Zero Trust Planning

CCZT Study Guide

cloud security alliance®

CCZT™
Certificate of
Competence in Zero Trust

The official location for SDP and Zero Trust Working Group is
https://cloudsecurityalliance.org/research/working-groups/zero-trust/

Disclaimer

Cloud Security Alliance designed and created this Zero Trust Training course study guide (the "Work") primarily as an educational resource for security and governance professionals. Cloud Security Alliance makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Version Number: 20240820

About Cloud Security Alliance

The Cloud Security Alliance℠ (CSA) (www.cloudsecurityalliance.org) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. Cloud Security Alliance harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. Cloud Security Alliance activities, knowledge and extensive network benefit the entire community impacted by cloud—from providers and customers, to governments, entrepreneurs and the assurance industry—and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA Address

709 Dupont St.
Bellingham, WA 98225, USA
Phone: +1.360.746.2689
Fax: +1.206.832.3513

Contact us: support@cloudsecurityalliance.org
Website: https://cloudsecurityalliance.org/
Zero Trust Training Page: https://knowledge.cloudsecurityalliance.org/page/zero-trust-training
Zero Trust Advancement Center: https://cloudsecurityalliance.org/zt/
Provide Feedback: support@cloudsecurityalliance.org
CSA Circle Online Community: https://circle.cloudsecurityalliance.org/
Twitter: https://twitter.com/cloudsa
LinkedIn: www.linkedin.com/company/cloud/security/alliance
Facebook: www.facebook.com/csacloudfiles
CSA CloudBytes Channel: http://www.csacloudbytes.com/
CSA Research Channel: https://www.brighttalk.com/channel/16947/
CSA Youtube Channel: https://csaurl.org/youtube
CSA Blog: https://cloudsecurityalliance.org/blog/

Acknowledgments

Dedicated to Juanita Koilpillai, a pioneer in software-defined perimeters whose contributions to the Certificate of Competence in Zero Trust (CCZT), Zero Trust training, and CSA are immeasurable.

The CCZT and Zero Trust training was developed with the support of the Cloud Security Alliance Zero Trust Expert Group, whose members include volunteers from a wide variety of industries across the globe. Made up of subject matter experts with hands-on experience planning and implementing Zero Trust, both as cloud service consumers and providers, the Zero Trust Expert Group includes board members, the technical C-suite, as well as privacy, legal, internal audit, procurement, IT, security and development teams. From cumulative stakeholder input, the Zero Trust Expert Group established the value proposition, scope, learning objectives, and curriculum of the CCZT and Zero Trust training.

To learn more about the CCZT and Zero Trust training and ways to get involved please visit: https://cloudsecurityalliance.org/education/cczt

We would also like to thank our beta testers, who provided valuable feedback on the CCZT and Zero Trust training: https://cloudsecurityalliance.org/contributors/cczt-contributors

Lead Developers:

Alex Sharpe
Clement Betacorne
Heinrich Smit
Mark Schlicting
Michael Herndon
Michael Roza
Prasad T.
Richard Lee
Shruti Kulkarni
Sky Hackett

Contributing Editors:

Aunudrei Oliver
Emilio Mazzon
Ledy Eng
Matt Lee
Ron Kearns

Expert Reviewer:

Agnidipta Sarkar
James Lam
Jaye Tillson
Robert Morris
Roland Kissoon
Ron Martin (Dr.) , PhD
Vani Murthy
Farid Gurbnov

CSA Global Staff:

Anna Schorr-Campbell
Chandler Curran
Adriano Sverko
Daniele Cattedue
Noelle Scheck
Hannah Rock
Leon Yen
Stephen Smith

Table of Contents

List of Figures

Course Intro

Welcome to Zero Trust Planning by the Cloud Security Alliance (CSA). This training module is part of a larger series titled the Certificate of Competence in Zero Trust (CCZT). In this course, learners will get an in-depth look at the crucial facets of ZT planning, from initial considerations such as stakeholder identification and supply chain risk, to organizational security policies, to compliance. Use cases for prioritization, scoping, and gap analysis are also covered.

Course Structure

This course consists of 8 units, each geared towards helping learners gain competency in the following topics:

1. Starting the Zero Trust journey
2. Planning considerations
3. Scope and priority
4. Gap analysis
5. Defining the protect surface and attack surface
6. Documenting transaction flows
7. Defining policies for Zero Trust
8. Developing a target architecture

Course Learning Objectives

After completing this course, learners will be able to:

- Demonstrate understanding of the ZT maturity model, and how it supports an organization's ZT planning process
- Identify the crucial ZT planning steps and key considerations
- Understand ZT pre-requisites and common ZT use cases
- Possess a working knowledge of how industry-recognized methods (e.g., gap analysis, risk register, RACI diagrams) fit into a ZT planning process
- Demonstrate an understanding of the concepts of protect and attack surface
- Demonstrate understanding of how to map organizational data flows within the scope of the ZT approach
- Demonstrate an understanding of how to plan ZT policies
- Demonstrate an understanding of variables to consider when planning for a ZT target architecture

1 Starting the Zero Trust Journey

Congratulations, your board of directors and senior management are committed to starting the organization's ZT effort. Now your journey begins!

The following roadmap identifies the primary phases of your organization's journey to ZT and maps them to the respective units and sections covered in this module.

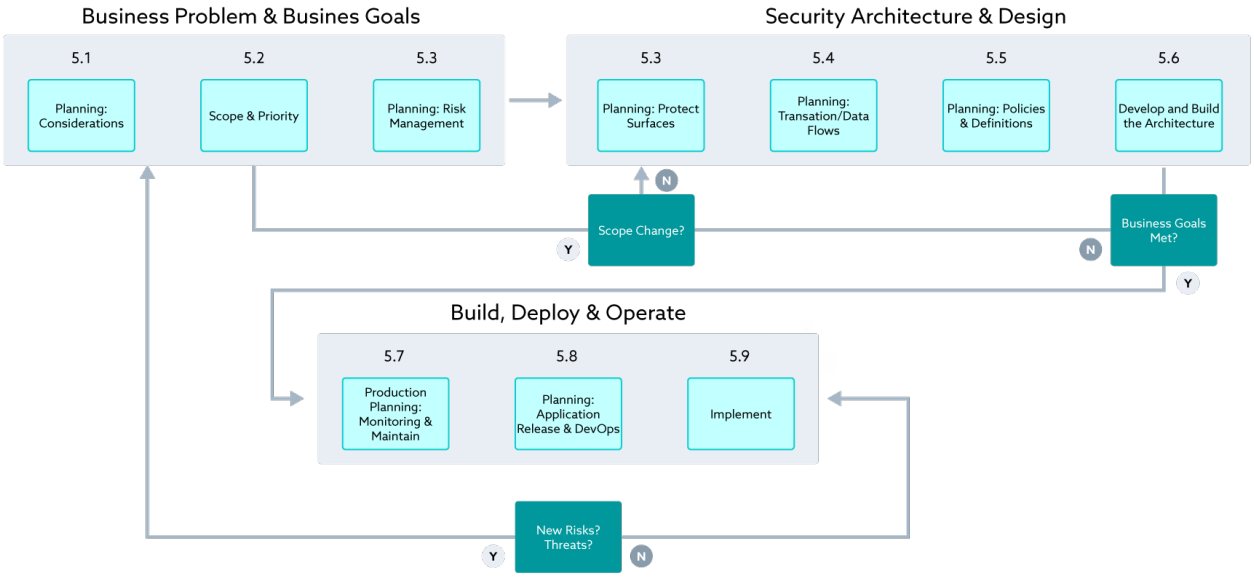

Figure 1: *The ZT Journey Roadmap*

During the course of this module, we explore the various considerations and steps to plan your ZT journey. During ZT planning, the primary focus should be aligning activities and resources to achieve business outcomes, with acceptable risk levels defined by the board of directors and senior leadership.

In this unit we will cover:

- Module assumptions
- Initial considerations

1.1 Module Assumptions

It is most likely that ZT will be implemented in an existing environment with existing controls (in either on-premises, hybrid, or cloud-only scenarios). However, this module applies to completely new implementations as well. While these considerations are similar to implementation in existing environments, they have little or no dependencies on existing business systems and may be implemented more deeply and quickly. Additionally, this module focuses on items specific to ZT and presumes that learners possess foundational knowledge in areas like project planning, enterprise risk

management (ERM), information security (InfoSec), systems engineering, and enterprise architecture design.

The module also assumes an understanding of core ZT principles, including the following:

- **Never trust; always verify:** Claimed identities and authorized entitlements should be verified before access is granted to assets.
- **Inside-out security:** Starting with the assets, the mission-critical elements that are most valuable or vulnerable should be protected.
- **Risk-based security approach:** ZT planning efforts should stem from risk-driven business decisions; that is, assuming budget scarcity, the organization should allocate resources based on risk and opportunity. For example, the decision to protect a specific asset should depend on how it contributes to the company's financial value and its criticality to the organization's mission.

To foster learning and clarity, this course treats the ZT initiative as an atomic unit; in reality, a single organization may pursue a portfolio of initiatives with different motivations and success criteria. In general, larger organizations will likely pursue a portfolio of ZT initiatives based on geography, line of business (LOB), function, regulatory concerns, and more, while smaller organizations may only have a single ZT effort. For example, a multinational, publicly-traded enterprise may pursue three ZT initiatives—one in Europe to address General Data Protection Regulation (GDPR) compliance requirements, another for the firm's manufacturing business in South America, and a third for its U.S.-based operations. In contrast, a privately held small and medium-sized business may pursue a single ZT project to fulfill requirements when bidding for government projects with ZT-related requirements.

1.2 Initial Considerations

A plan for implementing ZT philosophy, approach, and design principles should consider the following five steps, as outlined in the 2022 U.S. National Security Telecommunications Advisory Committee (NSTAC) Report to the President[1]:

1. Define the protect surface: Identify the data, applications, assets, and services (DAAS) elements to protect.
2. Map the transaction flows: Understand how the networks work by mapping the transaction flows to and from the protect surface, including how various DAAS components interact with other resources on the network. These transaction flows provide insight to help determine where to place proper controls.
3. Build a Zero Trust Architecture (ZTA): Design your ZTA, tailored to the protect surface, determined in steps 1 and 2. The way traffic moves across the network specific to the data in the protect surface determines design. The architectural elements cannot be predetermined, though a good rule of thumb is to place the controls as close as possible to the protect surface.

[1] NSTAC. (2022). NSTAC Report to the President on Zero Trust and Trusted Identity Management.

4. Create a ZT policy: Instantiate ZT as an application layer policy statement. Use the Kipling Method[2] of ZT policy writing to determine who or what can access your protect surface. Consider person and non-person (services, applications, and bots) entities.
5. Monitor and maintain the network: Inspect and log all traffic, all the way through the application layer. The telemetry gathered and processed from this process helps prevent significant cybersecurity events and provides valuable security improvement insights over the long term. As a result, each subsequent protect surface can become more robust and better protected over time.

Figure 2: *Five-Step Process for ZT Implementation*[3]

Proper risk management should form the basis of any competent cybersecurity approach, as establishing a framework for identifying and mitigating risks is crucial for minimizing project failure and, in the case of already existing system deployments, disrupting existing systems and business processes. ZT migration tactics depend on the organization's risk profile and risk appetite. For some, ZT design principles will be applied to a limited set of assets; others will apply ZT to all assets across the organization. In either case, the migration to ZT will follow a risk-based, staged approach with numerous iterations culminating in the final transformation into a ZT-driven organization.

Frameworks and models such as the Cybersecurity and Infrastructure Security Agency (CISA) *Zero Trust Maturity Model*[4] can provide organizations at the start of their ZT journey with a reference roadmap for charting their transition towards a ZTA.

[2] NSTAC. (2022). NSAC Report to the President on Zero Trust and Trusted Identity Management. Table 3: Key Zero Trust Foundational Concepts and Definitions.
[3] Figure adapted from: NSTAC. (2022). NSTAC Report to the President on Zero Trust and Trusted Identity Management.
[4] CISA. (2023). Zero Trust Maturity Model (Version 2.0).

