macOS	MDE
Turn on Microsoft Defender Firewall	MDE
Enable Microsoft Defender Antivirus email scanning	MDE
Set Microsoft Defender SmartScreen Microsoft Edge site and download checking to block or warn	MDE
Set Microsoft Defender SmartScreen app and file checking to block or warn	MDE
Disable 'Store LAN Manager hash value on next password change'	MDE
Disable SMBv1 server	MDE
Enable Microsoft Defender Antivirus cloud-delivered protection in macOS	MDE
Disable the built-in Guest account	MDE
Disable 'Insecure guest logons' in SMB	MDE
Enable 'Safe DLL Search Mode'	MDE
Turn on all system-level Exploit protection settings	MDE
Enable cloud-delivered protection	MDE
Disable the built-in Administrator account	MDE
Set 'Remote Desktop security level' to 'TLS'	MDE
Disable 'Anonymous enumeration of SAM accounts'	MDE
Restrict anonymous access to named pipes and Shares	MDE
Disable 'Always install with elevated privileges'	MDE
Enable System Integrity Protection (SIP) in macOS	MDE
Set 'Reset account lockout counter after' to 15 minutes or more	MDE
Set 'Account lockout duration' to 15 minutes or more	MDE
Disable sending unencrypted passwords to third-party SMB servers	MDE
Enable Explorer Data Execution Prevention (DEP)	MDE
Block Flash activation in Office documents	MDE
Enable 'Limit local account use of blank passwords to console logon only'	MDE
Disable 'WDigest Authentication'	MDE
Enable 'Domain member: Digitally sign secure channel data (when possible)'	MDE
Enable Set 'Domain member: Digitally encrypt secure channel data (when possible)'	MDE
Enable 'Domain member: Digitally encrypt or sign secure channel data (always)'	MDE
Enable 'Domain member: Require strong (Windows 2000 or later) session key'	MDE
Disable 'Network access: Let Everyone permissions apply to anonymous users'	MDE
Disable 'Domain member: Disable machine account password changes'	MDE