Lodestone
Navigating
Cyber Risks
Introducing Lodestone

Lodestone is a cyber security company focused on reducing risk.

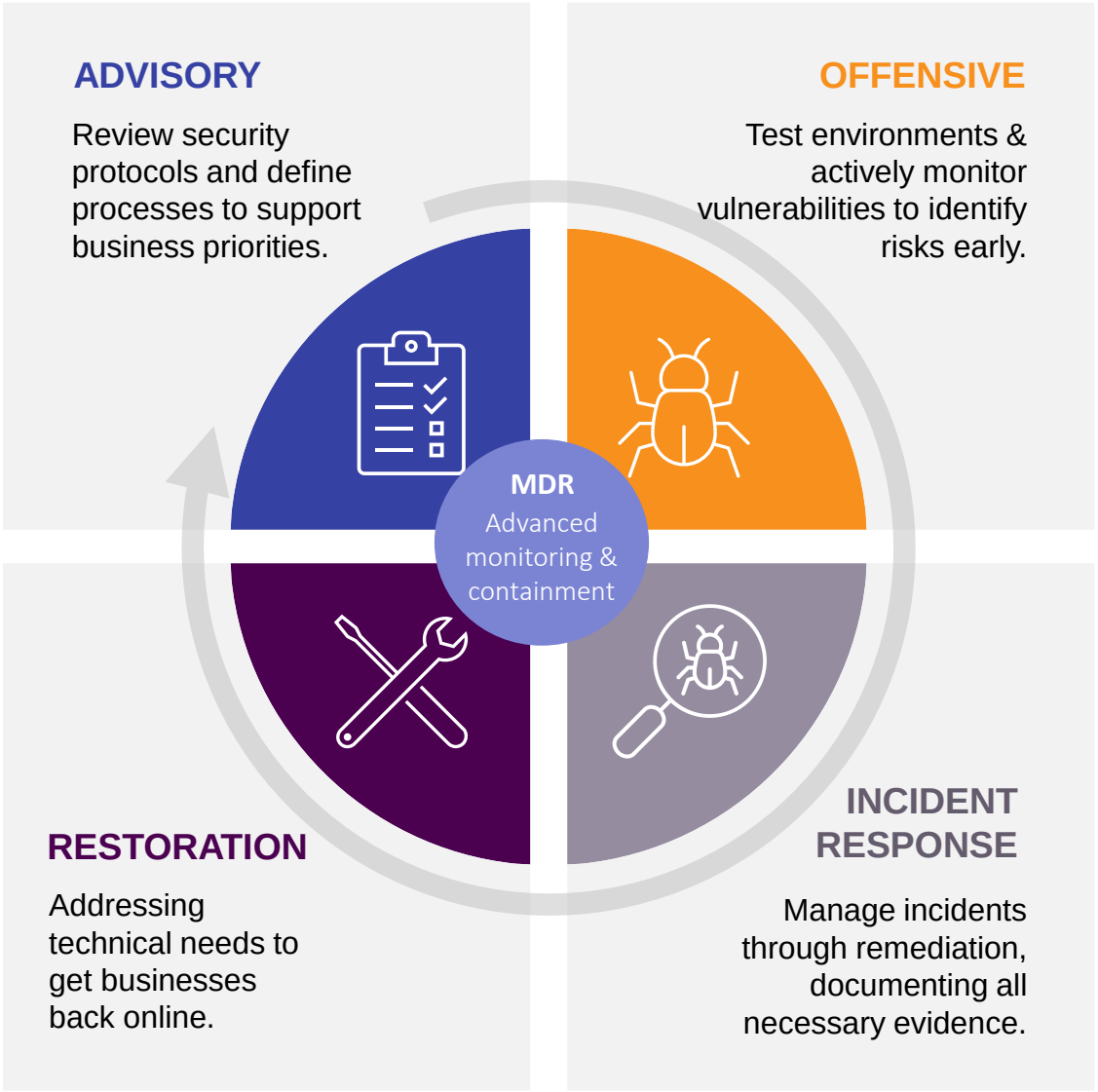
- **Founded in 2017 by Beazley Insurance**
  to improve the cyber claims experience
- **Expanded Focus in 2023**
  to include services that reduce risk, using data from thousands of incidents to improve resilience
- **100% Client Focused**
  tailoring our solutions to meet the individual challenges of clients
- **Fast, Flexible, and Experienced Teams**
  proven effective with high client satisfaction

Our Services Are Tuned To The Client Journey

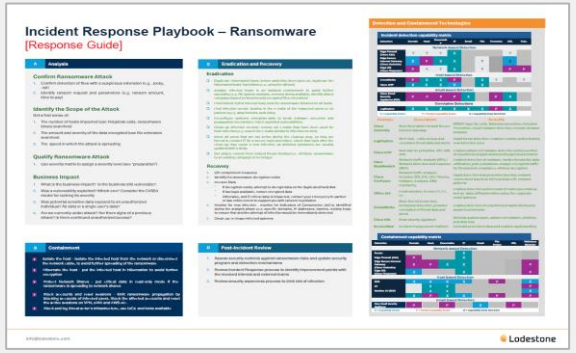
From Proactive Preparations to Continuous Monitoring or Rapid Response, Lodestone has you covered.