1.2.1 CISA High-Level Zero Trust Maturity Model

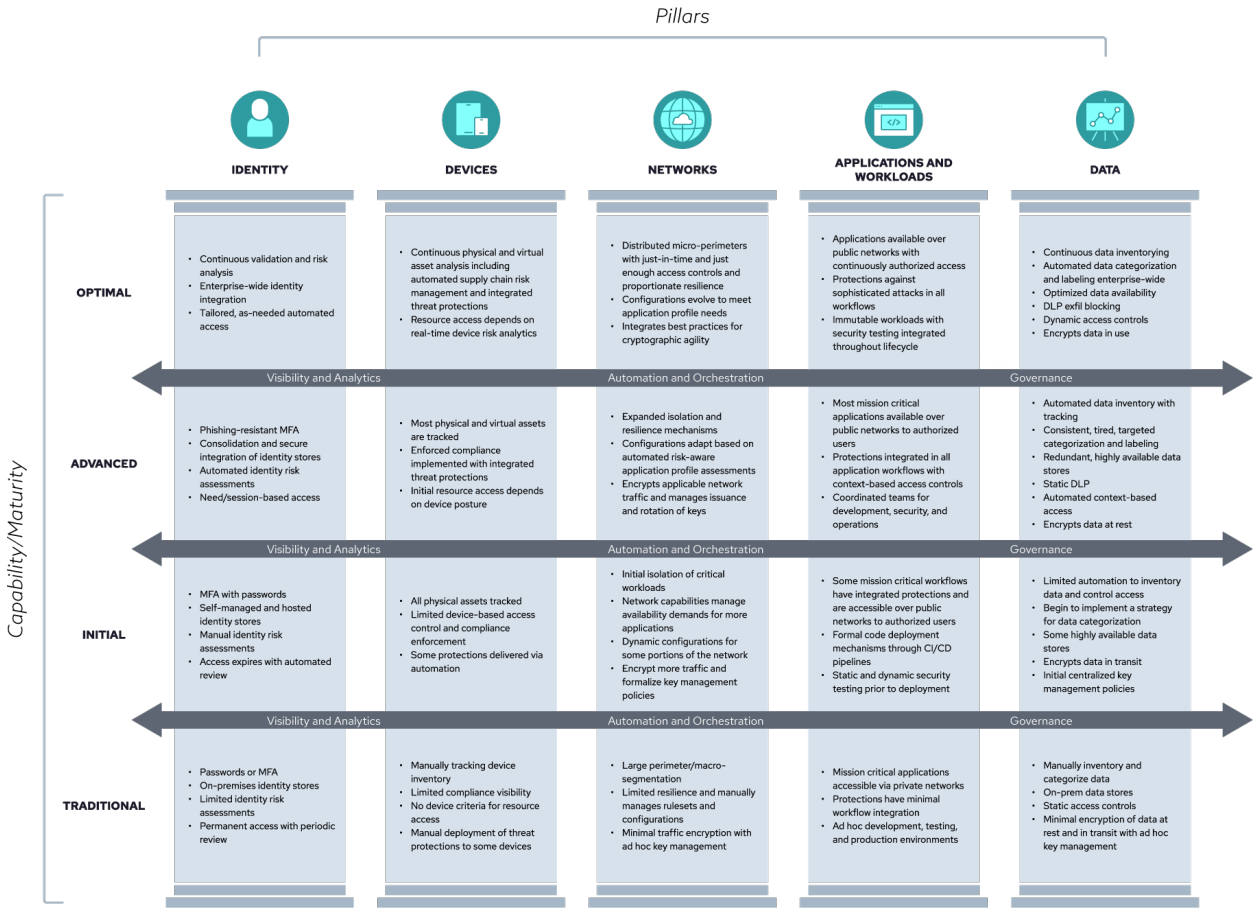

Figure 3: *CISA High-Level ZT Maturity Model*[5]

CISA's *Zero Trust Maturity Model* consists of five pillars, three cross-cutting capabilities, and four cross-functional maturity stages that together form the crucial foundations for ZT. In some diagrams (i.e., from the US Department of Defense[6]), the cross-cutting capabilities (Visibility and Analytics, Automation and Orchestration, and Governance), are depicted as foundational pillars. This representation emphasizes the significance of incorporating these capabilities into the planning process as they assist in defining objectives for the five pillars.

The five pillars are:

- Identity
- Devices
- Networks
- Applications & Workloads
- Data

[5] Figure adapted from: CISA. (2023). Zero Trust Maturity Model (Version 2.0).
[6] U.S. Department of Defense. (2022). DoD Zero Trust Strategy.

In this course, as well as in our other courses, the three capabilities (represented by arrows) are discussed individually due to their frequent need for revision and modification. Additionally, the arrow that lists these capabilities is intentionally repeated several times to highlight the importance of implementing tasks or projects to adapt them as your organization progresses from a traditional model to more advanced security stages.

CISA's *Zero Trust Maturity Model* also consists of several stages. Traditional, the first stage, is where most companies will likely find themselves before embarking on their ZT implementation journey. Attempting to reach the highest level of maturity in a single implementation is impractical and virtually impossible. By incorporating the maturity model into planning discussions, teams will be able to focus on setting clear expectations regarding the desired outcomes for each iterative ZT implementation they commit their resources to.

The four maturity stages, along with a brief example of their criteria, are as follows:

> - **Traditional** - Utilizes multi-factor authentication (MFA), employs manual deployment of threat protection, and maintains an on-premises network
> - **Initial** - Implements MFA with passwords, tracks all physical assets, initiates isolation of critical workloads, and employs formal deployment mechanisms through the CI/CD pipeline
> - **Advanced** - Implements phishing-resistant MFA, tracks most physical and virtual assets, makes most mission-critical apps available over public networks, automates data inventory with tracking, and encrypts data at rest
> - **Optimal** - Engages in continuous validation and risk analysis, grants resource access based on real-time device risk analysis, establishes distributed micro perimeters with just-in-time (JIT) and just-enough access controls, conducts continuous data inventorying, and encrypts data in use

The CISA *Zero Trust Maturity Model* outlines specific examples of Traditional, Initial, Advanced, and Optimal ZTA elements within each pillar. For example, an organization beginning its ZT journey (e.g., it has not yet implemented ZT) may find itself at the traditional tier. According to ZT principles, the organization still would not have enough protection or security even after moving to the initial tier. The two lower maturity stages fail the organization because they lack essential features for a secure and effective ZTA. In this example, the organization would want to move to a future state of advanced and optimal tiers to manage access control effectively. Which would require implementing authentication and identity management, authorization, encryption, monitoring and logging, data protection, and segregation of duties. In later sections (Gap Analysis, Developing a Target Architecture), the CISA *Zero Trust Maturity Model* will be covered more in-depth as a tool for moving across tiers.

2 Planning Considerations

Planners should consider several key factors and variables prior to undertaking the organization's journey to ZT. These include, but are not limited to:

- Stakeholders to engage
- Technology strategy
- Business impact analysis (BIA) results
- The risk register
- Supply chain risk management
- Organizational security policies
- Architecture options
- Compliance requirements
- Workforce training

These key considerations have far-reaching implications on the organization's ZT planning efforts. For example, results from stakeholder identification, BIA, and risk register development activities should dictate how subsequent policies are created.

2.1 Stakeholders

Though seemingly straightforward, stakeholder identification is a critical step that, in practice, requires a significant, concerted time and energy investment. More than any other, this stage can make or break the organization's ZT effort.

Stakeholders include, but are not limited to:

- Business/service owners
- Application owners
- Infrastructure owners
- Service architecture owners
- CISO/security teams
- Legal officers
- Compliance officers
- Procurement officers

Once stakeholders are identified, planning efforts should proceed to mapping out their respective responsibilities, and a communications plan should be developed.

2.1.1 Stakeholder Responsibilities

Stakeholder identification efforts should result in a Responsible, Accountable, Consulted, and Informed (RACI) chart and communications plan. Also referred to as a responsibility assignment matrix, a RACI chart maps out task roles and responsibilities to streamline project management efforts. The RACI chart should reflect the cloud's shared responsibility model, as well as the ability to delegate responsibility, but not accountability—the risk register also shares both attributes.

IT will likely run the organization's ZT initiative daily, with sponsorship by business units, risk management, compliance, or the CISO. Both sponsors and stakeholders should be relevant to the ZT initiative's expected business outcomes. As a starting point, governing documents approved by senior management and the board of directors should designate the executive sponsor and provide insights into reporting expectations.

The most critical ZT-specific role is the asset owner, who will more than likely reside in the business units. As part of their data governance role, the asset owners determine valid users, valid roles, privileges, data usage, and more. Because ZT is an inside-out strategy based on asset value, identifying both assets and asset owners is crucial. However, asset owners should not be confused with asset custodians (e.g., database administrators), who are responsible for implementing directives set by asset owners. Asset owners typically exist in the business while asset custodians are almost always part of IT.

Organizations pursuing ZT should not lose focus on other internal users and groups in human resources (HR), legal, risk management, audit teams, end users, and senior management. An effective, well-informed ZT initiative must consist of stakeholders spread across the organization and at all levels, including functional areas. Functional areas should be consulted or informed, at the bare minimum. For example, HR should serve as the primary source of truth for the organization's identity, while procurement should serve as the source of truth for contractors and vendors. Internal audit, compliance, and the CISO office will likely play crucial roles in the go-live approval.

Bringing in stakeholders across the organization early and keeping them engaged helps the ZT initiative remain well-balanced and focused. To this end, stakeholders should be well-informed of the organization's collective mission and ongoing priorities in order to avoid operational conflicts, aid in prioritization, and ensure the most efficient assignment of resources.

2.1.2 Stakeholder Communications

A communications plan is an essential enterprise tool and is especially critical to a ZT initiative. Because of ZT's prescribed, fundamental philosophical changes and enterprise nature, organizations should develop and adhere to a well-designed communications plan; chiefly, the document should serve as a roadmap for team communications with stakeholders, staff, customers, business partners, and regulators. At a minimum, the communications plan should:

- Define a communication strategy, including tools and any required guidance
- Establish cadence (e.g., forums, format, etc.)
- Incorporate mechanisms for setting proper expectations with interested parties
- Include a means to communicate and document key decisions

2.2 Technology Strategy

Most organizations have a technology strategy consisting of the principles, objectives, methods, plans, processes, and budget for using technology to achieve business objectives. At the beginning of their ZT journey, organizations need to ensure that ZT planning activities are happening in the context of the broader technology strategy. In other words, the ZT strategy and planning need to take into account the existing technology strategy and then update that technology strategy.

During the planning process, organizations should be asking themselves the following essential questions:

- How does the ZT strategy fit into the organization's technology strategy?
- How does the ZT strategy need to be updated to incorporate the technology strategy?
- How does the ZT strategy impact existing plans, processes, and procedures?
- How does the ZT strategy affect existing budgets and investments?
- How does the ZT strategy affect existing internal standards and best practices?

2.3 Business Impact Assessment

Larger organizations operating in highly regulated environments and firms with mature ERM programs are likely to have already carried out a recent BIA. A BIA provides organizations with a list of assets followed by their relative values and owners, valuable information like recovery point objective (RPO) and recovery time objective (RTO), interdependencies and priorities, and an assessment of resources required to restore and maintain each asset. Based on this information, organizations can establish more comprehensive and accurate service level agreements (SLAs), business continuity/disaster recovery (BC/DR) plans, third-party risk management (TPRM) programs, as well as streamline prioritization and stakeholder identification efforts for ZT planning.

2.4 Risk Register

In a similar vein, organizations with a mature ERM or InfoSec program are likely to have developed a risk register containing an inventory of potential risk events, recorded and tracked by likelihood, impact, and description. The risk register should also contain controls for reducing risk levels within the organization-defined risk appetite thresholds, along with the risk owner and the control owner.

With a well-developed risk register, organizations are better equipped to understand what cyber risks their ZT implementation will mitigate. However, the risk register will require continuous updating as the organization adopts new technologies and its infrastructure evolves. For example, the ongoing shift to expanded connectivity and the cloud mandates shared responsibility, and while responsibilities can be outsourced or delegated, accountability cannot. In this case, the risk register must be updated to reflect the cloud's shared responsibility model.

2.5 Supply Chain Risk Management

Modern organizations exist as ecosystem players on a myriad of fronts, from retailer order fulfillment logistics to outsourced human resources. When it comes to technology acquisitions and implementation, the same applies—whether software, hardware, or cloud-based services. Solutions on the market are, to a greater or lesser degree, an assemblage of components developed by third parties. As a result, an organization's visibility into its supply chain is limited by nature, since many components are outside the organization's control. Attestations regarding the validity, security, and quality of third-party components are typically the primary driver behind the organization's technology acquisition decisions.

Crucially, ZT planning considerations should address supply chain risk, since lack of visibility into potential third-party exposures and security glitches (e.g., coding errors, intentional or unintentional hardware or software back doors, unpatched libraries) could result in a data breach or compromise. In the absence of a ZT approach, supply chain participation requires organizations to inherently trust that the initial processes, degree of scrutiny, and approvals to use third-party components in downstream offerings (e.g., hardware, software, or systems) were sufficient; as a result, the required assumption is that the third-party risk of that technology acquisition was and remains acceptable.

