2024 PMIWDC CONFERENCE

Back to The Future

AUGUST 23 - 24, 2024

Moving towards Zero Trust Architecture - a Methodical Approach!

Dr. Sarbari Gupta

Founder and CEO

Electrosoft

Project Management Institute. Washington, DC

The Challenge of Zero Trust

- The cybersecurity landscape is evolving.
- Federal agencies are mandated to adopt Zero Trust Architecture (ZTA).
- ZTA is not just a technical shift but requires organizational and process changes across agencies.

Electrosoft

Agenda

- Fundamentals
- Legislation and Policy
- Challenges
- Approach
- Further Details
- Conclusion
- Q&A

Electrosoft

Fundamentals

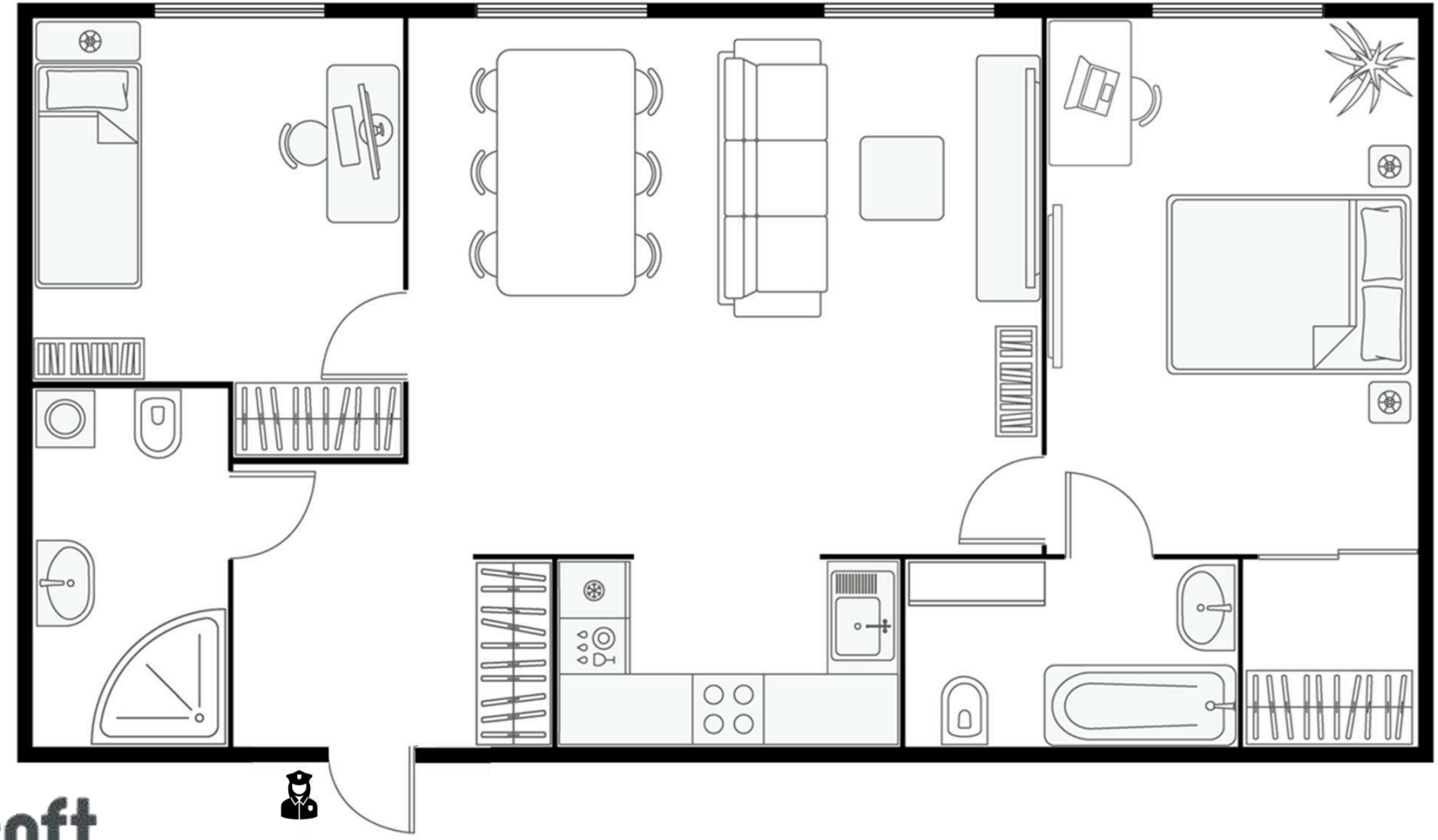
Electrosoft

What is Zero Trust Architecture (ZTA)?