We prescribe solutions that:

- Reduce Risk
- Validate Controls
- Monitor & Respond
- Improve Resilience



Incident Response Plan Development



Ransomware Readiness Overview

Incident Response Plan
BCP/DR Plan
Ransomware Playbook

- Core Documentation Review
- Alternative Work Strategies
- Supplier and Vendor Continuity
- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

Discussion on key security controls:
Account Management, Vulnerability Management, Email & User Security, etc

- Defined and refined access control measures to restrict and monitor user access appropriately
- Outlined strategies for timely patching of systems and software to address vulnerabilities.
- Implementation of principle of least privilege to minimize potential security risks.

Backup Architecture and Strategy

Backup and recovery procedures

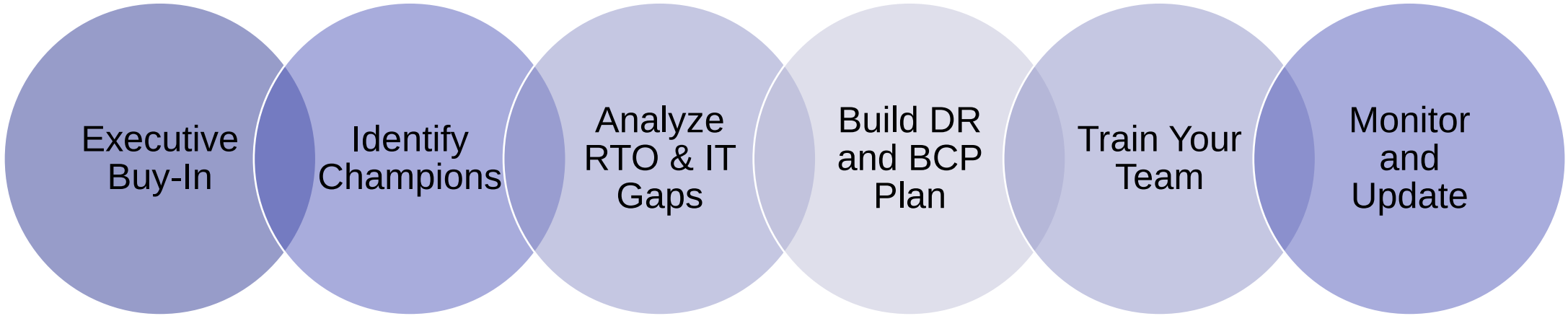
- Air-Gapping Strategy
- Network Segmentation
- Data Encryption
- Access Controls
- Offsite Storage Strategy
- Cloud Integration

Active Directory Review
OSINT Review

- *AD Review Requirements*
- Evaluation of AD structure, domains, and trusts.
- Review of group memberships and permissions.
- What can an attacker discover about an organization

Business Continuity Plan Development

Disaster Recovery (DR) and Business Continuity Plan (BCP) Development involves multiple key steps to ensure the organization can effectively respond to and recover from disruptive events



Offensive Security to Test Resilience

Testing your effectiveness provides the information and insights to increase preparedness, improve security postures, and reduce risk.

Sample offerings:

- **Internal / External Vulnerability Assessment**
- **Internal / External / Web Application Pen Tests**
- **Red / Purple Team Programs**
- **Email Hardening Assessment**
- **Active Directory Assessment**
- **Phishing Campaign Assessment**
- **Physical Penetration Test**

Lodestone

Advisory Services to Strengthen Security

Configurable to client needs, budget, and timing requirements; delivered with professional project management.

Sample offerings:

- **Cloud Security Advisory:** M365, GCP, AWS
- **Compliance as a Service**
- **Vulnerability Mgt as a Service**
- **Board Reporting**
- **M&A Activity**
- **Ransomware Readiness Assessment**
- **Virtual CISO Retainers**
- **Gap Assessments:** CIS-18, NIST CSF, HIPPA
- **Threat Landscape Briefing**
- **Tabletop Exercises:** Executive & Technical, Crisis Management
- **Security Policy Review & Development**
- **Incident Response Plan Development**
- **Security Awareness Training**

Lodestone

Managed Detection & Response

Delivering powerful detection capabilities through an integrated client platform to rapidly identify and contain threats.

