InterSec
Ignite . Inspire. Innovate

Zer0 Trust

A Simplified Implementation Approach

Whitepaper

Foreword

As cyber-attacks become more prevalent, cybersecurity must rise to encapsulate, prevent, and recover against more varied and complicated threats.

Protecting enterprise resources, particularly sensitive data, and business-critical assets have become increasingly challenging as resources have become distributed across both on-premises environments and multiple clouds. Many users need access from anywhere, anytime, or on any device to support the organization's mission.

Data is programmatically stored, transmitted, and processed across different boundaries under the control of different organizations to meet ever-evolving business use cases like accelerated requirements of pandemic and digital transformation.

It is no longer feasible simply to enforce access controls at the perimeter of the enterprise environment and assume that all subjects (i.e., end users, applications, third-party providers, and other non-human entities such as APIs that request information from resources) within it can be trusted.

A Zero Trust Architecture (ZTA) addresses this challenge by enforcing granular, Zero Trust Architecture, whether located on-premises or in the cloud, for a remote workforce and partners based on an organization's defined access policy.

What is Zero Trust?

Zero Trust is an emerging cybersecurity best practice that is not new but has gained popularity in recent years with newly surfaced external attack vectors.

It is a fundamental change in how we approach security, and it can guide us through many challenges we face today as threats become increasingly sophisticated and complex.

The traditional cybersecurity tenet of “TRUST BUT VERIFY” has failed repeatedly for a new and better way of thinking in terms of “NEVER TRUST, ALWAYS VERIFY”.

In the past, perimeter-driven implicit trust was enough to validate any actor or network that had access to privileged data; nowadays this often leads to increased attack surface for attackers' leverage and lateral movement to take control of business-critical assets and Data for ransomware and extortion.

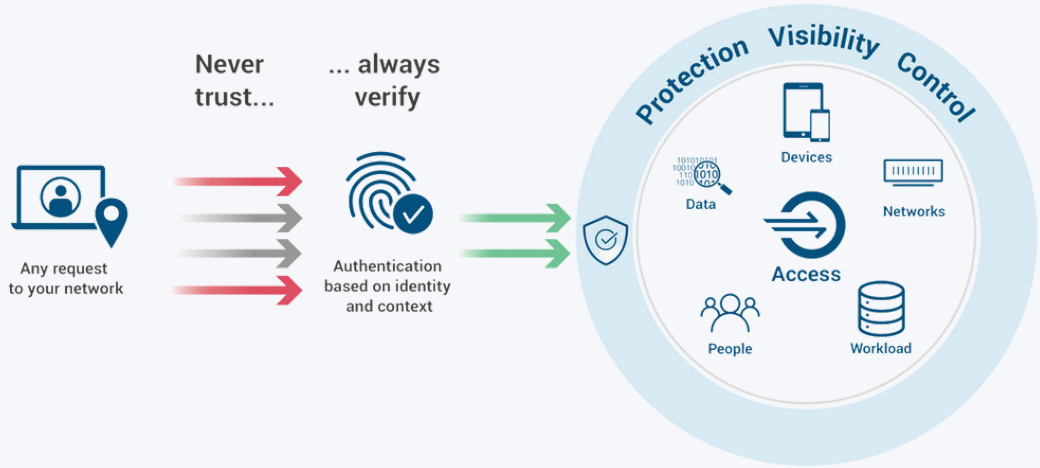
What Zero Trust is not?

- A product or solution
- Security Awareness Training
- A certification
- A fixed set of security controls

Zero Trust works towards granular, segmented systems and resources that ensure the least privilege to complete necessary business activities while protecting valuable assets against attacks.

It also constantly assumes compromised networks and assets, so when or if that happens, an organization is better prepared to handle and recover from attacks.

In Zero Trust, all network traffic is untrusted. This means that security professionals must ensure that all resources are accessed securely regardless of location and device, adopt the least privilege strategy, strictly enforce access control, and inspect and log all traffic.



In Zero Trust, all network traffic is untrusted. This means that security professionals must ensure that all resources are accessed securely regardless of location and device, adopt a least privilege strategy, strictly enforce access control, and inspect and log all traffic.

A Detailed Roadmap is Vital to Achieving Zero Trust

NIST SP 800-207 defines Zero Trust Architecture as a conceptual and architectural framework for moving security from a network-oriented, perimeter-based security model to one based on continuous verification of trust.