- **Definition:**
  - Zero Trust Architecture is a security model that assumes all entities, both internal and external, are untrustworthy.
  - Every entity, whether user, device, or application, must be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to resources.

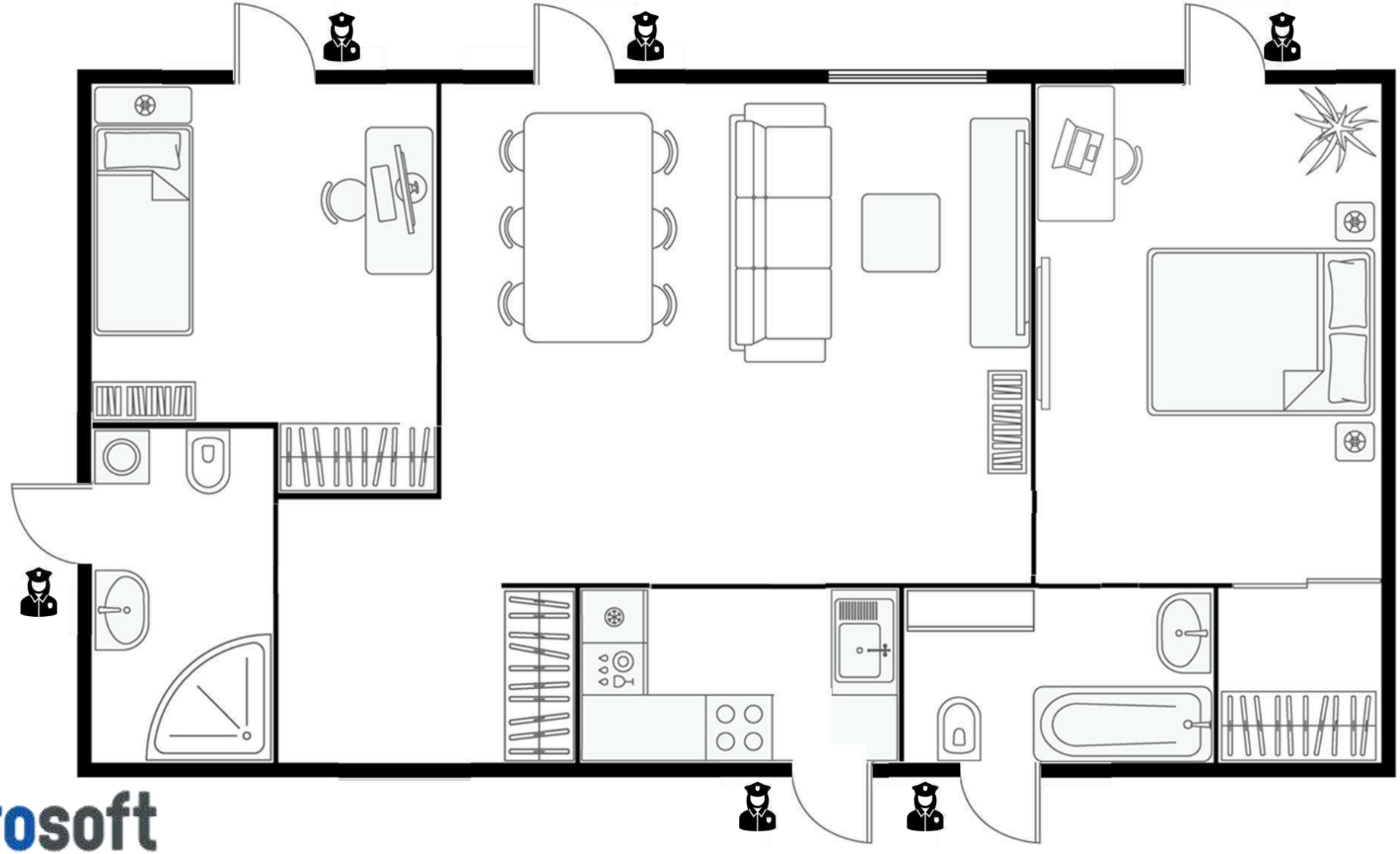
- **Key Components:**
  - **Identity**: Verify and authenticate all users.
  - **Devices**: Ensure that all devices accessing the network are secure and compliant.
  - **Networks**: Implement secure, micro-segmented networks.
  - **Applications and Workloads**: Monitor and secure applications and workloads in real-time.
  - **Data**: Protect and monitor data at all times, both in transit and at rest.

