Microsoft 365 and Azure Active Directory Information Security Best Practices

PONDURANCE

The following information is intended to provide common recommendations and is developed for informational purposes only. This guide is not designed to be comprehensive, and some recommendations may not be suitable to an organization based on its requirements and integration with additional business applications.

ENFORCE MULTIFACTOR AUTHENTICATION (MFA)

- Create and *enforce* an MFA registration policy for administrators (and eventually all users) using Azure Identity Protection. The policy will give applicable users 14 days from their next sign-in to register for MFA.

CONDITIONAL ACCESS POLICY FOR MFA

- Require MFA for all administrators by creating a Conditional Access Policy. Appropriate exclusions should be configured initially to avoid losing access to the tenant.
- Require MFA for all users by creating a Conditional Access Policy. Appropriate exclusions should be configured initially to avoid losing access to the tenant.

DEDICATED ADMINISTRATOR ACCOUNTS

- Dedicate Microsoft 365 administrator accounts for administration of the tenant only. These accounts should not be associated with an email address.

CREATE EMERGENCY ACCESS ACCOUNT

- Create a cloud-only administrator account that only has access to your *.onmicrosoft.com domain to prevent being accidently locked out of your Azure active directory. The account should be limited to emergency use. Emergency access accounts should be excluded from any Conditional Use Policy that would normally restrict access.

TRUSTED LOCATIONS

- Configure to allow a trusted range of IP addresses or restrict access from specific locations or countries

BLOCK LEGACY AUTHENTICATION

- Block legacy authentication for users not currently using these protocols by creating a Conditional Access Policy. Initially, to avoid user disruption, configure the policy in "report-only mode" so administrators can evaluate the impact the policy will have on existing users.
- Observe current legacy authentication usage by viewing sign-ins within the Azure portal using the following steps:
  - Navigate to Azure Active Directory > Sign-ins
  - Filter by Client App > check Other Clients and click Apply

BLOCK ACCESS FOR UNKNOWN/UNSUPPORTED DEVICES

- Use Conditional Access Policy to restrict access to organization resources when an attempt to login from an unknown/unsupported device is detected

RISK-BASED CONDITIONAL ACCESS

- Configure Azure Identity Protection (Azure Premium P2 license required) for a second factor of authentication is required based on the risk score associated with a sign-in event. Microsoft's algorithms calculate the risk score by tracking account behavior to identify anomalies such as unfamiliar locations, impossible travel, and anonymous IP address usage.

IDENTITY AND ACCESS MANAGEMENT

- Configure active directory-connect hash sync to protect on-premises active directory accounts
- Configure banned passwords
- Configure self-service password reset
- Customize smart lockout features in Microsoft 365
- Monitor and improve Microsoft Secure Score

DISABLE BROWSER PERSISTENCE

- Prevent a trusted session from an unmanaged device from remaining logged in after a web browser has been closed by the user. Require reauthentication after one hour.

ENABLE LOGGING

- Ensure logging is enabled for all accounts and test configuration by reviewing log entries. Enhanced logging features are available based on licensing that can allow for one year of retention.
- "Mail items accessed" logging feature will capture each event when an email or attachment is accessed in an account

SECURITY MONITORING, ALERTING, AND THREAT PREVENTION

- Monitor and review identity protection alerts for risky logins, risky users, and risk detections
- Enable and configure Azure Advanced Threat Protection (ATP)
- Review Microsoft 365 security and compliance center alerts
- Enhance anti-spam settings

INFORMATION PROTECTION AND DATA LOSS PREVENTION (DLP)

- Use Azure Information Protection, a cloud-based solution that allows organizations to automatically protect, analyze, and track on-premises and cloud data by applying labels
- Implement access controls that follow the principle of least privilege
- Educate users on how and where to store data throughout respective workflows
- Test Azure Information Protection unified labeling scanner for automated classification, labeling, and protection of supported on-premises files (requires Azure Information Protection P2 licensing)

SET EXTERNAL EMAIL WARNING

- Set a warning for external emails to alert users that the email comes from an external source

SPF, DKIM, AND DMARC FEATURES

- Utilize Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) as anti-spoofing and email authentication techniques that use domain name system records to validate the sender of an email

PONDURANCE

SAFE LINKS

- Use the safe links feature to mitigate phishing attempts. The links sent in an email are initially scanned by Windows Defender and rewritten in the email. After a user clicks a link, the user is routed to a Microsoft website that checks the validity before redirecting the user to the intended destination.

CONDITIONAL ACCESS "WHAT IF" TOOL

- Allow an administrator to test a Conditional Access Policy before implementation by using this feature

TERM OF USE POLICY

- Establish a Term of Use Policy that is presented to employees and/or guests before granting access to the tenant

SECURITY AWARENESS TRAINING

- Provide continuous education to users on how to recognize tactics and techniques used by cybercriminals. Employees should have a central reporting contact to report suspicious emails.

HOW PONDURANCE CAN HELP

Our mission is to ensure that every organization is able to detect and respond to cyber threats — regardless of size, industry, or current in-house capabilities. We combine our advanced platform with decades of human intelligence to decrease risk to your mission.

CLOSED-LOOP MANAGED DETECTION AND RESPONSE

Recognized by Gartner, Pondurance provides 24/7 U.S.-based security operations center services powered by analysts, threat hunters, and incident responders who utilize our advanced cloud-native platform to provide you with continuous cyber risk reduction. By integrating 360-degree visibility across log, endpoint, and network data and with proactive threat hunting, we reduce the time it takes to respond to emerging cyber threats.

Pondurance Managed Detection and Response is the proactive security service backed by authentic human intelligence. Technology is not enough to stop cyber threats. Human attackers must be confronted by human defenders.

INCIDENT RESPONSE

When every minute counts, organizations need specialized cybersecurity experts to help them respond to a compromise, minimize losses, and prevent future incidents.

Pondurance delivers digital forensics and incident response services with an experienced team capable of assisting your organization and legal team every step of the way. This includes scoping and containing the incident, determining exposure through forensic analysis, and providing confidence to continue normal business operations.

SECURITY CONSULTANCY SERVICES

Our specialized consultancy services will help you assess systems, controls, programs, and teams to uncover and manage vulnerabilities. Our suite of services ranges from penetration testing to red team exercises, along with compliance program assessments for highly regulated industries. We provide security incident response and business continuity planning to put you in the best position to defend against and respond to cyberattacks.

CONTACT US

Emergency IR Hotline: 888.385.1720
Email: dfir@pondurance.com

pondurance.com