

## CHECKLIST

# PREPARING FOR ZERO TRUST ADOPTION

By diligently completing each step in this checklist, organizations lay a solid foundation for a successful transition to a Zero Trust model, ensuring alignment with security objectives and fostering a culture of cybersecurity awareness.



### Evaluate Current Security Posture

#### Thorough Security Analysis:

- Conduct a comprehensive evaluation of existing security measures, policies, and infrastructure.
- Identify vulnerabilities, assess the effectiveness of current security protocols, and understand potential gaps in protection.

#### Baseline Establishment:

- Use the evaluation findings to establish a baseline understanding of the current security posture.
- Document areas that require improvement and realignment with Zero Trust principles.



### Identify Critical Assets & Data

#### Asset and Data Classification:

- Meticulously identify and classify critical assets and sensitive data.
- Prioritize assets, including customer information, intellectual property, financial records, and other data critical to business operations.

#### Tailoring Protection Measures:

- Use the prioritized asset list to tailor Zero Trust implementation, focusing on protecting the most valuable and sensitive components.



### Educate & Engage Stakeholders

#### Key Decision-Makers Engagement:

- Engage key decision-makers to communicate the significance of Zero Trust adoption.
- Foster a shared understanding of Zero Trust principles and their impact on organizational security.

#### IT Teams Involvement:

- Collaborate with IT teams to ensure they comprehend the changes and requirements associated with Zero Trust.
- Encourage active participation in the planning and implementation process.

#### End-User Education:

- Conduct training sessions and awareness programs for end-users.
- Help employees understand the importance of their role in maintaining a secure environment under the Zero Trust model.

#### Cultural Shift Emphasis:

- Emphasize the cultural shift required for successful Zero Trust adoption.
- Instill a sense of collective responsibility for cybersecurity across all levels of the organization.



### Communicate & Align

#### Clear Communication:

- Ensure transparent communication regarding the organization's journey towards Zero Trust adoption.
- Clearly convey the expected changes and benefits to all stakeholders.

#### Stakeholder Alignment:

- Confirm alignment among stakeholders regarding the goals and objectives of Zero Trust adoption.
- Address any concerns or questions to foster a supportive environment.



### Document & Plan

#### Documentation of Preparatory Phase:

- Document the findings and outcomes of the preparation phase for reference and continuous improvement.
- Create a roadmap for transitioning from the current security posture to the desired Zero Trust model.

Learn more about our complimentary, 4-hour [ZTA Workshop](#).