Traditional Perimeter Security



Electrosoft

Security through Zero Trust Architecture



Electrosoft

Legislation and Policy

Electrosoft

Legislative and Policy Drivers (I)

- **Executive Order 14028:**
  - Signed on May 2021, this EO focuses on improving the nation's cybersecurity and mandates the adoption of Zero Trust Architecture across federal agencies.
  - Agencies are required to implement specific security measures that align with Zero Trust principles.

- **OMB Memorandum M-22-09:**
  - Issued in January 2022, this memorandum provides a federal Zero Trust strategy, outlining vision statements and specific actions across the five pillars of Zero Trust: Identity, Devices, Networks, Applications, and Data.

Legislative and Policy Drivers (II)

- **NIST Special Publication (SP) 800-207 - Zero Trust Architecture:**
  - Defines Zero Trust and provides a comprehensive framework for implementing ZTA
  - Serves as the primary guide for civilian agencies in developing and deploying Zero Trust strategies
- **CISA Zero Trust Maturity Model v2.0**
  - Provides additional guidance and clarity for agencies as they move forward in their Zero Trust journey.
  - Includes enhanced descriptions of the Zero Trust pillars and desired outcomes at each stage of maturity.
- **CISA Cloud Security Technical Reference Architecture (CSTRA)**
  - Offers guidance on securing cloud environments using Zero Trust principles.
- **DoD Zero Trust Strategy**
  - Outlines the DoD's vision and goals for achieving a comprehensive Zero Trust Architecture by 2027
  - Seven pillars: User, Device, Network/Environment, Application and Workload, Data, Visibility and Analytics, and Automation and Orchestration
- **DoD Zero Trust Reference Architecture**
  - Provides a detailed technical framework for implementing Zero Trust within the DoD. It describes the core principles, components, and technologies required to build a Zero Trust environment

