

Securing Microsoft 365

Moving your business into Microsoft 365 isn't just upgrading your email — it's opening the door to powerful collaboration tools, mobility, and automation. But with that comes new risks: phishing, account takeovers, unauthorized access, and misconfigurations.

We help you secure your Office 365 environment end-to-end so your email, users, files, and identities stay protected — with zero disruption to your business.

Why Securing Office 365 Matters for Your Business?

- ✓ Email is the #1 target for phishing and ransomware
- ✓ Attackers abuse weak MFA, outdated policies, and user consent prompts
- ✓ Misconfigured mail rules can silently forward sensitive emails
- ✓ Business email compromise (BEC) happens due to identity misuse
- ✓ Legacy authentication allows attackers to bypass MFA
- ✓ Poorly configured Teams, SharePoint, and OneDrive expose data

Did you know?

Over 85% of Microsoft 365 breaches start with a compromised email account — not a server.



85%



Before You Can Protect It, You Have to Understand It

Our Approach to Securing Office 365

We follow a clear, structured security process:

📌 Identity Hardening (Most Important Layer)

- ✅ Assess your current Microsoft 365 configuration
- ✅ Identify gaps in identity, email, Teams, and SharePoint security
- ✅ Deploy strong Microsoft 365 security policies
- ✅ Harden all admin roles and disable insecure authentication
- ✅ Implement monitoring, alerts, and monthly reporting

🌟 Hackers target email, MFA, Teams, SharePoint, and weak admin settings every day. We lock down your Microsoft 365 environment so your users, email, files, and business stay protected.



Did you know?

Most businesses leave legacy authentication ON, which allows hackers to bypass MFA completely.

100%

Before You Can Protect It, You Have to Understand It

How We Secure Your Office 365 Environment

We use a structured, proven security framework specifically built for Microsoft 365.

✦ Identity Hardening (Most Important Layer)

- ☒ Enforce strong MFA everywhere
- ☒ Implement Conditional Access to block risky logins
- ☒ Disable legacy authentication
- ☒ Lock down global admin accounts
- ☒ Create privileged admin roles with proper separation

✦ Email & Exchange Online Protection

- ☒ Disable external forwarding rules
- ☒ Enable anti-phishing, anti-malware, and anti-spam policies
- ☒ Protect shared mailboxes (block sign-in, use delegated access)
- ☒ Monitor for suspicious inbox rules and auto-forward attacks



Did you know?

Attackers often break in by setting hidden inbox rules that forward your emails to external accounts.



100%

User App & Consent Control

- Block unauthorized app consent
- Restrict third-party apps from accessing corporate data
- Enable admin review workflow for app requests

Teams & Collaboration Security

- Block external Teams messaging (unless approved)
- Restrict external calendar sharing
- Limit external file sharing from OneDrive/SharePoint
- Monitor guest access and external sharing links

Monitoring, Logging & Alerts

- Enable Microsoft 365 audit logging
- Forward logs to SIEM or SOC for 24/7 monitoring
- Detect unusual authentication behavior or high-risk logins
- Track device sign-ins and suspicious MFA prompts

Compliance & Data Protection

- Enforce Data Loss Prevention (DLP)
- Enable safe attachments & safe links
- Apply retention policies for email and files
- Protect sensitive files with sensitivity labels



Did you know?

A single misconfigured mailbox can leak thousands of emails without anyone noticing.



100%

GET IN TOUCH

Partner with Experts Who Secure
Your Business



CONTACT US



212-219-2422
407-502-8881



www.netsectechnologies.com



info@netsectechnologies.com

★ Our Advantages

We bring deep expertise in Palo Alto Networks, cloud security, and network architecture—all guided by a business-first approach focused on practical outcomes.

Our solutions are tailored, secure, and scalable, backed by responsive support and real-world experience across diverse industries..

ABOUT US

NetSec Solutions is a business solutions provider based in New York and Florida, specializing in Palo Alto Networks, cloud security, next-generation firewalls, and advanced network protection.

We support clients across a wide range of industries—including legal, healthcare, education, finance, and government—helping them secure critical infrastructure, ensure compliance, and stay ahead of emerging threats.

**Secure Your Future with Trusted
Cybersecurity Experts**



1

✓ Expertise that matters

Certified specialists in Palo Alto, cloud, and advanced security.

2

✓ Security at every layer

From firewalls, routers, switches, to the cloud, we cover it all.

3

✓ Fast responsive support

We're here when you need us — no waiting

4

✓ Tailored for your business

Custom solutions for law, healthcare, education, and more.