While this sounds simple, it requires both a shift in mindset and major changes in the deployment and use of security technologies. Creating a detailed roadmap that outlines the main work streams and projects necessary to protect business-critical resources and incremental implementation of the Zero Trust strategy is critical for success.

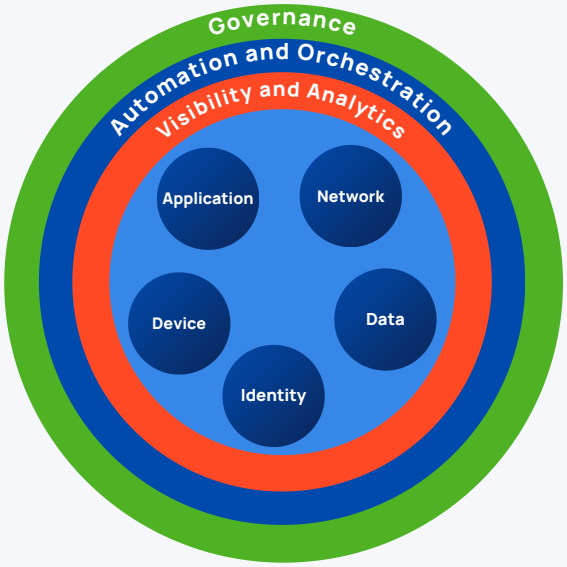
In addition, it shows executives exactly what is in the plan for incremental delivery, how much they will need to invest, and what specific business and security outcomes they will achieve through this investment, and this can drive business acceleration as an enabler.

Before beginning formalizing the organization roadmap, we recommend that the organization become familiar with the Department of Homeland Security (DHS) Critical Infrastructure Security Organization (CISA) Zero Trust Maturity Model (ZTMM).

The DHS CISA Zero Trust Maturity Model

CISA's maturity model has five pillars as foundational architecture for Zero Trust. However, compared to the traditional maturity model, Zero Trust allows for each of the pillars to be built up simultaneously, and independently of each other, targeting accelerated protection of sensitive data, applications, and systems communication.

This allows organizations to move towards Zero Trust maturity at their own pace and according to their immediate business needs that matter the most for incremental value. For example, an organization that has lackluster device security, initially, could work to improve on that pillar, over other pillars to bring efficiencies to deliver incremental value to the business.



Moving towards a more mature model includes an overlapping and interconnectedness of the five pillars and strives toward automated systems that use artificial intelligence and machine learning to monitor, mitigate, and control potential threats to organizations.

CISA ZTMM Pillars of Zero Trust

The pillars of Zero Trust are interconnected but can be built up independently. This allows organizations to prioritize which sections of their organization and resources are in the greatest need of protection to rebuild Zero Trust foundations eliminating the perimeter-driven architecture so that resources can be assigned and prioritized accordingly.

Identities

An Identity refers to an attribute or set of attributes that uniquely describe a user or entity authorized on behalf of organization resources to conduct business activities. Essentially, it is a person, system, department or division, entity, or the whole organization.

Organizations should ensure and enforce that the right users and entities have the right access to the right resources at the right time. Identity forms a core tenet of ZT. The least privilege access, which underpins Zero Trust, depends on the ability to confirm an entity's identity.

ZT moves away from implicit trust and passwords towards a combination of identity attributes to validate and continuously verify that identity throughout their interactions with services, data, and systems employed by the organization.

Identity ZT Maturity

Traditional

- Password or MFA authentication
- Lack of SSO between cloud and on-premises applications
- Visibility into identity risk is very limited

Advanced

- MFA, SSO, Least Privilege, and Just-in-Time access
- Cloud identity federates with on-premises systems
- Analytics improve visibility

Optimized

- Organization continuously validates identity, not just when access is initially granted.
- Global identity awareness across cloud environments and on-premise environments
- Fully orchestrate the identity lifecycle with dynamic user profiling, dynamic identity and group membership, just-in-time and just-enough access controls are implemented.

Devices

Devices are any hardware assets that can connect to an organization network such as laptops, servers, and phones including internet of things (IoT) devices and all that can establish two-way connectivity/ communication to the network.