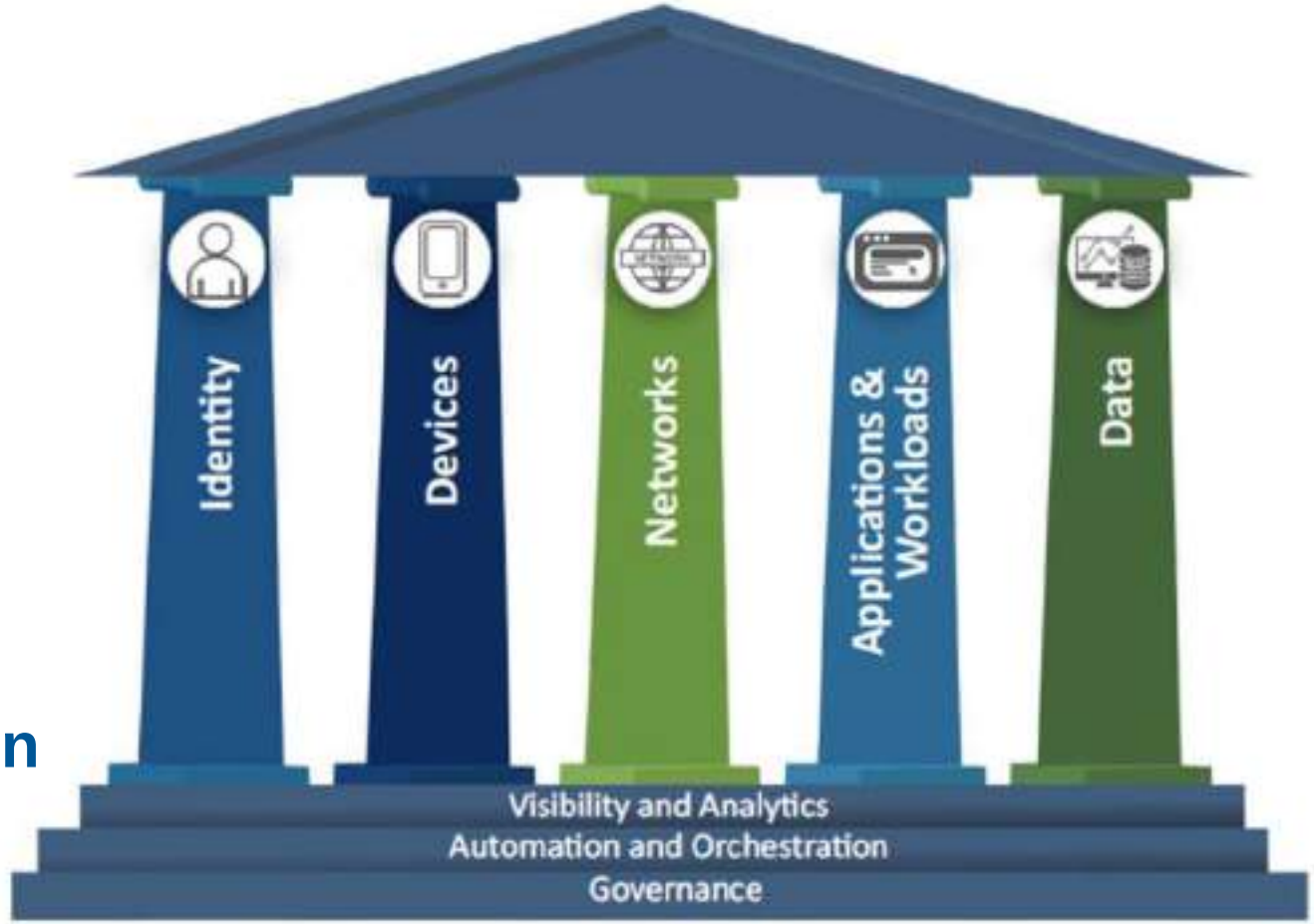
Seven Tenets of Zero Trust (NIST SP 800-207)

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

Electrosoft

CISA Zero Trust Maturity Model

- **5 Pillars**
  - Identity
  - Devices
  - Networks
  - Applications & Workloads
  - Data
- **3 Cross Cutting Capabilities**
  - Visibility & Analytics
  - Automation & Orchestration
  - Governance



Electrosoft

DoD Zero Trust Model

User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Devices

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.

Visibility & Analytics

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Automation & Orchestration

Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Applications & Workloads

Secure everything from Applications to hypervisors, to include the protection of containers and virtual machines.

Data

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Network & Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.

Electrosoft

Challenges

Electrosoft

Complexity of Zero Trust Implementation

- **Challenges:**
  - ZTA is not just a technical challenge; it impacts policies, processes, stakeholders, and the entire IT environment.
  - Agencies may feel overwhelmed by the scope, as the journey towards Zero Trust affects nearly every aspect of operations.
- **Scope:**
  - The Zero Trust journey is a multi-year process that requires careful planning, resource allocation, and continuous adaptation.
  - Agencies must be prepared for a complex and multi-faceted implementation process.