Several tools and frameworks can help organizations better understand and mitigate supply chain risk in their ZT implementations. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 presents ZT tenets that apply to a supply chain and its supplier organizations across all ZT pillars, namely Identity, Devices, Networks, Applications and Workloads, and Data. Since 2018, the National Telecommunications and Information Administration (NTIA) has pursued the concept of a software bill of materials (SBOM) as a tool for advancing supply chain risk management, with CISA having announced its intent to support this work. This effort aims to create a mechanism for exposing software components, enabling organizations to make better risk decisions when deciding what software products to incorporate into their products or offerings.

Additionally, the following non-exhaustive list of tools and resources can help organizations in determining supply chain risk:

- CSA STAR Program[7] (STAR Level 1 and STAR Level 2)
- ISO 27001 assessments
- SOC 1 and 2 assessments
- Systems audits
- Bridge letters & attestations
- Supplier organization and service offering reputation research

With these frameworks, tools, and resources at their disposal, organizations can apply ZT principles in evaluating potential supply chain risk exposures more comprehensively and effectively.

2.6 Organizational Security Policies

ZT planners should keep in mind that various policies will change across all domains (e.g., HR, identity and access management [IAM], technical, and privacy). Also, pre-existing policies affect how ZT will be implemented. From a ZT perspective, organizational policies affecting identity, devices, networks, applications and workloads, and data should be considered for updates, at the very least.

These policies are designed to provide direction across the enterprise. The policies updated (or created) for ZT will be provided to the team(s) for implementation.

The most relevant policies will fit into roughly three categories:

1. Policies that dictate or constrain the ZT initiative
2. Policies that require updating due to ZT
3. Policies that need to be created to support ZT

[7] https://cloudsecurityalliance.org/star/

While the list of relevant policies and how they fit into each category vary widely between organizations and potentially groups within organizations, the following are common policy types for a ZT initiative:

- General IT and security
- ZT
- Data governance
- Cloud
- Key management policy
- Incident response
- User and IAM
- Monitoring
- Disaster recovery (DR)
- Business continuity (BC)

2.7 Architecture

During the ZT planning process, especially in the early stages, planners should identify the relevant architecture capabilities and components that could impact ZT or require updating due to ZT. These capabilities may include architectural frameworks such as The Open Group Architecture Framework (TOGAF)[8], Sherwood Applied Business Security Architecture (SABSA)[9], CSA's *Enterprise Architecture Reference Guide*[10], and other less formal frameworks and standard organizational configurations. It is also necessary to identify key components such as architecture requirements repositories, architecture landscapes, solution landscapes, and standards information bases. Architecture will be discussed in greater depth in later sections.

2.8 Compliance

At this time the United States is at the global forefront in the pursuit of ZT. For instance, U.S. government agencies have produced artifacts that provide critical ZT guidance like the NSTAC *Report to the President on Zero Trust and Trusted Identity Management*, and the NIST Cyber Security White Paper (CSWP) 20[11], to name a few. Other jurisdictions like Europe and Asia are also preparing ZT guidance or regulations.

However, even without fully realized ZT-based regulations and laws, the ZT approach can be invaluable in achieving compliance with existing cybersecurity and data privacy laws and regulations. A ZT approach will be helpful in two ways:

- First, it will increase control over regulated data by enforcing controls that foster accountability and by segregating data within dedicated micro-segments.
- Second, it will drive better overall cybersecurity, which in many cases exceeds most existing legal and regulatory requirements.

[8] The Open Group Architectural Framework. (2022). The TOGAF Standard, 10th Edition.
[9] Sherwood Applied Business Security Architecture. (2009). SABSA White Paper (W100).
[10] Cloud Security Alliance. (2021). Enterprise Architecture Reference Guide.
[11] NIST. (2022). Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators (CSWP 20).

Implementing ZT across an organization or system impacts all in-scope architectures. This implies that potentially every system, control, and process will change. These potential impacts across the organization should be kept in mind during the planning phase. Potential impacts, considerations, and updating needs may surface in unforeseen areas (e.g., infrastructure support, incident management, BC/DR, and end-user support).

2.9 Workforce Training

As one the most critical aspects for the success of a ZT journey, training is undoubtedly a key component of every cyber security program and represents a foundational component of the ZT approach, despite being often left to the last minute. Because ZT is essentially a paradigm shift, it will benefit from a shift in existing training programs along with the typical user training that accompanies any technology rollout. Your organization most likely has a training and awareness program and a security awareness program. ZT principles should be integrated into the security awareness program in all phases — onboarding, role changes, yearly reviews, drip feed, and termination.

Special attention needs to be paid to the training of the:

- Staff who determines access controls
- Staff who configures the access control rules
- Support Team, including the Help Desk, who need to be ready to handle the paradigm shift is paramount to a smooth transition
- Staff who audit what has been done, including IT audit and security audit
- Upper management who need to fully embrace the cultural shift that ZT might impose

Finally, it is important that the board of directors and CEO have the necessary level of awareness to be able to fully understand the progress and challenges of the ZT project.

3 Scope, Priority, & Business Case

As mentioned at the start of this module, the ZT approach should be regarded as a journey of several stages, eventually taking the organization to a state where the business operates on a ZT model. Each stage of the journey should be seen as an individual project.

The organization may start its ZT journey with a project focused on a critical protect surface, then expand onto the rest of the organization's protect surfaces. In the event that the organization has identified several critical protect surfaces, the key questions are prioritization-related: Where does the ZT journey start? How does that define the scope of the initial ZT project? The answers to these questions are discussed in the next section, while protect surfaces are covered more in-depth in a later section.

ZT concerns securing the protect surface to reduce the risk of data and process-compromise. To do this, the protect surface's data, assets, processes, and the identities that access it must be comprehensively understood and mapped out. The organization may choose to include one or several protect surfaces in a project.

Regardless of the number of protect surfaces in a project, organizations at this stage should start with the prerequisites for understanding the protect surface, followed by a definition of the ZT project's scope and priorities, and lastly, a development of a business case. The last section in this unit provides several examples for assessing scope and priorities per use case.

3.1 Prerequisite to Understanding the Protect Surface

The first step in defining the priorities within a ZT journey is understanding what the organization wants to protect using a ZT approach. In other words, the starting point for prioritizing ZT efforts is identifying the data and assets that the organization seeks to secure, the location of the data, the asset where data is hosted, and the services, processes, and classifications.

To this effect, several prerequisite actions need to take place in order to have a clear understanding of the organization:

- Data and asset discovery and inventory
- Data and asset classification
- Entities/user discovery and inventory

3.1.1 Data & Asset Discovery & Inventory

To effectively protect its data, the organization needs to know where that data resides. This can be achieved with data discovery activities. At a minimum, more mature organizations will have a current asset inventory that contains a list of itemized data, devices, applications, services, and more, followed by an assessment of each asset's value.

Ideally, the asset inventory will exist in the form of an up-to-date, automatically updated configuration management database (CMDB) that contains all the relevant information about the assets (e.g., hardware, software, devices, etc.) and the inter-component relationships. As ZT is driven by the asset's value, the CMDB should be viewable based on these models and parameters.

Alternatively, in the absence of an asset inventory, the organization may decide to run a data discovery activity using automated tools, followed by the population of a CMDB with the metadata obtained during the data discovery activity.

3.1.2 Data & Asset Classification

With a new or existing asset inventory on hand, the organization must classify data and assets based on the sensitivity of data handled by the business transaction. Data and asset classification activities are meant to be a prerequisite for any ZT project. This helps in the identification of the protect surface and enables organizations to plan for the proper security controls in their ZT implementations. It also plays a crucial role in identifying relevant regional laws and regulations that may apply to the organization.

3.1.3 Entities/User Discovery

The discovery of entities, both person and non-person users, is another essential prerequisite before the scope of a ZT project can be defined. In order to be able to access the organization's IT assets and data and carry out business transactions, those entities need to have an identity assigned and eventually a set of different personas.

These entities may be person or non-person users (e.g., machines, service accounts, APIs). Organizations should understand whether the entities run transactions in the background and whether they are authorized to run the transactions after being authenticated. The discovered entities should be mapped to all relevant protect surfaces, (creating an inventory of entities/users) and their identities used to define the ZT policies discussed in later sections.

3.2 Scope

Once the prerequisites are met, the organization needs to define the scope of the ZT project. Scope would typically include:

- Success criteria identified for the ZT projects
- Business units that are identified for the ZT journey
- Protect surfaces that are part of the business units, including identification of:
  - The data and the assets that are part of the protect surface
  - The identities that access the protect surface
  - The entities mapped to the identities/personas

3.3 Priority

Once the scope is identified, the organization needs to determine how and in what priority to implement ZT. Some approaches to this include the following:

- **Prioritization based on complexity:** Building from simple to complex, the organization may choose to select a smaller, simpler protect surface as a pilot project and progress to more complex protect surfaces. This approach allows a better understanding of the ZT project life cycle, document learnings, and apply them to the next set of protect surfaces. Starting small and simple makes it easier to apply the relevant planning considerations.
- **Prioritization based on risks:** Selecting a protect surface high on the risk register may help in scenarios where the organization has experienced security compromises or incidents involving protect surfaces. This approach may help reduce any cyber risks brought about by access control. After completing the high-risk protect surface projects, the organization may then move on to lower-risk projects.
- **Prioritization based on use case:** This approach is suitable for organizations with a definite use case in mind. Use case examples are provided later in this unit.

3.4 Development of a Business Case for ZT Planning

After the identification of data, assets and identities, classification of data, and the critical processes are identified, the organization can move forward and define a business case that would justify why a certain asset should move under the protection of a ZT approach.

The business case is supposed to be briefed and approved by senior leadership and most likely, the board of directors. This will outline expectations, motivations, funding, and any other requirements that the team may choose to share.

Most mature organizations have existing business case templates which should be utilized for this purpose. Factors to be considered in the business case would include:

- The BIA
- The risks that the ZT program is designed to address
- The cost of the project (e.g., capital costs, operational costs, resourcing and administration costs)
- The cost of not doing the project (i.e., the impact of not implementing ZT), to include costs incurred due to any data breaches or security incidents involving access controls
- What the organization stands to gain through ZT (e.g., ease of access administration, reduction of the visible attack surface, and more)
- Additional benefits that come about through improving the organization's security culture

ZT adoption may help the organization position itself favorably among competitors. For example, a software as a service (SaaS) provider may include ZT in its marketing collateral and sales materials to demonstrate the optimal security posture of its platform as well as its forward-thinking commitment to protecting customer privacy.

3.5 Use Case Examples

The following use case examples can help organizations anticipate priority and scope-related concerns regarding specific access types and environments.

3.5.1 Role Based Access Control for Internal Staff

Assuming that the organization has implemented network segmentation, network zones, and micro-segmentation with different security requirements, administrators can define policies accordingly. For example, a soap manufacturing company may place all the trade secrets related to soap recipes and formulas in a network segment that only server administrators and recipe/formula engineers can access. Implementing ZT means that any malicious movement using compromised credentials is preempted with device verification, thus securing trade secrets.

3.5.2 Remote Access

Remote access is the new normal way of working. Remote access users include (but are not limited to) employees, contractors, temporary staff, suppliers, etc. Remote access also opens the possibilities for lateral movement via compromised access controls. Administrators mitigate this risk with technology like virtual desktop infrastructure (VDI) and/or corporate cloud workstation resources and by publishing applications and resources. However, application jailbreaking may be a residual risk in these scenarios.

Using ZT, administrators can define policies such that remote workers access only those applications and resources for which they are authorized. This reduces the attack surface that is available to remote workers. The attack surface can also be reduced with device authentication before granting access to users. As you may recall, device authentication relates to ZT's "verification before granting access." Administrators may also integrate opportunistic MFA with their ZT controls for behavior analysis and geofencing.

3.5.3 Services Accessed Using Mobile Devices

Organizations subscribe to services that can be accessed from mobile devices (e.g., smartphones, tablets). Services like HR portals, portals for salary/wage slips, and office directories can be accessed via mobile applications and web applications run on browsers. To ensure that compromise of users' credentials do not lead to compromise of data, ZT policies can aid in authenticating the users and their devices before granting access to the services. Additionally, MFA can be configured with ZT. As ZT policies can be made as granular as possible, separation of duties between the users and administrators help prevent any privilege escalation attacks. A caveat is that it should not be assumed that ZT can prevent access to these services via stolen devices.

