Zero Trust Strategy Workshop

Zero Trust secures all access points across your organization by requiring assets and people to earn trust before gaining entry to your environment. When you implement Zero Trust into your security plan, you remove the overall cybersecurity risk across the network, endpoints, and cloud.

Zero Trust is a strategic security approach that is woven throughout your organization’s architectures, technology selections, and operational processes. Its architecture allows organizations to map out internal and external entry points and related security threats to maximize the chances of timely mitigation.

Zero Trust Workshop

Our workshop engages your business and security leaders to gain a holistic evaluation of your current security environment to implement an effective Zero Trust strategy. Our experts start by giving you a closer look at how organizations are solving security problems with Zero Trust, followed by a discovery exercise to identify any existing tools that may aid in the Zero Trust journey.

To determine the best Zero Trust strategy for your business, a roadmap is created to identify business objectives, uncover business and technical challenges, outline an operational plan, and align capabilities versus requirements. Additionally, through a gap analysis based on the six standards of the Zero Trust Security Model, we will distinguish use cases and threats.

Gap Analysis

Zero Trust is a strategic approach that empowers security leaders to achieve practical and efficient security implementations. To succeed, Zero Trust needs to contain a combination of policies, practices, and technologies organized through six standards. The purpose of a Zero Trust architecture is to protect data, which is why data is the foundational base of the Zero Trust Security Model.

**USERS**
Ensure the user is who they say they are with multi-factor authentication (MFA) before authorization occurs.

**DEVICES**
The device is recognized by a certificate to prove it is the device it says it is.

**NETWORK**
Configured to detect, protect, respond, and recover against attacks.
**APPLICATIONS**
Application access ensures it is encrypted, authenticated, and authorized.

**AUTOMATION**
Confirms the security follows the workloads.

**ANALYTICS**
Analyze and feed information back into the model for decisions in policy, provisions, and reporting.

**Operational Outline**
Trace3 will guide the customer through a customized inquiry model that examines what technologies and processes exist to facilitate Zero Trust. This is followed by an in-depth review of tools the organization has in place that may be underutilized and can serve as part of a Zero Trust architecture. Lastly, our experts will assess the maturity of technologies and processes in relation to a Zero Trust architecture.

**USE CASES & THREATS**
- Map existing use cases to the Zero Trust implementation strategy
- Identify gaps within the existing people, processes, and technologies
- Based on the current implementation, what aligns with Zero Trust requirements

**Deliverables**
At the end of the workshop, Trace3 will provide a three-year Zero Trust Strategy Roadmap that outlines visibility, policy definition, enforcement, and transition of your organization's Zero Trust environment while also providing recommendations for each of the six Zero Trust standards to mature your security posture.

**VISIBILITY**
To provide guidance and focus on the direction.

**POLICY DEFINITION**
Align policies to current business requirements, with a development plan for mapping to a complete Zero Trust adoption.

**ENFORCEMENT**
Governing Zero Trust policies within your current environment, including additional tool-specific mapping, implementation, decommissions, etc.

**TRANSITION**
To realize full-scale Zero Trust within everyday operations and beyond.

**INNOVATIVE SOLUTIONS + ELITE CONSULTING SERVICES = EFFECTIVE SECURITY OUTCOMES**
To learn more or to engage our Zero Trust specialists visit www.trace3.com/zero-trust-workshop-request