

# Microsoft 365 Security Assessment

85% of Organizations Using Microsoft 365 Have Suffered Email Data Breaches according to [Egress](#).

Leveraging a combination of automated scanning and manual testing based in the CIS Microsoft 365 Foundation Benchmarks, NetSPI uses commercial, open source, and proprietary software to assess and identify Microsoft 365 security vulnerabilities and misconfigurations.

## NetSPI's 5 Steps to M365 Security Assessments

- 1 Automated Configuration Gathering** – Review Microsoft 365 and Azure Active Directory (Entra) configurations using a provisioned user account and automated tooling.
- 2 Manual Configuration Gathering** – Perform manual testing, conduct employee interviews, and confirm key business use cases for specific configurations.
- 3 Configuration Analysis and Vulnerability Enumeration** – Analyze gathered configurations for common best practices in alignment with CIS Microsoft 365 Foundation Benchmarks and additional security checks derived from NetSPI's years of testing.
- 4 Vulnerability Enumeration: Manual Verification** – Identify exploitable and significant vulnerabilities through manual verification of medium and high severity issues.
- 5 Reporting** – After discovering strengths and weaknesses of your Microsoft 365 environment, NetSPI will provide strategies for improvement and prioritize deficiencies based on potential business impact and likelihood of process failure or exploitation. Notable findings will then be analyzed and compared against program goals and compliance requirements.

### Provides Insights into:

- ◆ **Identity & Access Management** – Ensure that only authorized people have access.
- ◆ **Data Management** – Protect every form of data in your possession.
- ◆ **Data Storage** – Protect not only your data, but also where it is stored.
- ◆ **Email Security** – Protect from unauthorized access through email account attack vectors.
- ◆ **Account Protection** – Maintain integrity and confidentiality of account information.
- ◆ **Password Protection** – Ensure password best practices are followed.
- ◆ **Integrations** – Validate security of third-party integrations.

### Delivered in NetSPI's PTaaS Platform

- ◆ **Real-time Reporting** – Get notified of vulnerabilities in platform as they are found.
- ◆ **Remediation Guidance** – Vulnerabilities are delivered with remediation instructions and consultant support.
- ◆ **Project Management & Communication** – Effortlessly assign responsibilities, track remediation status, communicate with teams, and more.
- ◆ **Track & Trend Data** – Analyze findings and discover trends over time.













To learn more about NetSPI's SaaS Security Assessments, or any of our other offensive security solutions, visit [www.netspi.com](http://www.netspi.com) or [contact us](#).

## About NetSPI

NetSPI is the global leader in offensive security, delivering the most comprehensive suite of penetration testing, attack surface management, and breach and attack simulation solutions. Through a combination of technology innovation and human ingenuity NetSPI helps organizations discover, prioritize, and remediate security vulnerabilities. Its global cybersecurity experts are committed to securing the world's most prominent organizations, including nine of the top 10 U.S. banks, four of the top five leading cloud providers, four of the five largest healthcare companies, three FAANG companies, seven of the top 10 U.S. retailers & e-commerce companies, and many of the Fortune 500. NetSPI is headquartered in Minneapolis, MN, with offices across the U.S., Canada, the UK, and India.

## Global Leader in Offensive Security

RESOLVE | EAS | ASM

-  Application Pentesting
-  Cloud Pentesting
-  Network Pentesting
-  IoT Pentesting
-  Secure Code Review
-  Cybersecurity Maturity Assessment
-  Red Team Testing
-  Social Engineering
-  Blockchain Pentesting
-  SaaS Security Assessment