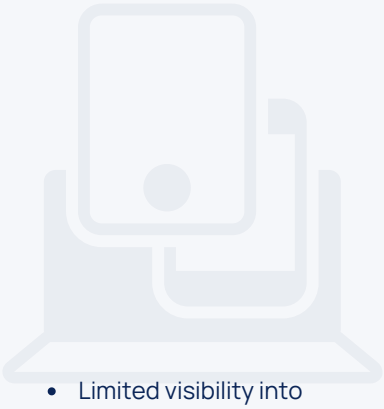
Organizations should inventory devices, secure all organizational devices, and prevent unauthorized device access to resources. Ensuring an organization's devices are secured is a fundamental component of ZT.

In practice, as the model matures, the focus should be on services and data on endpoints than the traditional access point. For example, instead of having access to a whole SharePoint site, giving minimal access to do the work.

This will just give the device access to the one or two services or data collections that users need to complete their workflows.

Strong access control will, in turn, bring device compliance and device integrity assurance.

Device ZT Maturity



Traditional

- Limited visibility into device compliance
- Access to data does not depend on visibility into the device that is being used to access the data.
- Simplified but error-prone and manually tracked device inventory.

Advanced

- Compliance enforcement mechanisms for most devices
- Access to data considers device posture on first access.
- Automated methods to manage assets identify vulnerabilities, and patch assets.

Optimized

- Constantly monitors and validates device security posture.
- Access to data considers real-time risk analytics about devices.
- Integrates asset inventory and vulnerability management across the organization environments, including on premises, cloud and remote.

Network

A network is an open two-way communications channel, 'intranet' including the organization internal network, wireless network, and 'public facing' Internet used to transport messages and other data with the external world

Organizations should segment (work towards isolating critical data and systems) and control networks to manage internal as well as external data flows. Network segmentation and protections are paramount in terms of priority; this allows the least privileged access to be configured or built in place of the implicit trust of traditional systems.

Organizations should evaluate where protections need to go; for example, a very select data set that is only ever accessed by limited users, a specific department or division should have protections that prevent anyone else from looking at it, as well as monitoring that department or limited users when they are accessing it.

When re-architecting network and micro-segmentation, ensure to take extra care and consider where to place these protections in the form of firewall rules.

Network ZT Maturity

Traditional

- Defines network architecture using large perimeter/macro-segmentation.
- Bases threat protections primarily on known threats and static traffic filtering.
- Explicitly encrypts minimal internal or external traffic.

Advanced

- Defines more of network architecture by ingress/egress micro-perimeters with some internal micro-segmentation.
- Includes basic analytics to proactively discover threats.
- Encrypts all traffic to internal applications, as well as some external traffic.

Optimized

- Network architecture consists of fully distributed ingress/egress micro-perimeters and deeper internal micro-segmentation based on application workflows.
- Integrates machine learning-based threat protection and filtering with context-based sensors/signals.
- Encrypts all traffic to internal and external locations, where possible.

Apps

These include organizational applications, systems, computer programs, and services that are operational on-premises, as well as in a cloud environment. Organizations should ensure that they secure, manage, and monitor the application layer, and containers and provide secure application development and delivery.

ZT emphasizes integrating protections on application workflows. This includes, but is not limited to, identifying actors, ensuring device compliance, and considering making applications available to users directly.

As the ZTA is being built, organizations may extend that model beyond the application itself and apply ZT principles to the development and deployment of the application.

Continuous integration and development models that integrate security testing and verification into each step of the process can alleviate future pitfalls; this, along with continuous monitoring, can assure the health and security of an application. Organizations should make sure they vet external and internal components of each application's workflow to ensure correct ZTA.

Apps ZT Maturity

Traditional

- Access to applications is primarily based on local authorization and static attributes.
- Threat protections have minimal integration with application workflows, applying general purpose protections for known threats.
- Critical cloud applications are directly accessible to users over the internet, with all others available through a virtual private network (VPN).

Advanced

- Access to applications relies on centralized authentication, authorization, monitoring, and attributes (IAM, IDAM, ICAM, and SSO with RBAC and ABAC.)
- Basic integration of threat protections into application workflows, primarily applying protections for known threats with application-specific protections.
- Cloud applications and some on-premises apps are directly accessible to users over the internet, with all others available through a VPN.

