Microsoft 365 Tenant Security Hardening

Liquid Mercury Solutions' Standard Information Sheet and Engagement Task List for Our Microsoft 365 Security Configuration Offerings

Compare Our Microsoft 365 Tenant Security Hardening Offers

Find the right engagement to fit your needs and budget.

Deliverable	Essential	Standard	Advanced	Enterprise
Engagement Timeframe	1 Day	3 Days	5 Days	10 Days
Security Briefing	20 min	40 min	60 min	90 min
License Review	Yes	Yes	Yes	Yes
Privileged Logins	Yes	Yes	Yes	Yes
Universal Auditing	Yes	Yes	Yes	Yes
E-mail/File Retention Policies (Defaults)	Yes	Yes	Yes	Yes
Defender ATP for Office 365 (Defaults)	Yes	Yes	Yes	Yes
Anti-spam/spoof: DKIM and DMARC (Defaults)	No	Yes	Yes	Yes
Identity Protection Policies (Defaults)	No	Yes	Yes	Yes
Self-service Password Reset	No	Yes	Yes	Yes
Universal MFA (Defaults)	No	Yes	Yes	Yes
Whitelisted IP Addresses	No	Yes	Yes	Yes
Secure E-mail Messaging Rules	No	Yes	Yes	Yes
Disable Legacy Client Access (Defaults)	No	Yes	Yes	Yes
Defender ATP for Endpoints (Defaults)	No	Yes	Yes	Yes
Enterprise Password Management (Trial)	No	Yes	Yes	Yes
Conditional Access Policies	No	No	Yes*	Yes
Break Glass Recovery Login	No	No	Yes	Yes
MFA Adoption (Custom)	No	No	Yes*	Yes
Trusted Locations (Custom)	No	No	Yes	Yes

Anti-spam/spoof: Custom mail sender/IP for SPF, DKIM, and DMARC configuration	No	No	Yes	Yes
Defender ATP for Office 365 (Custom)	No	No	Yes*	Yes
Defender ATP for Endpoints (Custom)	No	No	Yes*	Yes
Threat Intelligence / Simulation Walkthrough	No	No	Yes	Yes
Password-less Authentication (smartphone and Yubikey based login)	No	No	Yes	Yes

* Subject to fair use limitations based on number of users, hours required, etc. Ask your Account Executive whether Advanced or Enterprise level engagement is the best for your needs.

Other Available Security Offerings Not Covered in Packaged Engagements

Security and Compliance Briefings

- 360 Degrees of Defense: Microsoft 365 Cybersecurity Stack
  Leveraging the MS365 Stack to Stop Hackers Cold
- Factors Affecting the Choice Between GCC, GCC High, and Hybrid Approach
- Understanding the Shared Responsibility Model for MS365 and NIST Compliance
- SEIM Solutions

Workshops & Implementations

- Intune Jump Start
- Threat Simulation
- Cloud App Protection
- Defender ATP for Identity (Azure ATP)
- Hello for Business
- Seamless SSO
- Endpoint Manager (Intune) Deployment
- Deploying Office 365 to Stateless VMs for Secure VDI

Got What It Takes? Check Our Microsoft 365 Licensing Matrix

Know if you already have what you need to get secure, or if you must buy something extra.

Security Feature	Plans for IT/admins	Plans for end-users
Overall security readiness	Microsoft 365 E5, EMS E5, or combination of Plan 2 for DATP Endpoint, DATP Office 365, and Azure AD Premium	Microsoft 365 E3 / Business Premium, EMS E3, or combination of Plan 1 for DATP and Azure AD Premium

Mail and File Retention Policies	Mail enabled plan such as Office 365 F3 or Exchange Online Plan 1	Office 365 E3 or E5, AIP (Azure Rights Management)
Secure E-mail Messaging	Mail enabled plan such as Office 365 F3 or Exchange Online Plan 1	Office 365 E3 or E5, AIP (Azure Rights Management)
Identity Protection	Microsoft 365 E5, EMS E5, or Azure AD Premium Plan 2	Microsoft 365 E3 / Business Premium, EMS E3, or Azure AD Premium Plan 1
Conditional Access Policies	Microsoft 365 E5, EMS E5, or Azure AD Premium Plan 2	Microsoft 365 E3 / Business Premium, EMS E3, or Azure AD Premium Plan 1
Universal MFA Adoption	Basic: Office 365; Advanced: Microsoft 365 E5, EMS E5, or Azure AD Premium Plan 2	Basic: Office 365; Advanced: Microsoft 365 E5, EMS E5, or Azure AD Premium Plan 2
Defender for Office 365	Microsoft 365 E5, EMS E5, or combination of Plan 2 for DATP Office 365	Microsoft 365 E3 / Business Premium, EMS E3, or Plan 1 for DATP
Defender for Endpoints	Microsoft 365 E5, Windows 10 E5, or Defender ATP for Endpoints	Microsoft 365 E3 / Business Premium, EMS E3, or Plan 1 for DATP