AT&T Business

Bring Zero Trust to your network

Secure your network in 7 key steps

Multiple locations, cloud vendors, and endpoint devices make network security challenging.

A Zero Trust framework can help shield your business against threats by continuously authenticating and authorizing users. We have solutions to make your network more resilient while reducing cost and complexity.

7 Steps to Zero Trust

1 Develop your strategy

Start by asking why Zero Trust is important to your business. Be sure to factor in:

- The goals you need to accomplish
- The kinds of threats you are facing and where
- The departments and business segments that need to be included

This will help you formulate a Zero Trust strategy and build a strong case to get buy-in from leadership.

2 Define what you want to protect

Data comes in many forms and is in many locations. Consider:

- What data needs to be kept safe and why
- The different levels of classification and what that means for security
- Specific requirements for certain types of data, like Payment Card Industry (PCI) or electronic Protected Health Information (ePHI)

Classifying data according to its level of sensitivity will help you understand how to protect it.

3 Understand your data and traffic flows

Map traffic flows and data usage to get a detailed view of all assets, applications, and users. This includes:

- Access requirements for each application
- Application users, including where and how data is accessed
- Application owners, system owners, developers, database owners, and administrators
- Communication requirements on the network

The more complete the information, the better prepared you will be in developing your Zero Trust policy.

4 Assess your Zero Trust maturity

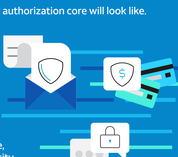
Review your current security environment. You may find you're already using some Zero Trust principles. These include:

- Remote access virtual private networks (VPN)
- Data loss prevention (DLP) software
- Next generation firewalls (NGFW)

Knowing what you need and what you don't will help shape your Zero Trust architecture, implementation, resources, and budget.

5 Design your Zero Trust Architecture (ZTA)

Create an outline to determine what your authorization core will look like. Consider how it will perform with:



- On-premises, cloud, and business transaction elements
- Data stores, analysis, threat intelligence, public key infrastructure (PKI), and identity and vulnerability management tools
- Software-defined perimeters, micro-segmentation, and identity governance authorizations

This will enable you to formulate a pilot program and work out issues in advance without impacting your entire business.

6 Build your Zero Trust Policy

Develop a trust algorithm to create a policy based on traffic flows and data classification. Include trust and risk elements and adjust authorizations as needed using analytics and automation.

7 Monitor and maintain

Like any security strategy, you'll need to monitor and adjust your Zero Trust policy based on performance, workload, activity, and threats. Doing so before a problem occurs reduces your risk and reinforces a continuous Zero Trust state.

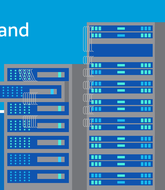
Have you developed an effective Zero Trust strategy?

According to Gartner, by 2026, 10% of large enterprises will have a mature and measurable Zero Trust program in place, up from less than 1% today.[1]

1. "Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero Trust Program in Place by 2026," Gartner, January 23, 2023. gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026

Data location and security go hand in hand

Check out the latest edge security insights and recommendations in our AT&T Cybersecurity Insights Report.



Why AT&T Business

Cybersecurity is complex. The threat landscape changes fast. How do you know if you're making the right security choices? Our skilled and experienced consultants have the expertise to help you understand cybersecurity issues and make the best choices for your business.

Learn more about AT&T Cybersecurity Solutions or contact your AT&T Business representative.