3.5.4. Third-Party Service Providers with Remote Access

Administrators can leverage ZT policies to authenticate third-party users and their devices to determine the required access privileges for resources while hiding all other assets to prevent any lateral movement. This helps reduce the attack surface for any supply chain risk materialization.

3.5.5 Staff Access to Assets in Hybrid Environments

Staff access to root accounts for cloud services such as AWS and Azure should be tightly controlled. Lack of awareness or speed to market may make staff miss out on controls like configuring MFA for such resources. Administrators can configure ZT policies for such accounts and subscriptions, thus ensuring that the same policies are applied to all accounts. In addition, these accounts and subscriptions remain hidden behind the policies leading to reduced visibility in the public domain resulting in reduced attack surface.

3.5.6 SaaS & PaaS

SaaS and platform as a service (PaaS) require access at two levels. One is access to the service and the second is access to the features within the service. Implementing ZT will help define attribute-based access control (ABAC) for the features within the service. For example, granting database administrators (DBAs) access to the master database in a SQL database-as-a-service but not to data persisted in user databases.

The applications are often consumed for managing the organization's private or sensitive data. It is important to ensure that only legitimate users can access the application, though it is a cloud-hosted one. ZTA can be designed such that access to the application or platform is allowed only for the traffic coming from the ZT gateway. Thus the user and the entity can be subjected to the validations and policies before sharing access to the assets. The design can be achieved via SAML authorization, where the SAML requests from the gateways alone are accepted at the SAML service provider residing at the SaaS/PaaS application.

3.5.7 Application Release & DevOps

High-velocity application release practices like DevOps and its supporting automation and continuous integration/continuous delivery (CI/CD) framework require thoughtful integration with ZTA. ZTA can be integrated with DevOps to secure authorized connections to the various deployment environments (e.g., development, test, staging, and production) to ensure proper connectivity to protected servers and applications. ZTA can provide a better developer experience by streamlining access provisioning. Ideally, ZTA should be integrated into the application stack to fully leverage its security features.

During planning for ZT implementation, the following usage areas need to be considered:

- Secure remote access during the application release cycle
- Access to individual protected servers and applications
- Integration of ZTA into the application stack

Common DevOps practices such as the use of virtualized environments and containers can streamline ZTA integration; that said, security architects must fully understand the chosen ZTA deployment model and how their organization's DevOps mechanisms will interact and integrate with it. When it comes to DevOps toolset integration, security teams should carefully review and evaluate third-party APIs and repositories supported by their ZTA implementation.

3.5.8 Industrial Control Systems, Operational Technology, & Internet of Things

Industrial control systems (ICS), operational technologies, and the Internet of Things (IoT) rely on generic non-user identities (service accounts, resource accounts, roles, etc.) to access resources. However, these identities can be enabled with interactive logon rights for users—a feature that can be potentially compromised or abused. Furthermore, investigating security events involving interactive

logon rights is challenging, as logging only records generic identity names, not the name of the user behind the generic identity. Implementing ZT in these environments ensures that identities have only the required access to assets for the task at hand, thereby limiting the attack surface in the event the identities are compromised.

4 Gap Analysis

A gap analysis is an industry-accepted tool that allows organizations to determine how to best realize their objectives. At its core, a gap analysis is a three-step process that compares where the organization is with where it wants to be and then defines a road map to close the gap. Most organizations have a preferred gap analysis framework like Strengths, Weaknesses, Opportunities and Threats (SWOT)[12], the McKinsey 7-S Framework[13], or the Nadler-Tushman Congruence Model[14], to name a few. Depending on the size of your enterprise, you may undertake several gap analyses for different business units, geographies, and functions.

A gap analysis consists of the following steps:

- Determine current state
- Determine target state
- Create a roadmap to close the gap
- Requirements

4.1 Determine Current State

The first step in the gap analysis is to make an objective, comprehensive assessment of the organization. Ideally, prior third-party assessments, maturity models, frameworks, and other existing resources can help inform this effort. For example, the *CISA Zero Trust Maturity Model* provides organizations with a framework to assess their current state regarding ZT adoption.

The following are crucial steps for determining the organization's current state:

- Define the current protect surface(s) and the implications for each ZT pillar: Identity, Devices, Networks, Applications & Workloads, and Data
- List current controls for each pillar, focusing on the protect surface for each respective pillar
- Determine and declare the current CISA maturity stage for each pillar

For example, an organization defining its current protect surface regarding data has determined that most of its data-at-rest is being stored unencrypted. Additionally, the organization is still using traditional password-based authentication for its systems and continues to rely on local authorization for security access to application workloads.

[12] Humphrey, A. (1960). SWOT Analysis.

[13] McKinsey & Company. (2008, March 1). Enduring Ideas: The 7-S Framework. McKinsey Quarterly. Retrieved 2023, January 20.

[14] Nadler, D., and Tushman, M. (1980). A Model for Diagnosing Organizational Behavior. Organizational Dynamics 9, no. 2.

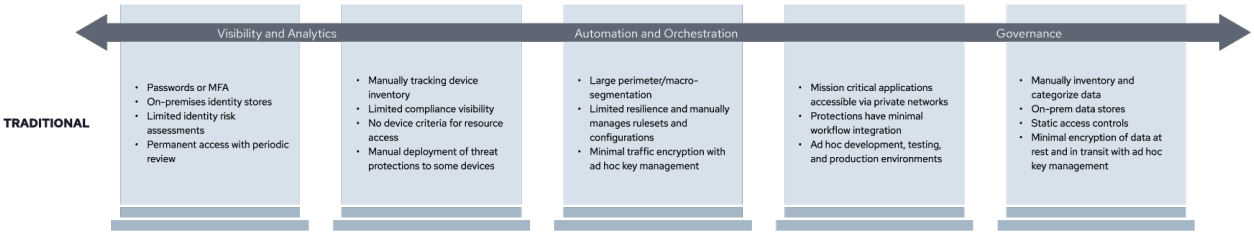

Figure 4: *CISA Zero Trust Maturity Model: Traditional*[15]

Per the CISA *Zero Trust Maturity Model*, a firm storing its data unencrypted falls into the Traditional tier; the same is true of this organization's application workload and identity protect surfaces. Part of this process also involves determining risk appetite, which should feed into scoping activities and decisions when the future state is decided/selected.

4.2 Determine the Target State

Once the planner, user, or organization has a solid understanding of the current state, the next step in the gap analysis is to determine the target state. During this second phase, the goal is to: Define the protect surface and the impact for each in-scope pillar across the organization (i.e., what each should look like when ZT has been implemented).

Determine and declare the desired target CISA maturity stage for each pillar. The CISA *Zero Trust Maturity Model* represents a gradient of implementation attributes across five distinct pillars, where minor advancements can be made over time toward optimization.

Regarding the previous example, the organization may determine that achieving an Optimal ZT maturity stage, while ideal, may be prohibitive due to several factors. The organization may require more long-term vetting of AI/ML technologies and may be unable to encrypt all of its stored data across each environment. The organization may elect to adopt MFA as its future state to bolster the identity protect surface, and to start with encryption at rest for cloud and remote environments to bolster the data protect surface.

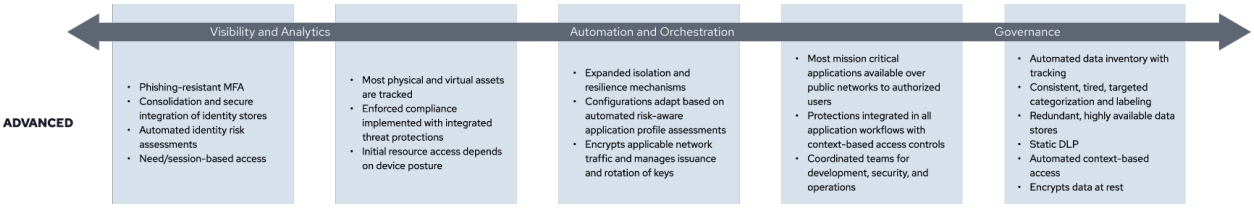

Figure 5: *CISA Zero Trust Maturity Model: Advanced*[16]

The organization's target ZT maturity stage and future state should ultimately fall under the Advanced or Optimal tier. However, achieving this requires a gradual evolution through incremental steps, first exhibiting characteristics of the Initial tier, then proceeding to the Advanced tier, and finally reaching the Optimal tier in all areas. As risk appetite was defined when determining the

[15] Figure adapted from: CISA. (2023). Zero Trust Maturity Model (Version 2.0).
[16] Figure adapted from: CISA. (2023). Zero Trust Maturity Model (Version 2.0).

current state, the scope is defined when determining the target state based on those previous assessments.

4.3 Create a Roadmap to Close the Gaps

Once an organization knows where it is and where it is going, it should create a roadmap of the required future state across all pillars. During the roadmap phase, the organization should compare the current state and maturity stage to the desired state and maturity stage, listing the future controls required to raise the current maturity stage to the future desired state.

For example, the organization mentioned previously must now plan for bridging the identified gaps between its current Traditional maturity stage and target state. By establishing the foundational ZTA, the ZTA can evolve to effectively manage access control, implement more encryption, increase data protection, and add segregation of duties and principles. Once this is integrated into operations, detailed risk assessments can be made, along with appropriate response plans for all risks related to compromised data or access control points.

The roadmap should include all the controls and procedures necessary to bring the organization from a Traditional to an Advanced maturity stage. As a simple example, in the Traditional approach, it is perhaps enough to have a login screen and get to enterprise-sensitive data or business functionality with a single password. For your initial ZT implementation (Initial stage), you couple the login screen with MFA requirements. In a subsequent ZT implementation project (an Advanced stage), you add safeguarding technologies so that the MFA process cannot be leveraged by a bad actor for phishing attacks. In a ZT implementation that further advances your login and MFA processes, you add enterprise-wide agents that can track network activity (Optimal stage). Now, your organization can set up monitoring consoles and security experts can be flagged to spot seemingly dangerous activity, enabling them to take corrective measures before a security breach can occur.

4.4 Requirements

One of the key outputs of the gap analysis will be requirements for ZTA implementation. There is a large body of work for requirements analysis. The following section focuses on key items unique to ZT.

How to define and document your requirements will largely depend on whether your ZT effort is stand-alone or part of a larger effort. If ZT is part of a larger effort, it is recommended to collect your requirements in a ZT-specific section to maintain focus. This may not be practical in all situations but should be the objective. If ZT is a stand-alone effort, you have the luxury of a dedicated requirements document that can be used by the project team.

Either way, a primary focus in the early phase(s) of planning will be to solidify your identification, entitlement, and access control infrastructure. At a minimum, you want to be sure you have requirements defined for:

- Source of truth for unique identities
- Management of those identities through the full life cycle of employees, contractors, and vendors

- Definition, provisioning, and management of entitlements
- Definition, provisioning, and management of access controls
- Segmentation/micro-segmentation
- Incident detection and response
- Reporting and analytics
- Special considerations (e.g., devices)
- Concept of least privilege
- Segregation of duties

5 Define the Protect Surface & Attack Surface

The following unit covers the crucial activities for identifying the protect surface and attack surface, outlines how the protect surface and attack surface are interrelated, and provides key considerations for designing the two surfaces to complement each other.

5.1 Identify the ZTA Protect Surface

Malicious actors compromise data confidentiality, integrity, and availability via improper access. Subsequently, ZT aims to reduce cyber attacks and data breaches through more stringent access requirements, that is, by requiring authentication and authorization prior to granting access to resources. Hence, to reduce cyber risk in this manner, organizations must understand and identify data and their locations. As data cannot exist in a vacuum and needs a house (i.e., the asset) to live in, the data and asset both need to be identified, as well as their respective criticality levels.

Extending this premise to the organization at large, ZT planners should define what needs to be protected in an organization, also known as its protect surface. NSTAC defines the protect surface as the area the ZT policies protect. Each protect surface contains a single DAAS element, and in turn, each ZT environment will have multiple protect surfaces.

5.2 Identify the Attack Surface

Along with defining and defending the protect surface, organizations should also define the attack surface—the surface through which data and assets can be attacked. NIST defines an attack surface as "The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment." [17]

Organizations more often experience difficulties in defining the attack surface for defense purposes, since defining an attack surface at a given point in time for most organizations can be a moving target due to the evolving usage patterns of devices and assets (e.g., BYOD, SaaS). In contrast, a protect surface has a defined boundary.

[17] NIST. (2018, October). Glossary: attack surface. NIST Computer Security Resource Center. Retrieved 2023, January 20.

The diagram below illustrates the Zero Trust Architecture as defined by NIST, originally in the SP 800-207[18], and then further elaborated in SP 1800-35B[19] draft.

