Microsoft

Zero Trust

Designated Engineering overview

Modernizing your security model allows you to effectively adapt to the complexities of the modern environment, embrace the hybrid workplace, and protect the people, devices, apps, and data within your organization. This DE provides you with guidance to help you along your Zero Trust security journey, enabling strong authentication and device compliance for your organization.

Zero Trust scenarios

Identity – Learn how to deploy and manage Microsoft Azure AD to administer remote workers, devices, partners, and bring-your-own-device (BYOD) scenarios utilizing principles of Zero Trust

Endpoint – Gain visibility into devices accessing the network. Ensure compliance and health status before granting access

Driving outcomes with a Zero Trust Designated Engineering

Your priorities

- Enforce a security policy to better support a diverse bring-your-own-devices (BYOD) ecosystem with a hardened security posture
- Ensure that potential threats are investigated and resolved
- Streamline device management and application management across cloud solutions for our internal users

Outcomes we deliver

- Provide a unified security management plan to enable robust capabilities that assume Zero Trust; allowing your employees to work securely from any device
- Learn how to leverage the expert-level threat monitoring and analysis capabilities within Microsoft Defender
- Simplify automated provisioning, configuration management, and software updates for all your endpoints

What your Designated Engineering package could look like

Your account team will design a specific program of services that is tailored to your organization's business and technology goals. If you are still defining your technology needs, our experts will work with you to assess your strategy and tailor an engagement for your organization. Here is what a sample **Zero Trust Designated Engineering** could look like:

	1	2	3
	Assess and discover	**Upskill and design**	**Configure and implement**
Example engagement	**Zero Trust foundation assessment**	**Secure endpoints with Zero Trust: Microsoft Defender for endpoint**	**Onboarding accelerator – implementing Microsoft Intune features**
Key focus	Receive a prioritized roadmap to enable effective protection and organizational resilience through the trust-by-exception model of the Zero Trust architecture	Gain an understanding for your Zero Trust maturity and set deployment objectives to reach the optimized maturity state for Zero Trust endpoints	Receive expert guidance for a successful implementation and prepare your environment to implement Microsoft Intune

Microsoft

Protect and Govern Sensitive Data

Designated Engineering overview

In today's cloud-first world, organizations need to ensure security and compliance capabilities are implemented to meet specific compliance mandates and regulatory standards.

Protect and Govern Sensitive Data scenario

Microsoft 365 Information Protection
Protect your organization's data and enable a governance process to address security and compliance requirements.

Driving outcomes with a Designated Engineering for Protect and Govern Sensitive Data

Your priorities

- Enable a secure remote work strategy using Office 365 and Microsoft 365 security and compliance controls.
- Improve overall security to better protect sensitive data across clouds, apps, and devices.
- Prevent phishing and malware emails and ensure your data stays safe when employees are accessing company assets.

Outcomes we deliver

- Maximize the benefit from information protection and governance capabilities built into Microsoft 365 apps and services.
- Identifies gaps in your security processes and provides you with a plan of action to protect, detect, and respond to threats.
- Upskill your IT staff to better protect against threats and improve your response strategy.

What your Designated Engineering package could look like

Your account team will design a specific program of services that is tailored to your organization's business and technology goals. If you are still defining your technology needs, our experts will work with you to assess your strategy and tailor a custom proactive engagement for your organization. Here is what a sample **Designated Engineering for Protect, and Govern Sensitive Data** could look like:

	1	2	3
	Assess and plan	**Upskill and design**	**Configure and implement**
Example engagement	**Microsoft Purview Compliance Optimization Assessment**	**Activate Microsoft 365 Security and Compliance: Purview Data Loss Prevention**	**Accelerate: Microsoft Teams Governance, Security, and Compliance**
Key focus	An IT assessment of your current compliance capabilities and recommended actions for improvement.	In-depth guidance for how to enable the protection of sensitive information using M365 Data Loss Prevention.	Receive tailored Microsoft Teams governance strategy guidelines and learn how to enable key Teams security and compliance features.

Microsoft

Security and Compliance

Designated Engineering overview

The journey to the cloud can come with new challenges. Our engineers will help you reach your goal through the Designated Engineering for Security and Compliance. Employing this accelerator enables you to optimize your security posture, improve operations, and respond to threats faster.

Security and Compliance scenario

Office 365 Threat Protection Improve operations, reduce threats and accelerate threat investigation as you enhance your organization's security posture with Office 365 security controls and policies.

Driving outcomes with Designated Engineering for Security and Compliance

Your priorities

- Gaining greater visibility and control with robust security solutions to accelerate response and remediation timeframes.
- Responding to increasing compliance obligations.
- Protecting, detecting, and responding to advanced threats, including email threats like phishing.

Outcomes we deliver

- Define a roadmap to accelerate the activation of security capabilities to protect, detect, and respond to threats.
- Develop secure email practices with Exchange Online Protection (EOP) and Microsoft Defender.
- Enable threat investigation and response capabilities.

What your Designated Engineering package could look like

Your account team will design a specific program of services that is tailored to your organization's business and technology goals. If you are still defining your technology needs, our experts will work with you to assess your strategy and tailor a Designated Engineering for your organization. Here is what a sample **Designated Engineering for Security and Compliance – Optimize O365 Threat Protection** could look like:

	1 Assess and plan	2 Upskill and design	3 Configure and implement
Example engagement	**Office 365: Security Optimization Assessment**	**Activate Microsoft Defender for Office 365**	**Office 365: Security Optimization Assessment Remediation**
Key focus	Identify gaps and define a plan of action to remediate blockers to effective threat protection.	Learn how to implement security controls to protect workloads from advanced threats (zero-day and malicious links).	Evaluate and implement the remediation plan to enable Office 365 embedded security capabilities to protect, detect, and respond to threats.