Optimized

- Continuously authorizes access to applications, considering real-time risk analytics.
- Strongly integrates threat protections into application workflows, with analytics to provide protections that understand and account for application behavior.
- All applications are context-aware, directly accessible to users over the internet.

Data

Organizations should protect and secure data on devices, networks, and applications, at rest and in transit including all storage devices. Organizations should inventory, categorize, and label data according to use and protection level (relevant data or personal and health records data to be protected such as PII and PHI.)

Data should be protected while at rest, and in transit, and deploy mechanisms for detection of data exfiltration. As organizations move towards an optimized ZTA, they must adopt a "data-centric" approach to cybersecurity. As you may recall, ZT focuses on "least privilege access" to protect valuable data and systems.

Organizations must identify, categorize, and inventory data assets. CISA recommends prioritizing data protections for their most critical data assets first (High-Value Assets, or HVA), and moving down to less critical assets over time.

This pillar of ZT is highly critical and tightly interconnect with other pillars. CISA offers a survey that will provide unique ZT maturity feedback, which organizations can use to identify security gaps and prioritize data protection.

Data ZT Maturity

Traditional

- Manually categorization of data and has poor data inventory, leading to inconsistent categorization.
- Governs access to data by using static access controls.
- Primarily stores data in on-premises data stores and where they are unencrypted at rest.

Advanced

- Primarily inventories data manually with some automated tracking. Organization performs data categorization using a combination of manual and static analysis methods.
- Governs access to data using least privilege controls that consider identity, device risk, and other attributes.
- Stores data in cloud or remote environments where they are encrypted at rest.

Optimized

- Continuously inventory data with robust tagging and tracking. Organization augment categorization with machine learning models.
- Access to data is dynamic, supporting just-in-time and just-enough principles, and continual risk-based determinations.
- Encrypts all data at rest.

Zero Trust Implementation

Engage both business and IT stakeholders in the development of the roadmap

Zero Trust implementation will require new investment or, at a minimum, shifting of investment, and it will also create an avalanche of technical and organizational change.

Identify the key players that are critical for your Zero Trust strategy and recognize that you will need to include at a minimum:

- The stakeholders (who are often the ultimate decision-makers) and business and IT executives (who will grant you the budget)
- Enterprise architects and application owners (who will ensure ZT supports the broader IT strategy and other projects),
- IT ops team (who will manage the infrastructure that you are building).

You must understand the concerns of each stakeholder and address them. Use interpersonal and communication skills to clarify the organization's Zero Trust vision, listen to the feedback, and communicate in a manner that each stakeholder can comprehend.

Identify interdependence with other security, IT, and business projects

A Zero Trust effort needs to include all existing security, IT, and business projects. These projects, from cloud migrations to engaging new business partners, can be the catalysts for Zero Trust transformation.

As you engage other stakeholders and participants, integrate the associated roadmaps into the Zero Trust effort. Ensure to properly map and clearly communicate project dependencies.

Plot Maturity to Discover Your Zero Trust Starting Point

Understanding your current maturity level and where you want to be in a given time frame will help you focus your projects and initiatives. For example, if you have a mature identity and access management (IAM) capability and have already implemented many of the necessary technologies from multifactor authentication to privileged identity management, you may wish to start with an area such as cloud workload security that is less mature.

To begin creating your detailed roadmap:

Establish your current baseline.

Assess your current Zero Trust maturity and establish a baseline of capabilities. For example, a government organization conducted a maturity assessment to understand its current state. The assessment highlighted that they required a large improvement of their IAM capabilities to enable Zero Trust. Use DHS CISA ZTMM maturity assessment to assess your current capabilities to implement the Zero Trust model.

Identify current business initiatives and existing security capabilities.

Before starting a Zero Trust initiative, learn what other business initiatives are in play. Based on our experience, public cloud migrations and other disruptive IT changes have often acted as a good vehicle for achieving a Zero Trust security model. For example, a Bank we worked with leveraged a move to Microsoft Azure to implement many Zero Trust tenets, making use of embedded cloud capabilities that were already being implemented to accelerate the journey. Security leaders should take advantage of these changes that the business has already sanctioned to deliver Zero Trust more effectively in their organization.