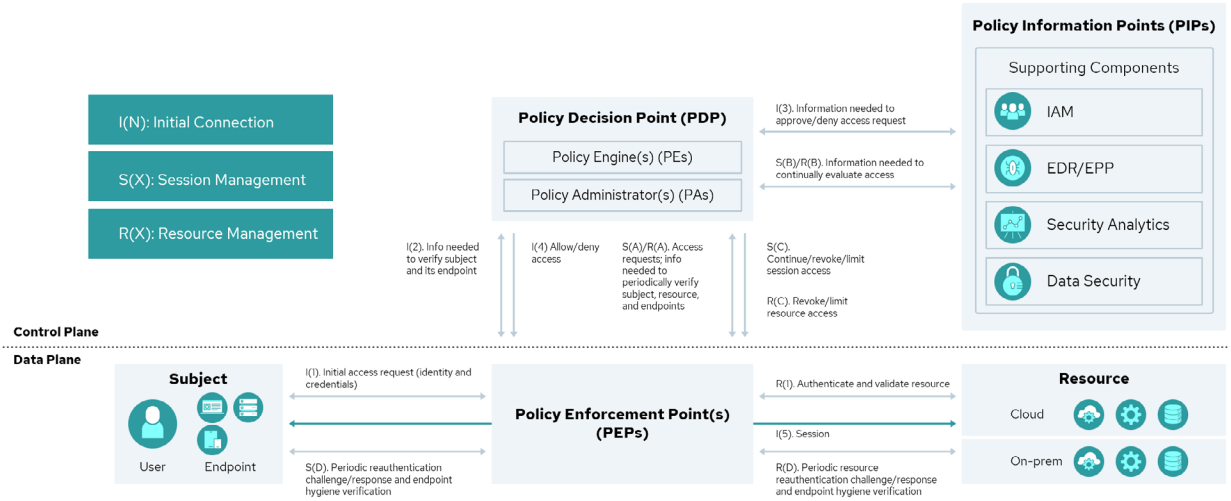

Figure 6: *General ZTA Reference Architecture*[20]

Applying the NIST definition to the above diagram, the attack surface is identified as follows:

- Endpoint
- Information flow between the endpoint and policy enforcement points (PEPs)
- Information flow between PEP and resource
- Information flow between PEP and policy decision point (PDP)
- Information flow between PDP and policy information points (PIPs)
- Policies
- Identity and access management used by ZT
    - End users' identities
    - API identities
- The application stack for PEP, PDP, and PIP
- The solution in the supply chain

The identified attack surface can be analyzed for threats, abuse cases, and mitigations as illustrated in the table below, an example of attack surface-focused threat modeling using STRIDE, a common threat modeling methodology championed by Microsoft.[21]

[18] NIST. (2020). Zero Trust Architecture (SP 800-207).

[19] NIST. (2022). Implementing a Zero Trust Architecture (SP 1800-35B). Second preliminary draft.

[20] Figure adapted from: NIST. (2022). Implementing a Zero Trust Architecture (SP 1800-35B). Second preliminary draft.

[21] Microsoft. (2009, November 12). The Stride Threat Model. Microsoft Learn. Retrieved 2023, January 20.

Attack Surface	Threat	Abuse Case	Mitigation
• Information flow between PEP and Resource • Information flow between PEP and PDP • Information flow between PDP and PIPs	• Spoofing • Tampering • Information disclosure	• A malicious actor can perform a man-in-the-middle attack to spoof the user of the resource • A malicious actor can intercept and manipulate data on the information flow channel between the resource and the PEP, between the PEP and the PDP, and between the PDP and the PIP	• Use TLS certs certifications as described in the Encryption section • Use mTLS for 2-way authentication
Endpoint and its environment	• Spoofing	• A malicious actor (malware/phishing attack), may try to harvest credentials used by the endpoint to log into the ZT endpoint agent	• Onboard the ZT endpoint agent as described in the earlier modules • Employ user- based / machine- based certificate for authentication (as recommended in Introduction to Zero Trust Architecture)
Policies configured on PIP/PEP/PDP	• Tampering • Information disclosure	• A malicious insider can try to add/ modify policies	• Use the supplier due diligence process to check if this is a possibility in the vendor's environment- (background checks, RBAC on the backend, etc.) • Logging and possible sharing of logs with customers

PDP and PIP administration console	• Spoofing • Elevation of privileges • Repudiation	• A malicious actor may try to spoof administrators to access the administration console for policies	• Use MFA to address spoofing threats via credential harvesting • Check for assurance from the vendor that an administrator cannot access the data belonging to a different organization • Logging of all actions carried out by an administrator with a possibility of sharing the logs with the customers
IAM for ZT users	• Spoofing	• Identity providers may become compromised leading to the harvesting of users' credentials by malicious actors	• Identity provider is assessed for security to make sure it is fit for purpose

Supply chain of ZT	• Spoofing • Tampering • Repudiation • Information Disclosure • Denial of Service (DoS) • Elevation of privileges	• Lack of governance, risk, and compliance in the ZT organization leading to lack of line-of-sight visibility to security posture in the organization. • Insider threat leads to the exfiltration of customer data • Vulnerabilities in the management plane / software components leads to the compromise of policies • Lack of vendor controls results in DoS for customers • DoS at the application layer • Lack of OS hardening, secure configuration, host-level intrusion detection, and network layer intrusion detection • Vulnerabilities on the management console lead to SQLi, XSS, and lateral privilege escalation for customers	• Information security management system implemented and practiced in the organization • Conduct background checks for the staff that works with customer data • Vulnerability management program to upgrade and update technologies that compromise the ZTA • Secure SDLC to ensure the management console is developed securely • Web application firewall (WAF) drops any packets that can result in DoS at the management console • Underlying infrastructure components (server endpoints, web servers, application servers, containers, etc.) are hardened, secure configuration is applied, host intrusion detection is enabled, file integrity monitoring is enabled, etc.

Table 1: *Example STRIDE Threat Model*

5.3 Illustration of Protect Surface & Attack Surface

The credit card example below illustrates the protect surface and attack surface:

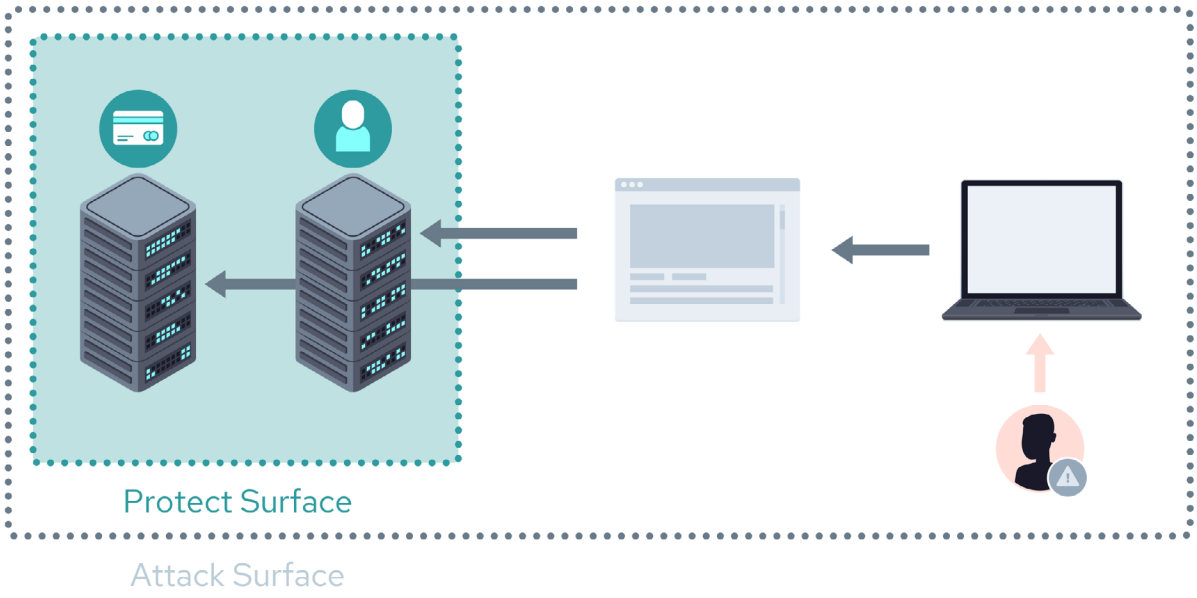

Figure 7: *Attack Surface and Protect Surface: Credit Card Example*

The cardholder data, personally identifiable information (PII), and underlying assets (i.e., server) comprise the protect surface, since any unauthorized access to the assets may subsequently lead to unauthorized data access, resulting in a data breach. Consequently, these assets should be covered with ZT policy that requires entity verification for asset and data access to ensure that such breaches do not occur.

Then the organization permits end-users and administrators to access cardholder data and PII housed on the server via an application accessible through their laptop's browsers. These laptops, browsers, and servers are potential entry points for malicious actors; any vulnerabilities or lack of hardening on the asset may enable malicious actors to compromise the server and data. Hence, the attack surface encompasses the end-user and administrators' devices and applications, as well as the protect surface.

The attack surface can increase with the addition of another laptop and a cloud service. This is because the entry points to the data increase with added assets and devices.

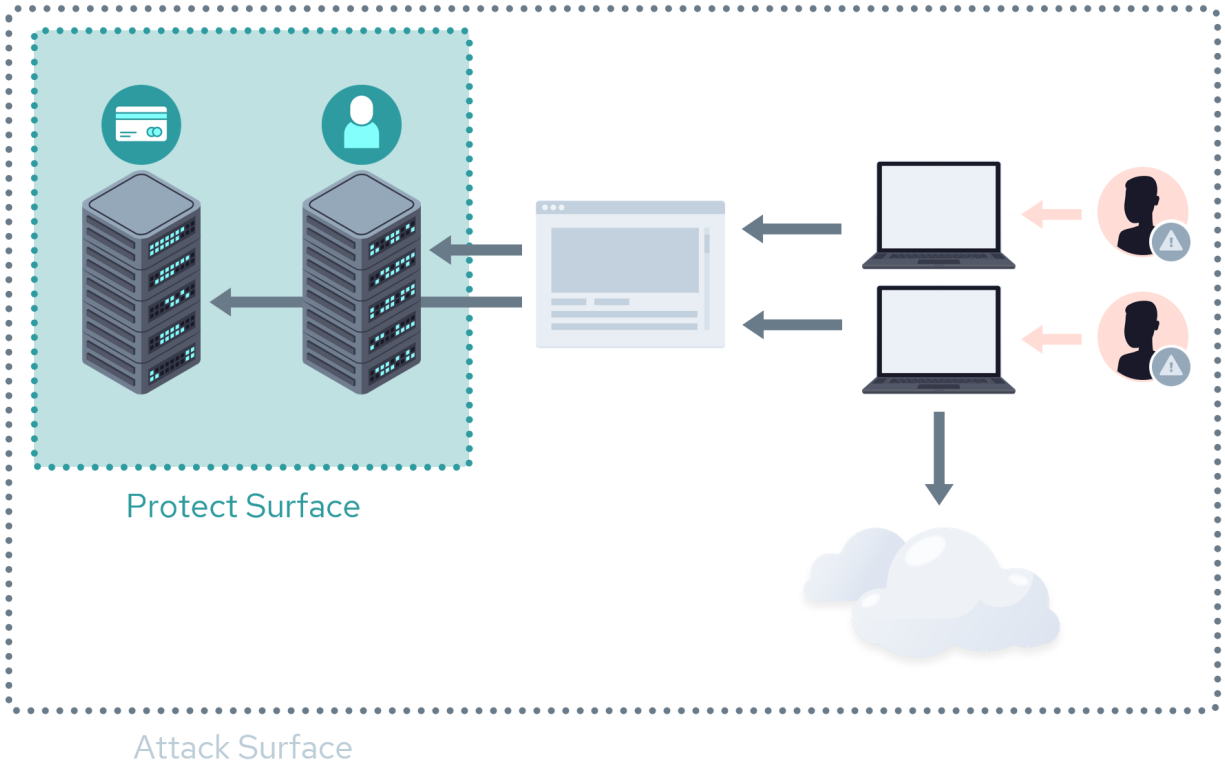

Figure 8: *Laptop and Cloud Services Expand Attack Surface*

However, the protect surface remains the same and is, therefore, more stable and constant than the attack surface. That said, the stability of the protect surface means:

- At the onset, it essentially identifies all the data and assets an organization should protect
- Along with data, it allows the organization to identify the location of the data, the assets that hold the data, and the critical services that the data requires to provide business functions

Once data, the assets, and the critical services are identified, the protect surface allows the organization to move controls closer to the assets at hand and essentially minimize the risk of compromise for critical assets via attack vectors like lateral privilege escalation and visibility to a public network.

