Zero Trust Readiness Assessment

Benefits:

- Minimize chances of facing a data breach
- Uncover organizational, functional and technological gaps
- Develop a strategy and roadmap that addresses planning and budgeting required to achieve desired Zero Trust State
- Addressing the complexity of integrating a ZeroTrust model with the existing environment

Designed for customers who need to evaluate the current state of their information security program and its maturity in attaining Zero Trust.

As data spreads across multiple locations, cloud vendors, and a variety of endpoint devices, traditional security that has relied on protecting organizations from the perimeter and trusting devices inside the network has become less effective.

An organization’s network architecture should evolve to a Zero Trust model to align with this absence of a true perimeter.

New business initiatives and processes have created broader attack surfaces. Applications, users, and devices are moving outside of the traditional corporate zone of control, dissolving what was once the trusted perimeter, and enterprise security and networks must evolve to help protect the business.
Our Service Approach

AT&T Cybersecurity Consulting will utilize the following 6 pillars of Zero Trust as a foundation of the overall assessment:

- **Users**: Authentication and verification of users on an on-going basis.
- **Devices**: Authentication of a device and its cybersecurity posture.
- **Workloads**: Development of applications, and access to applications.
- **Network**: Network segmentation, isolation, and protection of data in transit.
- **Analytics**: Real-time observation to understand user and device interaction.
- **Automation**: Make dynamic changes to access based on analytics.

**Present State to Next Generation**

The Zero Trust Readiness Assessment provides an understanding of your current maturity in achieving Zero Trust and a list of priorities and milestones that will lead to achieving a next generation environment.

**Discovery**

An on-site discovery workshop is conducted to gather information on the current posture of your information security program.

**Zero Trust Capabilities Assessment**

Information discovered within each of the 6 pillars is used to analyze the organization’s alignment with the major tenets of Zero Trust.

**Maturity Assessment**

A maturity assessment is conducted on the organizations capabilities within each of the pillars, as well as the overall security program, to understand required changes necessary to align with Zero Trust.

**Strategy and Roadmap**

AT&T Cybersecurity Consulting will use the current maturity to develop a strategy and roadmap tailored to your organization that addresses planning, budgeting, prioritization, time management, and implementation of strategic initiatives required to efficiently and effectively help achieve your desired Zero Trust estate.
Zero Trust Readiness Implementation

With unrivaled visibility across data, network and devices, leading insights from AT&T Alien Labs and our open source threat exchange, we can anticipate and act on threats to protect your business. As a trusted advisor we’re delivering a new era of transparency, giving you confidence in your decisions, your data, and your partnerships.

Why AT&T

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

About AT&T Cybersecurity

Contact us to learn more, or speak with your sales representative.