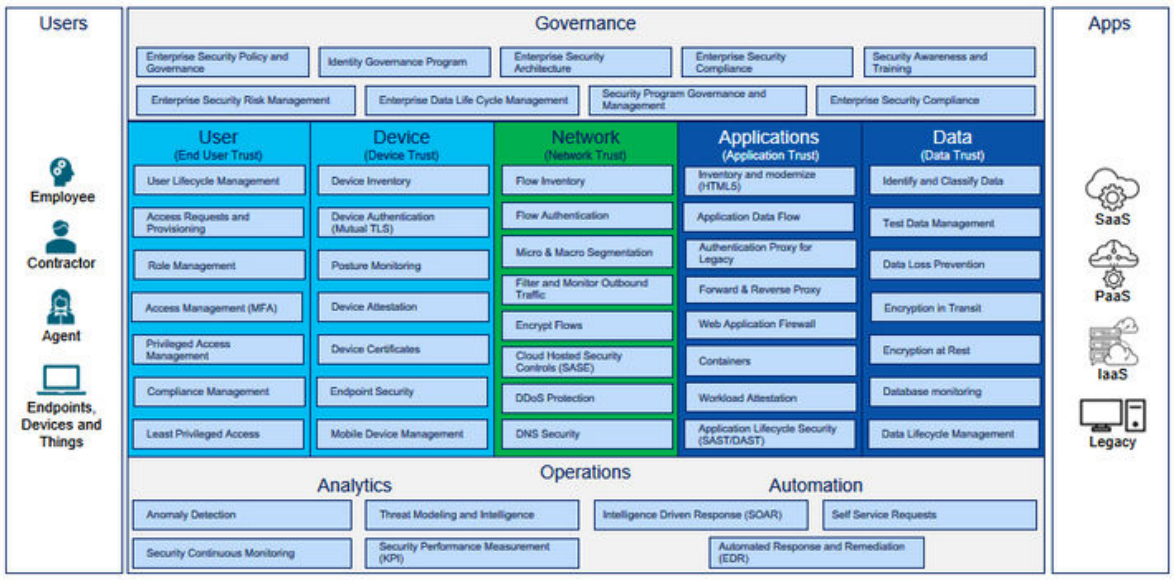
Set your desired maturity state and time frames to achieve.

Once you have conducted a maturity assessment, set the desired future stage maturity and time frame. Use the CISA ZTMM to target your next stage of maturity.

InterSec recommends a two-to-three-year horizon as a typical time frame to plan a detailed Zero Trust program roadmap. Most of the organizations we work with plan their Zero Trust roadmaps in this time frame to get a meaningful advance in maturity without necessarily expecting to achieve perfection. For example, one of our financial services clients determined its future state maturity for Zero Trust and security and decided to implement this strategy over three years.

Our Security Framework

Based on our experience delivering Zero Trust services, we have normalized various ZT frameworks in our own Zero Trust Security Framework. The core tenet of our Framework provides limiting the attack surface, reducing response time, improving user experience, and enhancing overall security posture by following the principles of Zero Trust.



All data sources and computing services are considered resources.

- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets. No asset is inherently trusted.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- 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.

Our Zero Trust Assessment Methodology

Our Zero Trust approach is a significant improvement over traditional perimeter-based defenses which have been deployed pervasively across most enterprise IT environments.

Recent attacks and modern technologies have made evident the need for a more granular and adaptive approach to security, which Zero Trust provides. InterSec uses a proven holistic approach that incorporates team-built tools and models that align with industry best practices and guidance.

While the Zero Trust Framework will describe how Zero Trust should be implemented and understood at a high level, organizations will require a methodology to assess its current state and measure progress towards a future state vision in the roadmap.