In reference to the previous diagram, if a malicious actor successfully compromises the entry points via the application running on a browser, it is only a matter of time before cardholder data or PII is compromised via a vulnerability exploit of the asset. Identifying the assets hosting cardholder data and PII (i.e., the protect surface) enables the organization to move controls like role-based access control (RBAC), system hardening, and secure configurations closer to these assets. For example, the base image of a server build can be hardened before deployment, and the web server hosted on the server asset may be separated from the database host; that is, the database may be moved to another physical server.

Additionally, the organization may create two protect surfaces with micro-segmentation while aligning itself to NSTAC's protect surface definition.

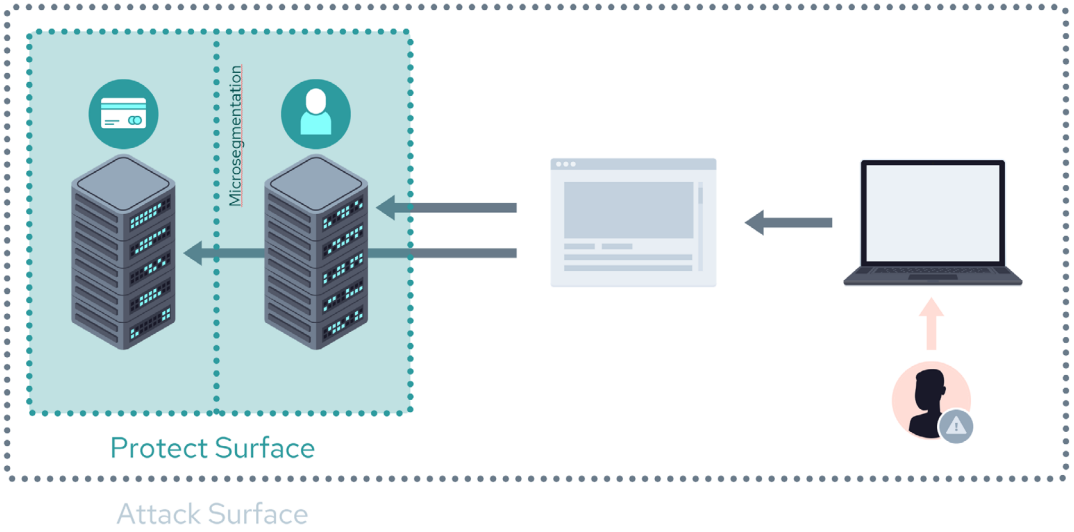

Figure 9: *Two Protect Surfaces Created with Micro-Segmentation*

5.4 Protect & Attack Surface Considerations

While the protect surface provides an inside-out view of the organization, the attack surface provides an outside-in view, or a view from the vantage point of the attacker trying to break in. The protect surface and attack surface complement each other in helping organizations identify what needs protection and how to optimally secure the most critical assets.

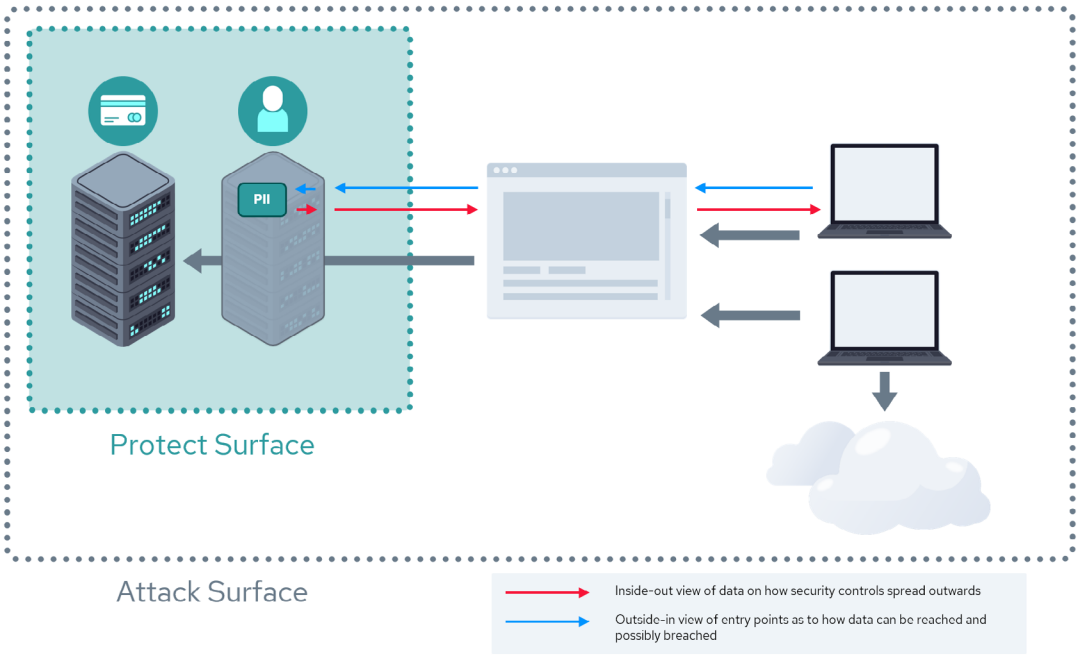

Figure 10: *Different Views of the Organization*

ZT calls for protecting access to any applications or servers shared privately with internal or external users. It is important to assess and plan for each of the assets. Each user should be granted the minimum required access to the assets following the principle of least privilege.

The following are crucial considerations for defining the protect surface:

- Data types involved (e.g., cardholder data, personally identifiable data, health data, trade secrets, by-products of business processes)
- Data and asset classification (e.g., public, internal-only, confidential, and restricted)
- Applications and/or services that handle the identified data
- Critical business functions (e.g., turbine health in a nuclear power plant)

Organizations should design ZTA protect surfaces that incorporate the following:

- The policies defined for ZT access
- The data defining the users (e.g., username, password, identification of the asset held by a user)
- The data defining the assets (e.g., servers, required services, and connections)
- The transport layer
- Business execution algorithms
- The logical and physical relationships between the asset at the core of the protect surface and other business and IT functions

6 Document Transaction Flows

As ZT planners acquire an understanding of the requirements for the system being built and define their protect surfaces, they should also identify what transactions occur with those protect surfaces and how they interrelate. Understanding and tracing of the data flows, application transactions, and business processes allows the planners to understand if the controls in place are sufficient to safeguard the protect surface. In other words, documenting the data and transaction flows ensures that access of entities to the protect surface happens within the defined risk appetite of the organization. Transactions in a system are often derived from the underlying business requirements as part of solution development. The transaction within a system exists because it addresses a business need and is often tied to maintaining business continuity. Business requirements can change over time as will the security considerations.

In the context of ZT, a transaction is any action within a system that needs verification. This could be any component in the architecture from person and non-person entities, an internal or external device to the system, or the process itself that owns the transaction in question. A number of these components are identified in the initial sections of this module.

If you are new to transaction flows and the tools available to create them, one way to look at this task is to envision the data's life cycle. What business transactions occur and what services are invoked to complete a transaction? This could be as simple as the data flow of an online retail purchase, or it could be more in-depth like a customer relationship management (CRM) transaction generating a sales prospect or lead record for a sales organization.

6.1 Example Transaction Flow: eCommerce

The following is a simple illustration of an eCommerce transaction, tracing the steps that occur when a purchase is made from the perspective of the credit card transaction.

In this example the identified protect surface is the payment process components.

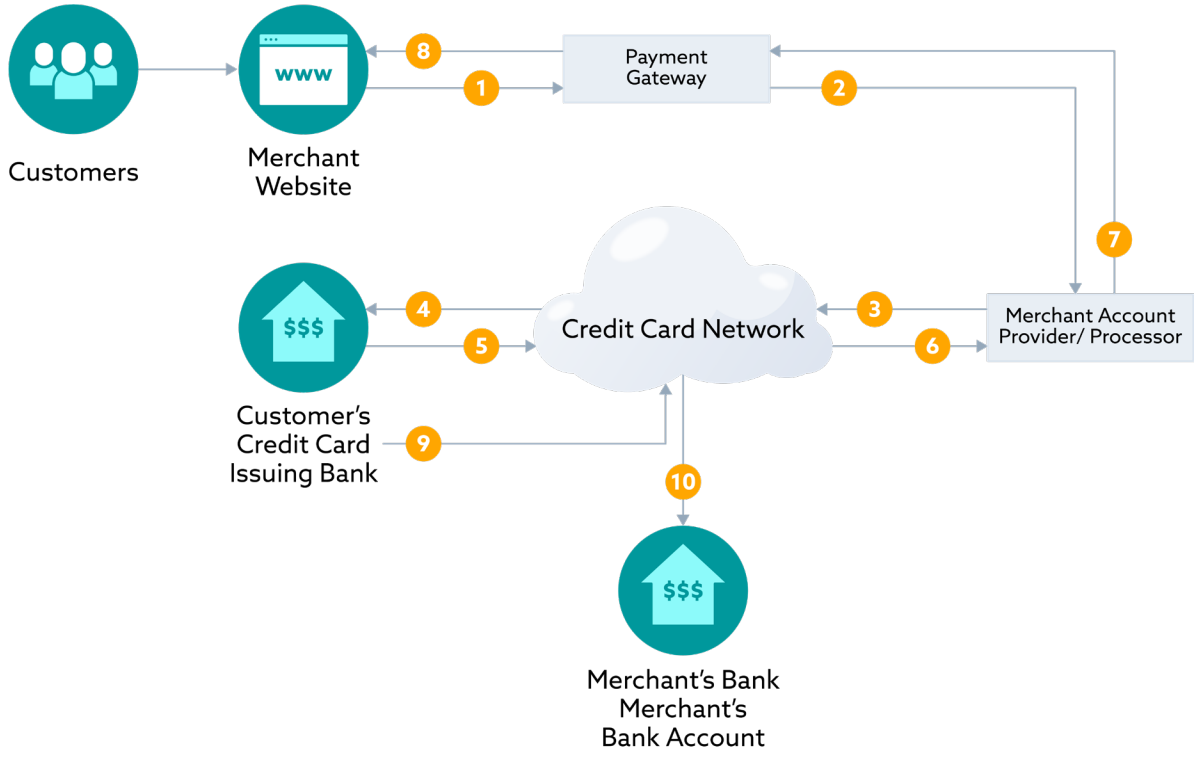

Figure 11: *Example Transaction Flow: eCommerce Payment Process*

1. The merchant's website sends a credit card transaction to the payment gateway via a secure connection.
2. The payment gateway receives the credit card transaction request and submits it using a secure connection to the merchant bank. For accepting payments, merchants need an account with a payment gateway.
3. The merchant bank's processor sends the transaction request to the credit network to process.
4. The credit network forwards the complete transaction to the institution which issued the card.
5. The credit card issuing bank accepts or refuses the transaction based on the card's valid card number, cardholder's name, expiration date, and card verification code and sends back the results to the credit network.
6. The credit network transmits the results to the processor for the merchant's bank account.
7. The merchant's bank processor sends the results back to the payment gateway.
8. The payment gateway saves the transaction results and transmits those results to the merchant's website, which in turn delivers them to the end customer. This is the end of the

approval process.

9. The customer's card issuing institution or bank checks the card number and name, and approves the transaction, sending the funds to the credit network.
10. The credit network sends the funds to the merchant's bank. The merchant's bank deposits the funds into the merchant's bank account and the payment is complete.

Several steps occur in an end-to-end transaction, all in a matter of seconds or milliseconds.

ZT planners should consider approaching the questions of **who, what, where, when, how** and **why** for the steps in this end-to-end transaction, and why each step needs to happen. This will help to ensure that the controls to guard the protect surface fall within the architecture being defined and adhere to organization policies and standards without introducing unmitigated risk. For instance, if the **who** element is a customer, the transaction may be handling PII. The protect surface must therefore be designed to keep the customer's PII data secure during the transaction. This analysis should occur at each step in the transaction process. Refer to the previous section discussing how the protect surface and attack surface are defined. When you measure the risk of transactions, the protect surface will need to be already defined. The attack surface could be modified as new transactions are added or existing ones are modified to keep the architecture in line with business requirements.

An example is provided below for illustration purposes. The transaction focus and protect surface in the last two right-hand columns are where you compare your risk and validate it against the protect surface discussed earlier in this module.

