CYBERSECURITY ASSESSMENT

Synoptek

Microsoft Security Control Plane Assessment

Enterprise-Grade Cybersecurity for the Midmarket

Identity-driven breaches account for the majority of modern cyber incidents. Misconfigured access controls, privilege sprawl, and unenforced endpoint baselines create accelerated ransomware pathways.

A typical engagement is delivered over 3–5 weeks. It includes discovery workshops and stakeholder alignment, Microsoft Secure Score baseline review, tenant configuration analysis, and framework mapping, risk ranking, with a final executive readout and detailed report.

ASSESSMENT OVERVIEW

Synoptek's Microsoft Security Control Plane Assessment is a structured, framework-aligned security maturity evaluation focused on:

- Identity enforcement
- Cloud governance (Azure & Microsoft 365)
- Endpoint configuration posture

This engagement provides a defensible, evidence-based baseline and a prioritized remediation roadmap aligned to recognized security standards.

APPROACH TO THE ASSESSMENT

- Configuration-driven
- Evidence-based
- Framework-aligned
- Risk-prioritized
- Non-intrusive (no production disruption)

***This is not a penetration test or a full compliance audit. It is a strategic security maturity baseline.**

WHAT IS IN SCOPE

Identity & Access Management (Core Pillar)

- MFA enforcement coverage
- Conditional Access design & segmentation
- Privileged role governance
- Legacy authentication exposure
- Guest access governance
- Authentication method strength
- Access review & lifecycle maturity

THE OUTCOMES YOU CAN EXPECT IFYOU IMPLEMENT RECOMMENDATIONS IN ASSESSMENT INCLUDE:

- Identify identity-driven breach paths
- Quantify enforcement gaps
- Reduce ransomware exposure
- Improve audit readiness
- Accelerate Zero Trust maturity
- Enable vCISO-led executive risk discussions

Cloud Control Plane (Azure & M365 Governance)

- Subscription governance & ownership clarity
- RBAC privilege distribution
- Defender for Cloud posture maturity
- Secure Score analysis
- Monitoring & alerting maturity
- Configuration drift risk
- Identity-cloud integration validation

Endpoint Configuration & Hardening

- Defender posture & ASR enforcement
- Credential protection validation
- Firewall enforcement
- BitLocker encryption validation
- Device trust & hybrid join validation
- Secure baseline coverage

Framework Alignment

Findings are mapped to:

- NIST Cybersecurity Framework (CSF)
- Zero Trust Maturity Model (CISA/NIST)
- ISO 27001 Annex A
- SOC 2 Security & Logical Access
- CCPA safeguards

Optional industry-specific overlays available (HIPAA, PCI-DSS, CMMC, etc.)

WHAT IS NOT INCLUDED

This assessment does not include:

- Vulnerability scanning or penetration testing
- Firewall rule review
- Application code review
- Secure SDLC assessment
- Full GRC or policy audit
- BCP / DR testing
- Security awareness program review

These services can be separately scoped if required.

DELIVERABLES

Each engagement produces:

- Executive Summary of Current Security Maturity
- Detailed Gap Analysis Workbook
  - Your performance mapped to industry frameworks
  - Vulnerabilities and priority investments ranked according to risk (High / Medium / Low)
- Prioritized Remediation Roadmap
- Executive Readout Presentation
- Technical Appendix (Evidence Artifacts)
- Optional: Ransomware Resilience Advisory Module

Deliverables are audit-defensible, board-consumable, and technically actionable.