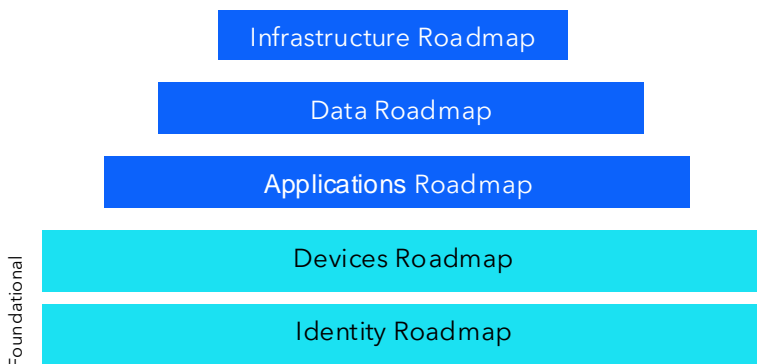


Create your security foundation: Slalom's Azure Zero Trust Assessment Workshop



Azure Zero Trust Assessment Workshop Building Blocks



Workshop outcomes

- **Enhanced Security Posture:** Zero Trust helps to control that only authenticated and authorized users and devices can access applications and data, thereby reducing the risk of security breaches and protecting sensitive information.
- **Improved Compliance and Control:** By implementing strict access controls and user verification, Zero Trust helps organizations meet regulatory requirements and maintain a robust compliance posture.
- **Increased Operational Efficiency:** With Zero Trust, organizations can streamline their security protocols and reduce the complexity of their networks, leading to improved operational efficiency and lower costs.

Start the conversation today!

Want to ask any questions or just have a conversation with one of our experts to learn more about Slalom's Azure Zero Trust assessment? We're here for you when you're ready.

Contact:
[Chris Elliott](#)
[John Brooke](#)

Slalom's Azure Zero Trust Workshop

We will work with your organization's security and infrastructure leaders to create a point-in-time snapshot of where you are in your security journey. From there, we can develop a customized road map to help you achieve your goals and set priorities on which ones should take precedence.

Workshop Agenda:

- Zero Trust Assessment Tool
- Identity Roadmap
- Devices Roadmap
- Application Roadmap
- Data Roadmap
- Infrastructure Roadmap

Duration:	1 Day - 8 hrs.
Cost:	TBD - MSFT funding may be available
Who it's for:	Security and Infrastructure leaders
How to get started:	Reach out to your Slalom contact for more information



[Learn more](#) about what you can do with Slalom and Microsoft

Azure Zero Trust Assessment

Evaluating Microsoft's Framework for Enhanced Cyber Resilience

What is Zero Trust?

Zero Trust Security goes beyond traditional organization perimeter. Its perimeter less security which secures the org data from all type of users, devices and apps from inside and outside of the network. Zero Trust emphasizes "Never Trust and Always Verify".

Why is Zero Trust Important?

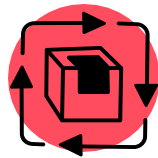
In today's digital landscape, breaches are not a matter of if, but when. The critical concern is how far an attacker can penetrate once inside the environment. Implementing Zero Trust helps protect users, customer data, and company assets by adhering to a combination of government and industry-standard best practices.

Where do I start in my Zero Trust Journey?

You can begin your Zero Trust journey immediately, regardless of your current stage. Slalom offers a Zero-Trust assessment package to provide a snapshot of your current security posture. Based on this assessment, we can create a customized roadmap to help you achieve your security goals and prioritize actions effectively.



Reduction in Data Breach Costs



Recovery Time & Cost Reduction



Efficiency in Security Operations



Improved Organizational Compliance

SLALOM + MICROSOFT

For over two decades Microsoft and Slalom have delivered innovation together. Our shared purpose is to realize greater impact through collaboration and enable every person and organization to achieve more. We lead with a people-focused approach to help our clients reach for and realize their vision of better tomorrows powered by Microsoft solutions.

8,600+

Microsoft projects delivered

2,200+

Microsoft certifications held by our delivery teams

50+

Times recognized by Microsoft as a valued partner



Why Choose Slalom for Your Zero Trust Journey?

With over 20 years of experience partnering with Microsoft, Slalom's security experts are ready to work with you to develop a customized road map to help you achieve your goals and set priorities on which ones should take precedence.

We will work with your organization's security and infrastructure leaders to walk through the Azure Zero Trust journey. This will include going through an assessment of over 14 different identity components related to the Identity Roadmap, 20+ devices components related to the device roadmap to set the foundation for infrastructure, apps, and data.