Adaptive Monitoring
Active Containment

Lodestone

MDR Enables Security at Scale

Delivering talent and infrastructure for continuous monitoring & rapid containment of suspected threats.

Key Advantages of Implementing an MXDR Solution

- **Overcome talent shortages and/or supplement your security organization**
- **Realize continuous monitoring across your technology ecosystem with minimal capital outlay**
- **Access advanced threat detections and stay current against trending attack vectors**
- **Customize security rules to your environment to minimize noise and ‘alert fatigue’**
- **Automation speeds threat containment for human intervention**

Recommended by:

Gartner FORRESTER IDC

MDR adoption grew 49% between 2020-’21; expected to reach $2.25B market by 2025

Lodestone

Proof & Results of MDR Services

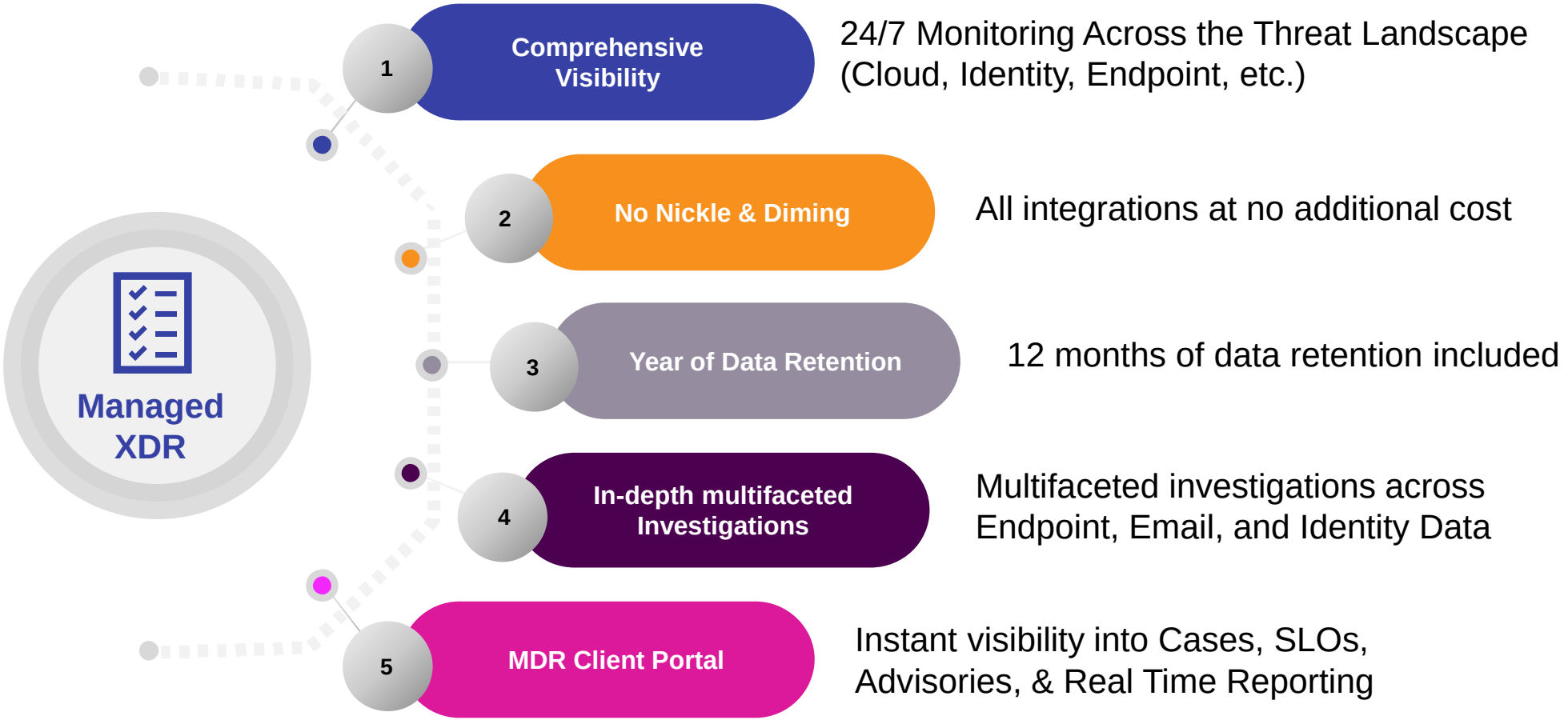
Organizations using an MDR service had a **62% reduction** in the average number of security incidents per year.

The Average Time to Detect a Breach

212 days without a SOC or MDR

32 days with a SOC

10 days with MDR

Source: Ponemon Institute

Lodestone Managed XDR: Value Proposition