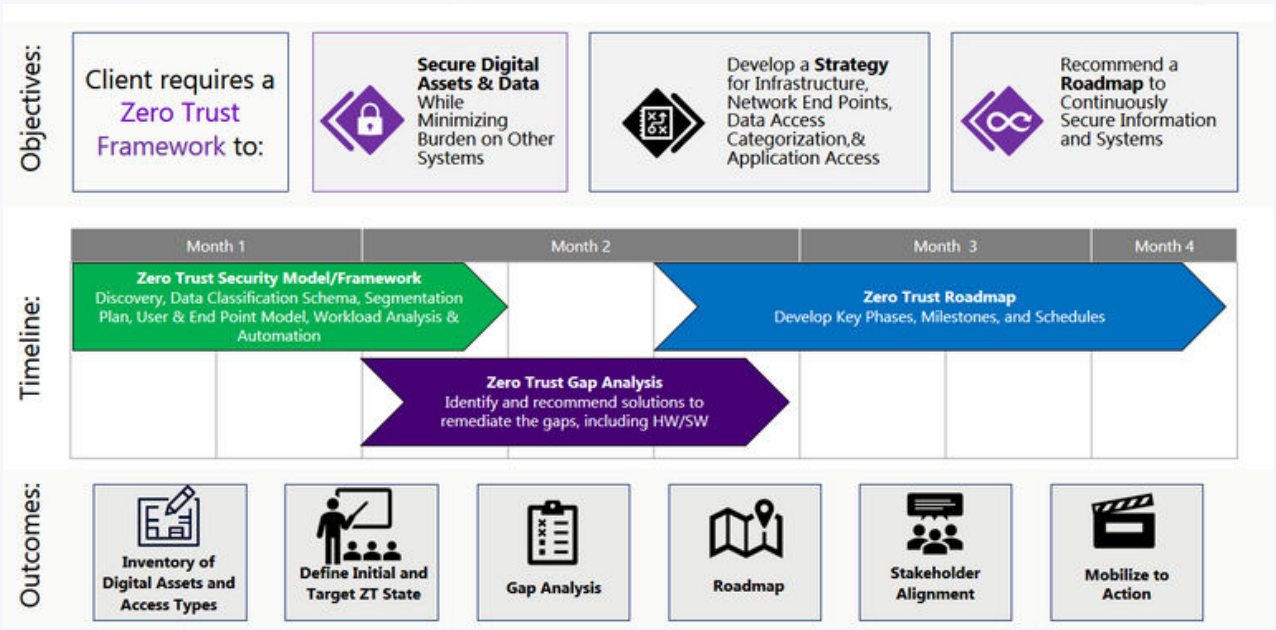
To accomplish this, InterSec will use a combination of in-person interviews and automation tools to understand an organization's business requirements and challenges. We bring the Total Access Control (TAC), a platform specifically designed to identify the effectiveness of the current cybersecurity infrastructure and to discover gaps in the Zero Trust Roadmap.

As shown below, our assessment project spans over 3 to 6 months depending on the complexity of the organization landscape starting with the inventory of assets, data classification, and access methods currently used.

Upon evaluation of assets and required protection levels in implementing Zero Trust foundations, we establish Current and Target architecture for Zero Trust so that fit-gap analysis can be conducted for a future state. An incremental roadmap will be presented to ensure business alignment and how it can deliver business value and outcomes as an organization gets ready for implementation efforts.

InterSec will be available in consulting and advisory capacity if there were any challenges in executing the implementation of Zero Trust and its roadmap.

InterSec Zero Trust Strategy Engagement



We have performed over 50 assessments using various frameworks such as NIST 800-37 RMF, NIST CSF, Ransomware Assessment, High-Value Asset Assessment, and Zero Trust Assessment. This has helped us develop internal assets and accelerators, partner with strategic vendors, and bring our experienced team to execute assessments with minimum friction and on time.

Benefits of our approach

4-12X Faster Than Manual Assessments

By automatically assessing an organization's ability to defeat the latest threats, TAC automates over 60% of access test activities – increasing assessment speed by 4-12X.

Test Zero Trust Control Efficacy

Traditional compliance checklists and vulnerability scans do not tell you if controls are effective. TAC automates tests against threats to prove efficacy.

Continuous Validation and Monitoring

With direct integration into ServiceNow and RSA Archer, TAC can continuously test and validate Zero Trust controls and populate the organization's ZT maturity scores.

Tailored Zero Trust Scoring and Maturity Model

TAC has built a flexible scoring methodology that allows consultants to tailor and implement their scoring rubric and maturity evaluations.

“Zero Trust is a Journey, not a Destination”

InterSec
Ignite . Inspire. Innovate

Ready to start your Zero Trust Journey?

Please contact us at inquiries@intersecinc.com
Call us at (833) 228-4858 (toll-free)

Website: www.intersecinc.com
NAICS Codes: 541511, 541512, 541519
GSA Multiple Award Schedule Contract: 47QTCA19D00EG
54151S – Information Technology (IT) Professional Services,
54151HACS – Highly Adaptive Cybersecurity Services (HACS), and OLM – Order Level Materials.