Electrosoft

Need for a Phased, Iterative Approach

- **Phased Implementation:**
  - Breaking down the Zero Trust journey into manageable phases is essential to making progress.
  - Each phase should focus on specific goals and objectives, allowing for incremental improvements.
- **Pilot Programs:**
  - A critical component of Zero Trust implementation.
  - Enable agencies to test new functionalities in a controlled environment, validate their effectiveness, and gather feedback for further improvements.
- **Iterative Process:**
  - Each phase and pilot should build on the lessons learned from previous efforts.
  - Iterative improvement ensuring that the Zero Trust implementation is constantly evolving and adapting to new challenges.

An Approach

Electrosoft

Step by Step Process

1. Establish Governance and Assess Current State

2. Develop Zero Trust Strategy and Roadmap

3. Prioritize and Plan Zero Trust Actions

4. Execute Pilot Programs

5. Continuous Monitoring and Iteration

6. Scale, Document and Share

7. Align with Compliance and Plan for the Future

Electrosoft

1. Establish Governance & Assess Current State

- **Executive Support & Governance:**
  - Secure leadership buy-in and establish a Zero Trust governance structure.
  - Form a Zero Trust Steering Committee to oversee the implementation process.
- **Current State Assessment:**
  - Inventory all IT assets (users, devices, networks, applications, and data).
  - Conduct a risk analysis and prioritize based on mission-critical assets and vulnerabilities.
  - Use maturity models (e.g., CISA's Zero Trust Maturity Model) to evaluate the current state.

Electrosoft

2. Develop Zero Trust Strategy and Roadmap

- **Strategic Vision:**
  - **Align Zero Trust objectives with the agency's mission and strategic goals.**
- **ZTA Strategic Roadmap:**
  - **Create a phased implementation plan with short-term, mid-term, and long-term goals.**
  - **Prioritize actions based on:**
    - **High-risk areas**
    - **Critical resources**
    - **Agency mission priorities and federal mandates**

Electrosoft

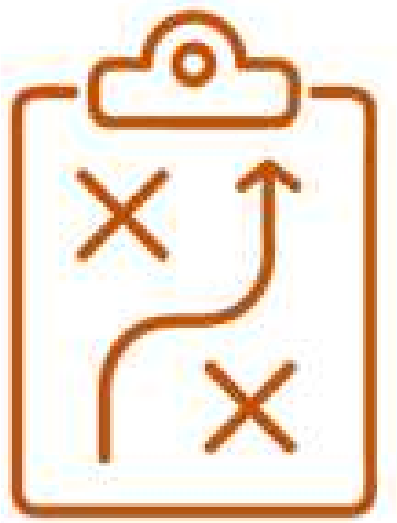
3. Prioritize and Plan Zero Trust Actions

- **Key Areas of Focus:**
  - Identity and Access Management (IAM): Implement MFA, least privilege, and continuous monitoring.
  - Device Security: Ensure devices are compliant and secure with tools like EDR.
  - Network Security: Adopt micro-segmentation and secure communications.
  - Application and Data Security: Implement encryption and monitor access.
- **Automation:**
  - Use automation to streamline security processes and reduce errors.

Electrosoft

4. Execute Pilot Programs

- **Pilot Implementation:**
  - Start with pilots for specific ZTA actions (e.g., MFA rollout, micro-segmentation).
  - Define success metrics and collect stakeholder feedback.
- **Iterative Process:**
  - Refine and expand successful pilots before broader deployment.



Electrosoft

5. Continuous Monitoring and Iteration

- **Periodic Reviews:**
  - Regularly assess progress against the strategic roadmap.
  - Adjust plans based on new risks, lessons learned, and evolving guidelines.
- **Iterative Improvements:**
  - Continuously improve ZTA capabilities, prioritizing impactful actions.

Electrosoft

6. Scale, Document, and Share

- **Phased Rollout:**
  - Gradually scale ZTA across the agency, ensuring each phase builds on previous successes.
- **Documentation:**
  - Maintain detailed records of strategies, challenges, and solutions.
- **Knowledge Sharing:**
  - Share lessons learned with other federal agencies to support broader ZTA adoption.

