Lodestone

SERVICE BRIEF FOR

MICROSOFT 365 EMAIL HARDENING

Lodestone's Microsoft 365 (M365) Email Hardening is designed to help defend your business against one of the most prolific and disruptive security incidents companies face: business email compromises (BECs). These incidents can result in the loss of important data, trust from your clients, and even direct monetary loss. Armed with real-world insight from our Incident Response team, our engineers have studied the ins and outs of one of the most popular email solutions, M365.

Our experts partner with your personnel to configure a more secure M365 environment with policies and procedures that help reduce the likelihood of your company experiencing a BEC.

BENEFITS

- Enabling secure, remote collaboration to bring your business into the future while reducing risk.
- Utilizing cloud storage with the configurations that best suit your business needs and keep your data safe.
- Allowing authorized users to increase their productivity by accessing data from anywhere while safeguarding against would-be attackers.

OVERVIEW

Lodestone's M365 Email Hardening helps ensure that your cloud collaboration platforms follow security best practices to deter threat actors attempting phishing attacks or BECs. Due to rapid rollouts, businesses often do not have the time or resources to thoroughly evaluate security configurations natively available, instead relying on defaults. However, this can make them low-hanging fruit for some of the most prolific types of cyberattacks.

The information gathered is compiled into a report that empowers your company to strengthen its security posture with customized configurations that make the most of your M365 resources. By optimizing these resources and adhering to industry best practices, our experts help your business work better and more safely.

WHY LODESTONE

Lodestone is a global cybersecurity firm committed to helping clients prevent, investigate, and prepare for security incidents. It was built from the ground up to offer an innovative, behavior-based approach to proactive cybersecurity and digital forensics and incident response (DFIR). We are comprised of top investigative talent and offensive security experts from several of the world's largest cybersecurity firms, as well as military veterans and former members of national security organizations, including the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). We combine this expertise with our unique understanding of legal requirements through our relationship with our parent company, Beazley, which has been at the forefront of cyber insurance for over a decade. Through this relationship, Lodestone has developed a unique understanding of the intersection between insurance and cybersecurity while preventing, preparing for, and responding to some of the toughest security challenges that industries face today.

Compliance
Since its founding as a subsidiary of Beazley in 2017, Lodestone has offered its customers insight into both cybersecurity and the cyber insurance industry. We help companies align and stay compliant with cyber insurance coverage requirements. In addition, we offer discounts to channel partners to form long-term relationships.

Security Focus
Lodestone's experts live and breathe cybersecurity and are committed to helping customers face some of the biggest challenges of their careers. We do not sell vendor security products – our offerings are purely service-focused, and any third-party tools we recommend are the product of genuine, vendor-agnostic, and tested endorsement, not business deals.

Expertise
Lodestone's approach to Incident Response is to have the top cybersecurity experts in the world, as the lead, and as the touchpoint, when responding to cybersecurity incidents. This is done with the backing of comprehensive, real-time threat intelligence to provide clients with protection across the life cycle of a potential security event or incident.

Tailored Approach
We understand the individual challenges of every situation and consider the human side of the equation, never taking a "one size fits all" approach. We blend design, threat intelligence, and technology with human insights to provide clients with the greatest cybersecurity advantage.

Threat Intelligence
Our deep understanding of threat actor tactics, techniques, and procedures (TTPs) is based on decades of experience in DFIR and the diligent gathering of threat intelligence from all possible sources.

Agility
Time is of the essence before, during, and after an intrusion. We stand ready to move in quickly and effectively at the first sign of an intrusion.

Team Experience

1000+
ENGAGEMENTS

200+ YEARS
COMBINED EXPERIENCE

50+
CERTIFICATIONS

Experts Unlike Anyone Else

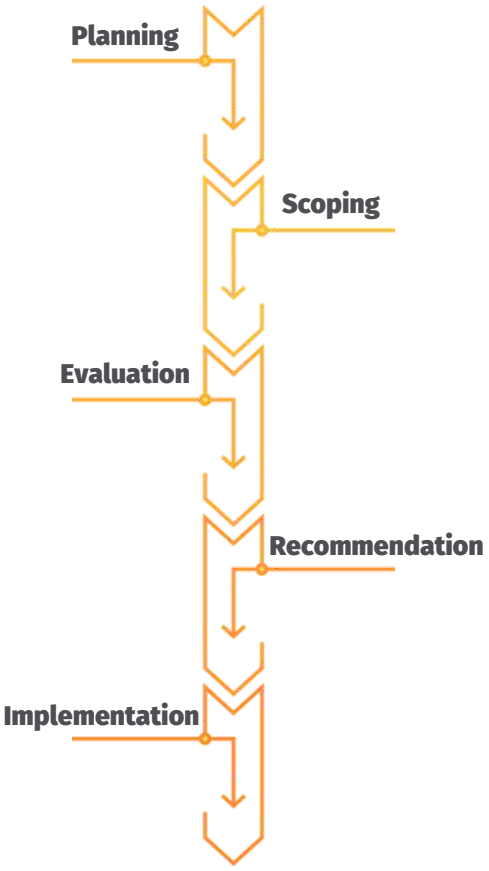
EX-
MILITARY
LAW ENFORCEMENT
INTELLIGENCE
TOP CYBER TECH
TOP CONSULTING
FORTUNE 100 ENTERPRISE

Global Presence - NA/Europe

METHODOLOGY

Lodestone's M365 Email Hardening helps balance convenient deployment and collaboration capabilities with secure practices and configurations to defend your company against increasingly common types of cyberattacks. The goal is to strengthen your security posture without impeding the day-to-day business flow.

Lodestone employs a standard methodology that includes multiple phases:



- Planning - Gathering details on your business and its unique needs and requirements for collaboration platforms. This includes minimizing the disruption that may result from altering existing configurations. It also may involve any regulatory standards your business is required to meet to protect its own or its customers' data.
- Scoping - Lodestone engineers collaborate with your company's IT personnel to identify the uses of M365 that best serve your business and its personnel. We work with you to ensure your environment balances productivity with security. We also identify the collaboration tools currently in place and their connections to your M365 tenant.
- Evaluation - Once Lodestone experts have pinpointed the backup requirements your company needs to meet, along with understanding your business flows, we work with you to understand the existing email policies and configurations in place. We develop a clear snapshot of your current setup in comparison to your unique needs.
- Recommendation - From minor alterations to major overhauls, Lodestone experts provide detailed solutions to help your company satisfy its objectives and secure or enhance M365. We provide an overview of the best practices that can boost the effectiveness of your M365 tenant and its ability to deter threat actors.
- Implementation - Lodestone engineers partner with your personnel to deploy new devices or update configurations based on customized and best practices recommendations. We provide you with step-by-step documentation of our actions so that your resources are focused on putting the best M365 configuration for your company into service.

DURATION AND DELIVERABLES

The delivery of Lodestone M365 Email Hardening varies in duration based on the size of the environment and resources required as determined during the scoping process.

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

- Best Practices and Recommendations Overview – A list that combines industry best practices and expert observations of your environment to help you strengthen your security posture.
- Implementation Documentation – A detailed documentation of the actions our engineers take to deploy configurations or devices to improve your M365 tenant.

Learn more at www.lodestone.com

Connect with us:

320 East Main Street, Lewisville, TX 75057, USA

Tel: +1-203-307-4984

info@lodestone.com