Who	What	Where	When	How	Why	Transaction Focus	Protect Surface Focus
Customer	Person or entity initiating a transaction	Anywhere	24x7 365 days a year	Application Interface	In need of the result the transaction will provide	Disclosing too much unnecessary data	Customer PII including PCI related Information
Merchant/ eCommerce Presence	Selling things	Online and possibly at a physical location	24x7 365 days a year	Through an online commerce portal	To make money	Web front end, customer data, inventory, business records	Customer data in motion and at rest. Entry point device(s), PCI compliance
Bank	Holder of all things monetary	In a giant vault and in the ether	24x7 365 days a year	Online transactions, transfers, in person	Money needs to be deposited or withdrawn	Customer data, PII information, account information, availability, fraud alerts	PII data, customer assets and corporate assets

Credit Card Issuer	Provide credit cards and credit limits to consumers	Everywhere	24x7 365 days a year	Online transactions, physical card, tied to an account	Ease of use, make money through interest	Similar to the banks	PII data, customer assets and/or corporate assets, PCI compliance
Payment Gateway	Provides a connector from the merchant	Between the merchant and credit card transaction process	24x7 365 days a year	API connections from merchant accounts, e.g., PayPal	Provide a mechanism for merchants to send credit card data to a credit card issuer	Inbound connections from ecommerce site, outbound connections to credit card industry	PII in motion and data at rest. PCI compliance

Table 2: *Transaction Flow: eCommerce Payment Process*

Following this eCommerce example, the question to ask is if the protect surface is meeting all requirements to ensure that customer data and financial information is not disclosed. Are you storing any credit card numbers as part of your interaction between the payment gateway and the credit card issuer? Is that transaction of data stored properly with the proper controls around it according to organizational and regulatory requirements (e.g., PCI-DSS)? Putting a matrix together such as this will help validate whether the protect surface is defined, monitored, and enforced properly. More details on data, monitoring, and transactions are discussed next. Additionally, the matrix that follows identifies transactions in your solution which may not be your responsibility, such as the banking institution itself, but that still need to be considered when planning your protect surface.

6.2 Transaction Discovery: Functional Analysis & Tooling

A critical, initial step is determining what data flows are involved. Establishing the proper visibility is crucial for discovering the transactions, their data, and data types (i.e., classification).

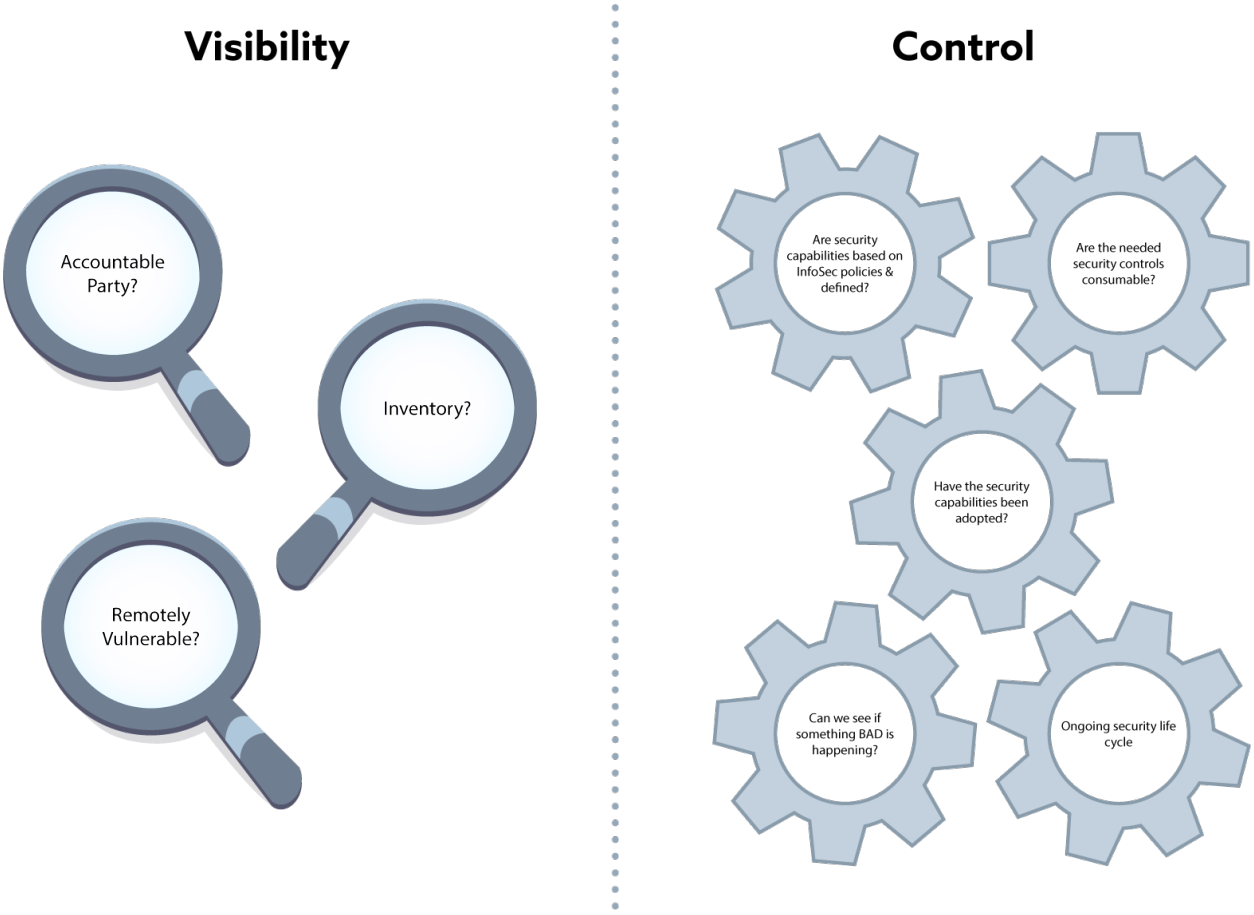

Figure 12: *Transaction Visibility & Control*

Whether the organization is operating in a private, public, or hybrid cloud, the analysis, tooling, and automation to identify what transactions are critical to the business and business processes are fundamentally the same. Below are some key functional areas to consider.

6.2.1 Collecting Data

To define a transaction, begin with an initial understanding of the data—what it is, where it is, and where it goes. Start with existing knowledge about the organization's business process and underlying architecture. It may help to leverage numerous sources such as packet captures, logs, or more sophisticated methods of traffic analysis between the service entities comprising the systems.

6.2.2 Discovery of Known & Unknown Transactions

From the data collection methodologies used, organizations will discover what transactions look like within the service or system being analyzed. They may discover unknown transactions they were previously unaware of. For instance, in the eCommerce example, there may be a transaction between the payment gateway and the eCommerce application to determine what tax to add to the full value of the transaction. Perhaps a tax rate changed based on doing business in a new market, or a shipping method changed or was added due to a new delivery requirement. While not specific to the method, this represents an ancillary process uncovered in the data collection phase.

6.2.2.1 Transaction Inventory

In completely new deployments, transaction inventories will be defined and developed during the architecture and design phase; nonetheless, organizations should create an inventory as part of the planning exercises. If organizations are pursuing an already existing deployment to migrate to a ZTA, they should collect and inventory the known transactions to maintain, highlight the ones that will change or become deprecated, and create entries for new transactions expected to be part of the solution as it is being developed.

6.2.2.2 Transaction Records

Transaction records are the historical paper trail of the behavior of transactions and the types of data involved. Recall that at every transaction layer, ZT controls will continuously analyze the processes and compare them to existing policy enforcement rules. Keeping and analyzing transaction records are part of the planning process and remnant samples of monitoring and analytics.

6.2.3 Monitoring & Analytics

Once you know what transactions are in your system, you will want to monitor them to collect statistics and profile the behavior. Again, as shown in the eCommerce example, monitoring the payment gateway and collecting analytics from dollar values being processed through your system will start to build a view of the behavior and trends of the process you ultimately want to protect. Monitoring and analytics are covered more in-depth later in this module. However, it is important to understand that ZT prescribes a continuous assessment of all transactions.

6.2.4 Identifying Anomalies & Edge Cases

During transaction discovery, ZT planners should identify what behaves unexpectedly or abnormally from the baseline. Edge cases may be greater in number than expected. Does this change the protect surface area as a result? Are new transactions required to mitigate any risks? Do any of them change?

For instance, in the eCommerce example, imagine the entire platform was designed at the baseline to allow for free shipping within the United States. The shipping provider charges the merchant for this behind the scenes. Suddenly, due to a marketing campaign in Hawaii and Alaska, there is great demand for overnight shipping to both locations which can't be met by the current provider integrated into your shipping workflow. Even though it is a small corner case sales and sales transactions, you need to bring in an additional third-party shipping partner to meet the shipping SLA. In doing so, do you need to supply them with any additional customer data? Do you have to set up a separate shipping workflow to integrate with them? Can they maintain the same level of privacy? Do you have to do any additional monitoring to ensure this new shipping partner doesn't create any new risk to you or the customer?

While this seems like a simple edge case on the surface, the seemingly benign act of offering a specific delivery mechanism to a specific subset of customers requires going through this new transaction again and checking all the boxes to ensure that your protect surface doesn't require additional controls.

7 Define Policies for Zero Trust

In a ZT approach, the visibility of and access to resources by any user or device is regulated and controlled by policies. Policy planning should be carried out with utmost care, with a granular understanding of who should get access to what resource, which actions are allowed, under which conditions, and for how long or at what time of day.

The policies need to be planned prior to implementation as doing so can help the stringent control for each of the user or user groups. The controls and policies allowed for each asset need to be documented for a better organized implementation and maintenance of the policies. Each of the newly introduced changes needs to be tracked down with a separate tracker that is peer-reviewed.

The user and the access are trusted after the authorization at the zero-trust gateway as the policies enable the authorization of the access.

Figure 13: *PDP/PEP & Zone Interactions*[22]

ZT systems enforce validation of the user and the device before permitting any access, hence the ZT policies allow organizations to plan and create access policies based on user or device attributes and contextual risks. By leveraging aspects such as directory group membership, IAM-assigned attributes and roles, location, and device posture, organizations can define and control access to cloud or data center resources in a way that is meaningful to business, security, and compliance teams.

7.1 The Policy

ISO 9001 defines policies as documents that include information about a set of standards. Within organizations, policies might appear in a hierarchical structure, and each policy defines the set of rules used to govern a different area of the business. To avoid any confusion, we want to clarify that in this section we are referring to rule-based security[23] policies that set the rules which control the access and the entitlements to a planned set of IT assets. The ZT policies are a set of rules which control the access and entitlements to a planned set of IT assets. The PDP will have two components/functions, an engine to maintain the set of rules, and another component to administer the rules at the user interface. The ZT policy can be applied to a combination of applications, application groups, user, or user groups based on the implementation planning. The policies can also vary the access, entitlements, and enforcements based on the dynamic contextual risks. The session management procedures take actions that enable the PDP to continually evaluate the session once it

[22] Figure adapted from: NIST. (2020). Zero Trust Architecture (SP 800-207).
[23] ISO. (1989). Rule-based security policy. In ISO 7498-2:1989(en)

has been established. The session will be revoked once the technical conditions are not met. The policy may define different levels of access and entitlements based on the attributes of the identity. For example, users coming from different locations or times of day may end up getting different levels of access.

ZT implementations typically use device, network, environment, user, and entity behavior analytics (UEBA), and IAM attributes for users (e.g., directory group memberships, directory attributes, roles) as elements for policies. For example, a policy may state that all users in the directory group **HR**, using an endpoint device with a level of security hygiene **medium**, may access server HR-Portal on port 443 from a specific country from 10:00 AM PST to 8:00 PM PST and perform actions A, B, and C, under standard **low** risk conditions. This example illustrates how a system can add value to, and extend the power of, an existing IAM deployment.

7.2 The Policy Workflow

ZTA policy planning should have the gateway enforcing access policies on a per-user/group basis, achieving the principle of least privilege by denying access by default. Additionally, the PEP/gateways should be situated at the entry point of each private cloud network controlling all inbound traffic based on the policies defined at the policy engine.

The planning phase should involve the planning for the required policies. The policy administrator (i.e., the previously mentioned logical component of PDP) allows for the planning and definition of policies at the policy engine. The PEP allows the ZTA to apply the policies based on which access can be managed for various assets such as, for instance, web application or secure shell (SSH) access.

