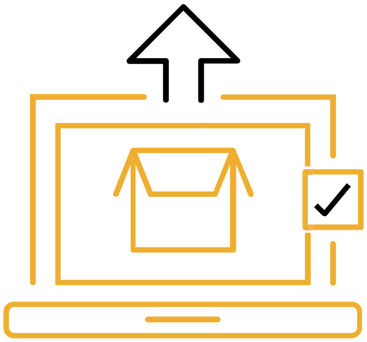
Lodestone

SERVICE BRIEF FOR EMAIL HARDENING ASSESSMENT



Lodestone Email Hardening Assessment targets Microsoft 365 (M365) tenants, in particular, to reduce risk by proactively reviewing and addressing common misconfigurations. M365 is a highly targeted resource by threat actors due to its prevalence as a business solutions service and value if infiltrated. A compromised M365 tenant can allow threat actors to remotely access sensitive and business-critical data, even without the need to breach your network's actual perimeter.

We work with you to identify risks in the most critical component of your M365 tenant: its security configuration. Our experts offer solutions that align with your business needs and help you optimize security and increase visibility into events occurring in a critical part of your workflow.

Lodestone's email hardening assessment is a structured engagement designed to help you understand your security posture within the context of what is often one of the most frequently used components of a business: the M365 tenant. We identify gaps and misconfigurations and connect with your personnel to create a customized roadmap for security controls that will reduce your risk of compromise.

We evaluate your organization's M365 tenant against the following security control areas:

- Account/Authentication
- Application Permissions
- Data Management
- Email security / Exchange Online
- Data security and storage
- Auditing
- Mobile device management (MDM)

Included in our findings are recommendations that balance industry best practices with your organization's productivity needs.

BENEFITS

- Identification of potential security challenges and their risks to your organization, including misconfigurations that could leave data exposed or susceptible to unauthorized access.
- Improvement of security posture through configuration evaluation and recommendations on security hardening and best practices.
- Insight into your current M365 tenant, including a high-level overview of your current configuration.

METHODOLOGY

As part of our email hardening assessment, Lodestone consultants will review your M365 configurations and settings for critical security control areas.

The Email Hardening Assessment is comprised of these primary phases:

- Initial Consultation – A brief overview of what the email hardening assessment entails, where we walk you through the security controls that will be assessed and how we will conduct the assessment.

- Configuration Review – We provide a thorough configuration review of your M365 tenant to ensure that security configurations follow industry guidelines and are optimized to your business's unique needs.

- Reporting – We provide a written final summary of the email hardening assessment with an executive summary of the engagement and a detailed description of the findings and any remediation procedures to better protect your M365 tenant.

- Report Review – We provide our clients at least two weeks to review the reports and formulate any questions or requests for clarification. At the end of every engagement, a report review call is scheduled to ensure that all of your concerns are addressed.

DURATION AND DELIVERABLES

An email hardening assessment takes approximately one week. As part of the engagement, Lodestone will provide the following:

Lodestone will provide the following deliverables to you as part of the engagement:

- Executive Summary Report – This report will provide a high-level overview of the process, methodology used, and overall risk to the organization based on the results of the assessment of your M365 tenant.
- A snapshot of the existing M365 security configurations.
- Prioritized and detailed recommendations for further hardening your organization's M365 tenant.
- An executive debriefing call to discuss findings and provide clarity on any lingering questions or concerns.

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specializing in incident response, digital forensics, offensive security, risk management, and threat detection.