rackspace technology

Discover Sensitive Data:

5-Week Workshop and Threat Assessment

Powered by **Rackspace Elastic Engineering for Microsoft 365**

Are you protecting your business data and communications from modern security threats? Are you confident that your organization is protected from phishing, malware, and credential theft? Are employees are using the right password protocols? Do you worry about data exposure via 3rd party cloud apps and shadow IT connected to your systems?

Organizations are facing increased exposure to data theft and breaches of critical IT systems as business data moves to the cloud. Phishing, malware, ransomware, and data exfiltration techniques are becoming sophisticated, while configuring protections can seem expensive and overwhelming. Given the volume and complexity, it’s essential to learn how secure your organization and how to mitigate and protect against threats moving forward.

Get a real report on current threats in your environment and a customized assessment of your security posture. Work with our engineers to design and implement threat prevention technologies for your organization.

> *“Rackspace brought a lot of knowledge, which we simply wouldn’t have been able to get on our own. It has really opened its doors to us and worked as a partner, not simply a service provider.“*
>
> - Amit Patel, Head of Enterprise Architecture, British Heart Foundation

Improve your cloud security posture with a Microsoft Modern Workplace Security Discover Sensitive Data Workshop followed by ongoing advisory and implementation services leveraging Rackspace’s Elastic Engineering for Microsoft 365.

SUPPLEMENT AND UPLEVEL SKILLS

- “Do-with” approach
- **On-demand access** to dedicated engineering resources with diverse skillset who know your environment and goals
- **Leverage expert hands-on-keyboard** management of your Azure environment
- **Scale up and down** monthly as business needs change

OUTCOME FOCUSED

- Business outcomes, not our SLAs
- **Document and work towards security priorities** and needs of the business
- **Identify real threats and protection features** in your environment
- **Prioritize and implement protections** for data and services
- **Reduce the attack surface** for hybrid workloads and business data stores

ONGOING INNOVATION

- Progressive business transformation
- **Accelerate your security journey** leveraging and staying current with an on-platform collection of security solutions
- **Continual review and optimization** of security operations to meet business outcomes and objectives

Your path to a robust threat protection system.

We can help you develop a strategic plan for your organization and based on the recommendations of Microsoft cybersecurity experts. We'll spend the first few weeks configuring the Microsoft 365 platform to collect threat signals in your environment to provide live data for analysis. You'll gain visibility into immediate threats and vulnerabilities across identity systems, email, and data, plus clarity and support on how to improve your security posture for the long term. The deliverable becomes the starting point for your dedicated Elastic Engineering for Microsoft 365 pod, strengthening your organization's approach to threat protection.

Discover Sensitive Data Workshop

- **Live Threat Check in your environment:** analyze active threats and current vulnerabilities
- **Discovery Strategy Planning Session:** Priorities and requirements are established in relation to securing your environment
- **Data Protection Prioritization Matrix:** Confidential data locations, labelling options and rules for sharing are identified and documented
- **Build and Test (Label and Protect):** Confidential data is labelled, and sensitivity levels are established leveraging Microsoft Information Protection (MIP) and Office 365® Data Loss Prevention (DLP).
- **Data Protection Planning Guide:** A working document is delivered that identifies next steps based on priorities.

Duration: 5 Weeks **Cost: $10,000**

Transition to Rackspace Elastic Engineering for Microsoft 365

The Security Workshop deliverable is used as starting point for the backlog of work on which your dedicated Elastic Engineering for Microsoft 365 pod of experts will engage. Backlog typically includes:

- **Data discovery and categorization:** classify business data and document location and sensitivity characteristics and keep the data protection matrix updated.
- **Label and protect data at rest:** create and test policies to protect data identified in the protection matrix.
- **Secure and protect data in transit**: create and test policies to prevent data exfiltration or leakage
- **Risk management and remediation:** when a security incident occurs, your pod will work with your team to design and implement new policies to remediate threats and help prevent similar incidents in the future.

READY TO GET STARTED?

Schedule your Discover Sensitive Data Workshop today!

ABOUT RACKSPACE TECHNOLOGY

With over two decades of experience helping customers succeed, Rackspace solves more than workload problems; we help create business advantages. Whether you're looking to spur innovation and agility, lower costs or build operational efficiencies, Rackspace Technology's thousands of experts are ready to put cutting-edge capabilities to work for your business.

Gold
Microsoft Partner
Azure Expert MSP
Microsoft

Gold
Microsoft Partner
Microsoft

Cloud Platform
DevOps
Application Development
Application Integration
Data Platform

Microsoft
5 Times Hosting Partner of the Year

Gartner
2020 Magic Quadrant Leader
for Public Cloud Infrastructure Professional and Managed Services, Worldwide

rackspace technology