the ame group

# MICROSOFT 365 SECURITY

[requires an active FLEX agreement]

Microsoft cloud security feature implementation and configuration is critical to securing your data and protecting systems.

Continuous monitoring of changes, security feature functionality, and operational metrics provide the information needed to make sound security or operational decisions based on potential risk.

## ENGAGE THE SECURITY TEAM

- Monthly Security Risk Assessment for M365
- Evaluate the configured security features available in Azure AD and Microsoft 365
- Review Findings and Recent Security Events
- Recommend ways to strengthen your business security posture
- Provide evidence of security implementations
- Use Advanced Security Tools for Continuous Monitoring, Reporting and Alerting

## TAKE ACTION

### PREVENT

Recommend Security Controls to Implement

### MONITOR

Continuous M365 Security Monitoring 24/7/365
Security Information and Event Monitoring (SIEM)
Threat Monitoring and Detection

### RESPOND

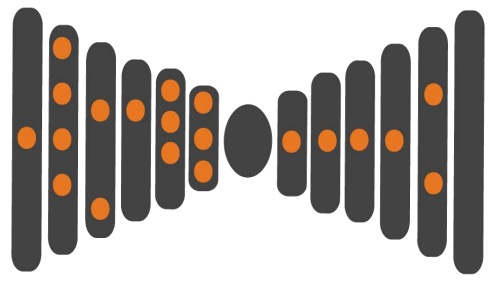
Triage Security Alerts and Reported Incidents
Respond to Priority Alerts 24/7/365

### REPAIR

Recommendations by Security Team
Remediation of M365 Vulnerabilities by Service Team

## STOP THREATS BEFORE THEY TAKE DOWN YOUR BUSINESS

**Example of Items Monitored**
New Global Admins
Permission Changes
Abnormal File Uploads / Downloads
Users Signing in from Unusual Locations
Third Party Access & Permissions
Changes to Mail Flow
Sharing Files with External Users
Inactivating Users
Implement New Security Features Available



### LAYERS OF SECURITY

Ensuring security across all layers of your network, from employees to the public. At each level of your organization and network, implementation of controls should address Physical, Technical and Administrative Security. Cloud Business App Security is a critical layer of protection and detection.

### WHAT IS MONITORED IN M365?

Email
SharePoint
Teams
Azure AD

### WHAT DOES SECURITY POSTURE MEAN?

Your business' overall level of readiness and preparedness to defend against potential security threats and attacks.

### SECURITY INFORMATION & EVENT MONITORING

SIEM is the cornerstone of threat detection practices. Log collection from multiple sources, network traffic analysis, and system events are aggregated and used to conduct threat hunting.

### DEDICATED SECURITY TEAM

The AME Group delivers managed IT services independently of the managed security services team. The security team has advanced security training and is independent of the service team. All AME staff are employees directly and services are not outsourced.

**CONTACT YOUR STRATEGIC ADVISOR TO LEAN MORE ABOUT CYBERSECURITY AND OTHER LAYERS OF PROTECTION.**