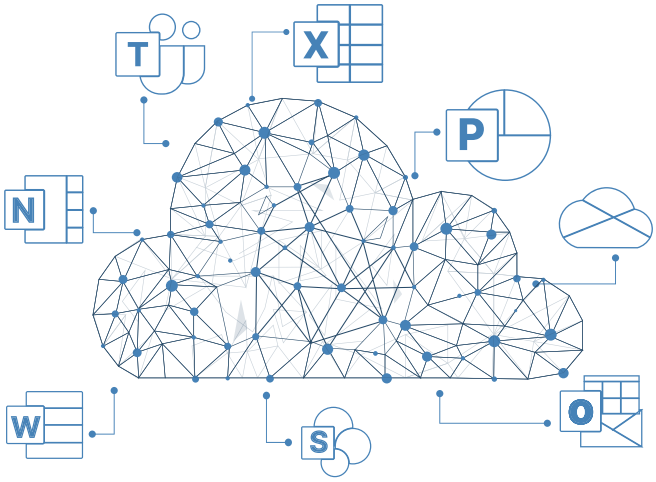
InfoSight®
www.infosightinc.com

M365 SECURITY ASSESSMENT

305-828-1003 info@infosightinc.com

Overview - The Challenge

Microsoft 365 (M365) is hands down the most common set of cloud-based business applications used by most organizations, and this makes it a primary target for attackers. M365 security presents several challenges that organizations need to address to protect their data, because although cloud providers have robust security measures, misconfigurations or weak access controls can be exploited by bad actors. M365 security is a shared responsibility model with default configurations set in favor of open, collaborative working, but secure configuration remains the customer's responsibility.



How We Solve It

We'll assess your M365 environment and provide security recommendations for:

- Authentication, Access, and Identity Management
- Auditing & Logs
- Email Security and Content Management
- Application Permissions
- Data Storage Management
- Mobile Device Management

InfoSight®
www.infosightinc.com

M365 SECURITY ASSESSMENT

The Outcome

Monthly or one-time assessment Microsoft Cloud environment scan and risk report.

Monthly or one-time assessment Microsoft Cloud management plan to mitigate any discovered risks.

Audit trail report documenting all changes to the environment and who made them.

Microsoft Secure Score trend report that compares your business security against benchmarks.

Optional ongoing analysis of cloud environment structure, performance and security.

From data protection and cybersecurity challenges to business continuity and cost control, understanding your M365 cloud environment is key to your organization achieving its business goals.

Digital reports are delivered via our proprietary **Mitigator Vulnerability and Threat Management Platform.** Reports can be exported in multiple formats and printed.

MITIGATOR™
VULNERABILITY & THREAT MANAGER

Other Assessments

Penetration Testing & Vulnerability Assessments

Consists of a multi-disciplinary, multi-faceted review of the organization's systems which identifies vulnerabilities outside and inside the network and attempts to exploit any vulnerabilities in the same way a malicious actor would.

Red, Blue & Purple Team Testing

Designed to test an organization's readiness to detect, withstand and respond to a targeted attack. The red team's goal is to find and exploit any identifiable weaknesses in the organization's security as the blue team works to defend the organization by finding and patching vulnerabilities and responding to successful breaches.

Code Review, Mobile & API Testing

Involves the security testing of web, mobile, and software application interfaces to identify privilege escalation, authorization creep, and security controls bypass. It includes a detailed report outlining discovered vulnerabilities and remediation steps.

Social Engineering

Encompasses comprehensive security tests conducted to establish the current state of security among the organization's personnel. It identifies vulnerabilities within human resources as well as gaps in awareness training. Social Engineering assessments are performed against electronic messaging, telephony and other onsite and human vectors.