Electrosoft

7. Align with Compliance and Plan for the Future

- **Compliance:**
  - Ensure ongoing alignment with federal mandates (e.g., OMB M-22-09, Executive Order 14028).
- **Future-Proofing:**
  - Keep the ZTA strategy adaptable for future technological advancements and emerging threats.
- **Continuous Learning:**
  - Stay informed about Zero Trust developments to ensure the agency's ZTA implementation evolves with the cybersecurity landscape.

Electrosoft

Further Details

Electrosoft

Developing a ZTA Strategic Roadmap

- **Inventory and Risk Analysis:**
  - Begin by conducting a thorough inventory of all IT resources, end entities, and business processes, as recommended by NIST.
  - Use this inventory to identify risks that can be addressed through Zero Trust principles.
- **Prioritization:**
  - Develop a ZTA Strategic Roadmap that prioritizes actions based on:
    - Agency mission priorities and budgets.
    - Mitigating the highest cybersecurity risks.
    - Protecting the most critical resources.
- **Strategic Drivers:**
  - Consider other ongoing or planned initiatives that can impact ZT progress.
  - Align the roadmap with government mandates and deadlines.

Electrosoft

ZTA Action Implementation Plan

- **Current Status Assessment:**
  - Evaluate existing products or solutions already in use.
  - Identify gaps and weaknesses that inhibit full implementation of ZT actions.
- **Implementation Steps:**
  - Define objectives and target requirements for each new/improved ZT functionality.
  - Pilot projects to vet each new/improved ZT functionality and gauge it against specific success metrics.
  - Implement select pilots, document findings and lessons learned, and update the ZT Action Implementation Plan quarterly.
- **Monitoring and Iteration:**
  - Continuously monitor the progress of ZT implementation against predefined metrics.
  - Iterate on the implementation steps based on feedback and lessons learned, ensuring continuous improvement.

Overcoming Common Challenges

- **Resource Allocation:**
  - Securing the necessary budget and staffing for ZTA implementation.
  - Aligning resources with agency priorities and gaining executive support.
- **Change Management:**
  - Managing change is crucial to the success of Zero Trust implementation.
  - Communicating the benefits of ZTA to stakeholders, addressing resistance, and fostering a culture of security.
- **Technology Use:**
  - Integrating new ZT technologies with existing systems.
  - Selecting the right tools and solutions that align with agency needs and capabilities, considering both current and future technology solutions.

Tools and Technologies

- **Key Tools:**
  - Identity and Access Management (IAM): Ensuring secure access based on identity verification.
  - Endpoint Security: Protecting devices that access the network.
  - Network Segmentation: Isolating network traffic to reduce risk.
  - Data Encryption: Ensuring data security in transit and at rest.
- **Technology Selection:**
  - Selecting the right tools based on the agency's current environment, future needs, and specific ZTA actions.
  - Interoperability and scalability in technology selection.

Collaboration and Governance

- **Inter-Agency Collaboration:**
  - Critical importance of collaboration among federal agencies in sharing best practices, tools, and lessons learned.
  - Opportunities for agencies to leverage shared services and resources to streamline ZTA implementation.
- **Governance Approaches:**
  - Need for future governmentwide governance strategies to support long-term ZTA goals, including establishing clear policies, guidelines, and oversight mechanisms.
  - Role of continuous governance in adapting to evolving cybersecurity threats.

Conclusion

Electrosoft

Summary and Key Takeaways

- **Recap:**
  - Principles of Zero Trust Architecture.
  - Challenges of ZTA implementation.
  - Need for a phased, iterative approach to ZTA implementation.
  - Methodical approach to guide agencies through the complex Zero Trust journey.
- **Call to Action:**
  - Start the Zero Trust journey by conducting an inventory, developing a strategic roadmap, and taking incremental steps towards full ZTA implementation.
  - High importance of continuous improvement and adaptation in the face of evolving cybersecurity threats.

Electrosoft

Questions

Electrosoft

2024 PMIWDC CONFERENCE

Back to The Future

AUGUST 23 - 24, 2024

Thank You!

Email

sarbari@electrosoft-inc.com

LinkedIn

https://www.linkedin.com/in/sarbari-gupta/

Website

www.electrosoft-inc.com