Insider Threat Protection Engagement

Implement a security policy to identify and protect against insider threats on Microsoft.

As your business adapts to a flexible working strategy with remote employees the threat of insider data breaches increases. The range of potential threats can include the accidental sharing of confidential data via email to the malicious saving of classified files outside of SharePoint®. To help you identify and protect confidential data, Rackspace Technology has developed an engagement that implements security policies leveraging automated features on Microsoft 365®.

Key Features and Benefits

The Insider Threat Protection Engagement will demonstrate how you can, for example, identify when and who is downloading confidential data from SharePoint. With properly labeled data, notifications can alert you to suspicious activity, allowing you to take appropriate and timely action.

Learn how you can securely manage your data with encryption, labelling and by limiting access to sensitive information through access policy implementation. Microsoft-certified engineers at Rackspace Technology will work with you to:

- Identify confidential data that's at risk from accidental or malicious breaches
- Establish data protection policies and catalog confidential data
- Manage your data protection policies

The Insider Threat Protection Engagement Overview

Following a discovery call, Rackspace Technology will provide a statement of work outlining the scope of your engagement. A dedicated project manager will work with you to establish your security priorities, after which Microsoft-certified engineers will build and test your policy. This engagement will include the following deliverables:

Discovery Strategy Planning Session: Priorities and requirements are established in relation to securing data

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 the Microsoft Information Protection (MIP) solution and Office 365® Data Loss Prevention (DLP). Authorized user groups and permissions within those groups are established to minimize the risk of this data being shared.

Data Protection Planning Guide: A working document is delivered that identifies next steps based on priorities.

At the end of your engagement, Rackspace Technology will conduct a review with you of the insider threat management tools used to identify and manage policies and alerts.

About Rackspace Technology®

Rackspace Technology is your trusted partner across cloud, applications, security, data and infrastructure.

- A leader in the 2020 Gartner Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide
- 2,500+ cloud engineers
- Hosting provider for more than half of the Fortune 100
- 20+ years of hosting experience
- Customers in 120+ countries
- Five-Time Microsoft Hosting Partner of the Year
- 2,350+ Microsoft certifications, including MCITPS, MCSAs, MCSEs and MCTSs
- Microsoft Gold Certified

"We knew that continuing to grow and stay on the cutting edge of our industry meant finding a partner to modernize our IT and guide us through our digital transformation."

Rob Cutler :: Executive VP, CEO of Delmar® International Inc.

Fanatical Experience™

Experts on your side, doing what it takes to get the job done right. From first consultation to daily operations, Rackspace Technology combines the power of always-on service with best-in-class tools and automation to deliver technology when and how you need it.

rackspace technology®

Prerequisites

The Insider Threat Protection Engagement is designed for Office 365 cloud-only solutions related to Microsoft 365. A separate statement of work is required for hybrid on-premises and cloud versions.

Licensing, such as Microsoft 365 E5 or add-ons which include MIP and DLP, are required. Access management and user groups should be pre-configured to gain the most benefit from this engagement.

This engagement is aimed at empowering decision-makers who share responsibilities for securing confidential data, including:

- Chief Executive Officers
- Chief Information Officers
- Chief Security Officers
- Data Protection Officers
- Data Governance Officers
- IT Security, Compliance and/or Operations Managers

Take the Next Step

Speak to a Rackspace Technology security expert to book your Insider Threat Protection Engagement today.

Learn more: **www.rackspace.com**
Call: **1-800-961-2888**

rackspace technology®