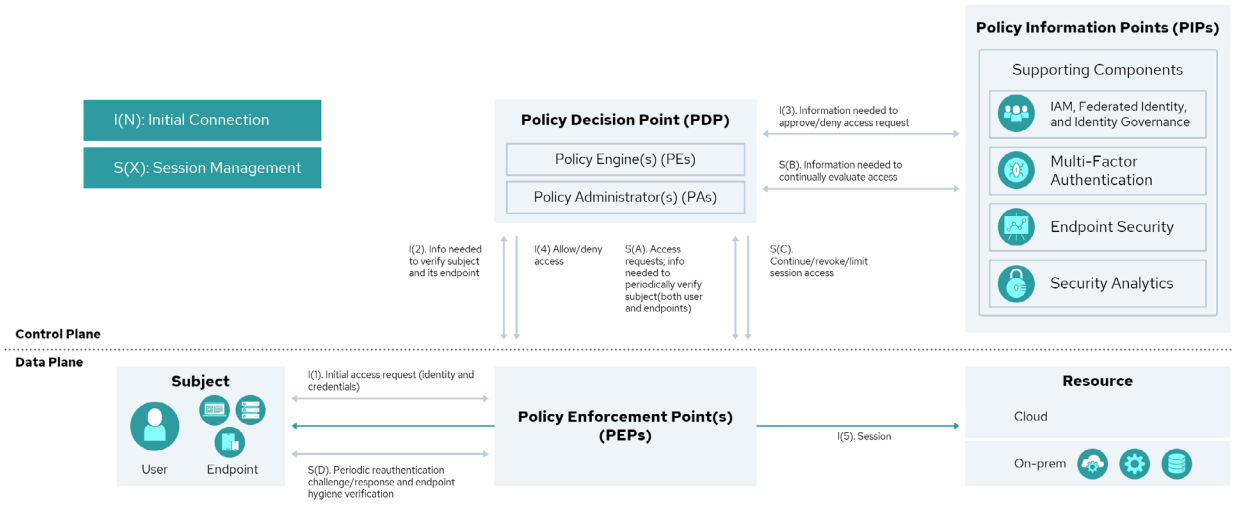

Figure 14: *Zero Trust Entities & Policy Workflow*[24]

The policies kept at the policy engine have to be planned with utmost care and acceptance from the respective decision makers. The policy administrator helps to add/modify and maintain the policies in a continual improvement model.

[24] Figure adapted from: NIST. (2022). Implementing a Zero Trust Architecture (SP 1800-35B). Second preliminary draft.

The PEP will authorize access based on the policies defined at the policy engine. The policy data will be percolated down to the PEP by the PDP. In turn, the subject is either granted or denied access to the protected resource in question.

Throughout the lifetime of the session, the PEP may periodically challenge the subject to re-authenticate itself, depending on the level of risk associated with the transaction. After doing so, the PEP will provide the PDP with the identity and credentials that the subject provided. Similarly, throughout the lifetime of the session, the PEP will request hygiene information from the subject's endpoint. After obtaining this hygiene information, the PEP will provide it to the PDP. The frequency with which the subject should be issued authentication challenges is determined by enterprise policy, as is the frequency with which the hygiene of its endpoint should be validated. In both cases the policy is a reflection of the risk-based decision.

The connection between the PEP and the subject may be terminated or reconfigured based on changes to the endpoint, resource, or operating environment that indicate the subject no longer conforms to enterprise policy. The policy may enforce various levels of access and entitlements based on the risk and current context of the user, device, endpoint, network.

It is important to highlight that the policy workflow is a logical representation that doesn't correspond to the actual physical architecture. The components defined are meant to represent logical functions, not physical devices.

7.3 Policy Considerations & Planning

As mentioned in the previous sections, ZT policies are the logic behind enforcement of ZT principles like least privilege and need to know. These policies are the gatekeepers that greet each incoming access request with a set of predefined questions such as:

- The identity of the requesting identity
- The target assets a particular entity/user is entitled to access
- The timeframe the entity/users is allowed access to the asset
- The geographical or logical origin of the request and requestor
- The device attributes
- The entitlements of the entity/user

Access should be planned at the group level as much as possible versus at the individual user and application level. The plan should define which group of users can access which group of applications (e.g., HR for HR Applications) while policies are planned for various levels of access and entitlements.

The following is a list of factors to consider in the definition and eventual enforcement of the ZT policies:

- **User attributes:** Is the requesting user authenticated? What is the level of certainty about the requesting user's assertion of identity? Is the user internal or external? Where, geographically, is the user located? Where do we expect the user to be located at the time of the request? How often should the user re-authenticate to the asset, and under which

circumstances? Which network/IP is consumed by the user?

- **Target resource attributes:** What is the classification of the data? Which services, devices, data, and other resources are available and allowed for a particular request? What level of access should a particular requestor be granted at the time of the request?
- **Time:** During which time windows do we expect requests from a particular requestor to a particular resource? When should access end?
- **Device attributes:** Which devices are registered with the enterprise, and do we allow unregistered devices to originate requests for access? Which attributes do we expect from an originating device (e.g., MAC address, profiles created by an agent)? Do we require that the originating device be registered and/or authenticated with the enterprise? Which patch levels and/or software suites do we require from the originating device? What is the overall security hygiene level expected from the device?
- **Entitlements:** What level of access should be granted to a particular user over a particular resource? How do the entitlements change based on a person's/user's attributes? How entitlements change depending on the level of hygiene of the device? How do entitlements change depending on risk factors?

ZT is ultimately about dynamic risk management, so the policies need to reflect the changes in the risk levels and allow access and actions depending on that risk context. The risk in a specific context is a reflection of all the previously mentioned variables (e.g., type of user/entity, environmental conditions, device posture, user behavior, etc.) Therefore, the possibility to access resources and perform certain actions changes depending on risk levels.

The policy should take into consideration the behavior of the user/entities. In case of anomalies, for instance, there should be a rule to ensure that the access is revoked or the entitlements are limited based on the level of deviation from the baseline measured behavior of the user/entity dynamically during the session.

It is important to note that establishing and enforcing policies based on behavior and risk assumes that the organization can collect and analyze telemetry data from the PIP.

In the planning phase, it is important to realistically define what, within the context of the protect and attack surface, can be subject to continuous monitoring and what data source the organization is able to collect and analyze.

7.4 Continual Improvement

The process of continual improvement should be well planned and documented with a track of reviews and approvals. The access rules and entitlements should always be subjected to recurring reviews and improvements based on need, risk, and context. The reviews can be planned to repeat after a fixed duration and scheduled accordingly. The changes introduced over the collection of attributes such as user, endpoints, applications, or the attack surface of the organization can often change the access and entitlements needs. Hence the planning should involve the possible processes and definition of controls in place.

New access points may be created according to needs that may arise over time; these changes should be reviewed and planned for ahead of time during the course of ongoing discussions

7.5 Automation & Orchestration

The effective implementation of ZT needs to ensure that the automation and orchestration are planned at each stage of the operation such as authentication, MFA, access provisioning, policy enforcement, and dynamic evaluation of the posture.

The strategy for automation and orchestration should be planned well in advance. The automated enforcement of access policies reduces the need to manually update and test firewall rules in response to user or server changes. In larger organizations, this is typically part of the daily workload for IT, and therefore presents an opportunity to reduce both workload and labor costs (especially in an outsourced model). It also accelerates business and technical user productivity, which while worthwhile in its own right, can also reduce hard costs (particularly for hourly or outsourced workers). The need for automation and orchestration varies for each organization and kind of access requirements. Hence, we need planning and preparation for the same.

8 Developing a Target Architecture

Identifying and developing a target architecture is the last step of the ZT planning phase. This step is about defining how your service and network architecture looks. The ZT target architecture will likely be an evolution of the existing architecture; alternatively, the change could be revolutionary.

The target architecture will be business-driven, as expected, by the nature of the business, technological environment, and consequently, the challenges that the organization is trying to address through the ZT approach. Is the organization addressing the challenges of multi or hybrid cloud? Is it about the security of a highly distributed supply chain and/or production chain? Is it about solving the issue of a highly distributed workforce with a need for remote access? Is the challenge related to securing an ICS, or more general operational technologies?

The definition of the target architecture should consider a number of technical variables which are described in the ZT five pillars (i.e., Identity, Devices, Networks, Applications and Workloads, and Data) and the cross-cutting functions (i.e., Visibility and Analytics, Automation and Orchestration, and Governance). This conceptual framework might be used for determining their **current** state, a desired **future** state, and finally a path towards developing a target architecture (**roadmap**). This topic of assessing the current state and determining the roadmap for the target architecture has been analyzed in an earlier unit.

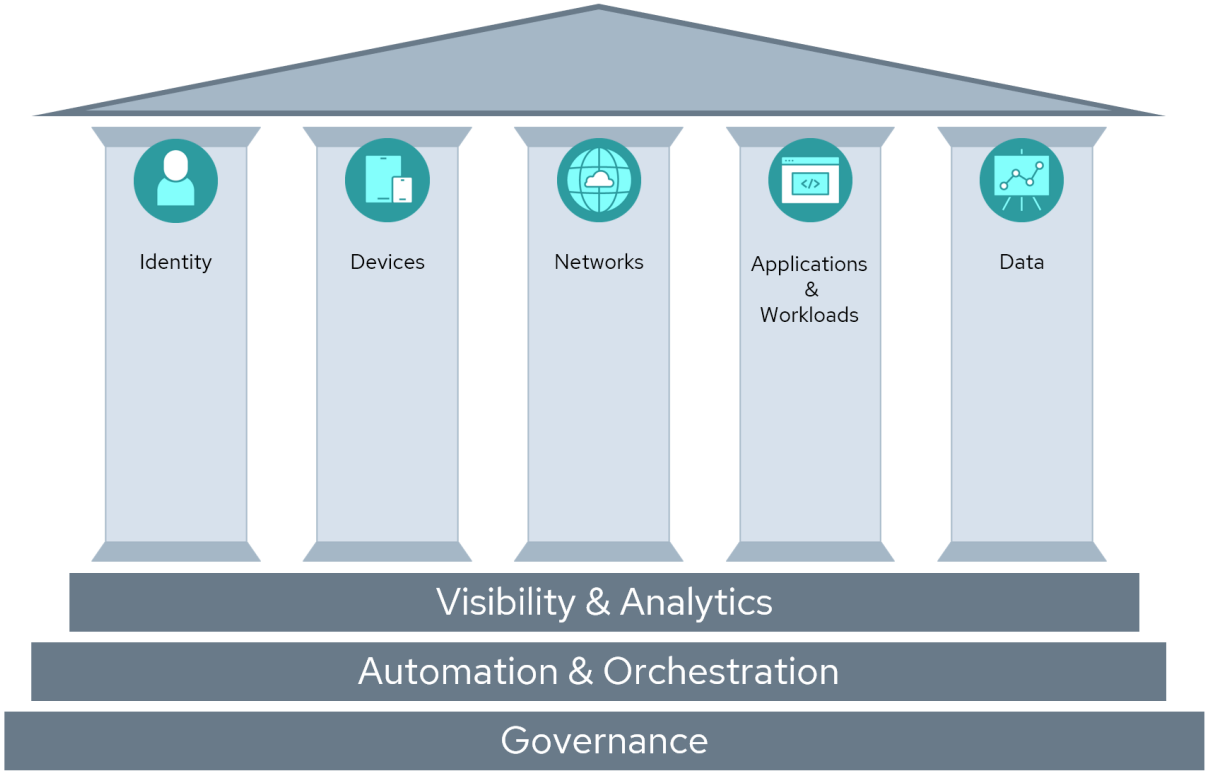

Figure 15: *Zero Trust Pillars & Foundations*[25]

In this unit, we discuss important considerations when planning for a target architecture in the context of these main pillars and functions.

8.1 Identity Considerations

Proper identity validation of the entity requesting access to a resource is paramount in a ZT environment. The principle of least privilege, which is a key component of ZT, can only be assured with validated entities (e.g., human user, computer services, etc.). This validation should be performed when the entity is requesting access to a resource and also periodically throughout this access, with the frequency and technology determined by the sensitivity of the information being accessed (data classification). As a rule, MFA should be leveraged to validate the identity of the entity. In some cases, step-up/adaptive/conditional authentication (additional rigorous authentication steps) should be required for access to more sensitive information. As ZT maturity improves, real-time machine learning analysis to highlight any user or device behavior that is unusual should be performed for further analysis and follow-up to ensure the security of the information protected by ZT.

Identity stores contain the entities and associated information. These stores are queried during the authentication process by the ZT process. Mature ZT implementations include a global identity store that can be leveraged for both on-premise and across cloud environments.

[25] Figure adapted from: CISA (2023). Zero Trust Maturity Model (Version 2.0).

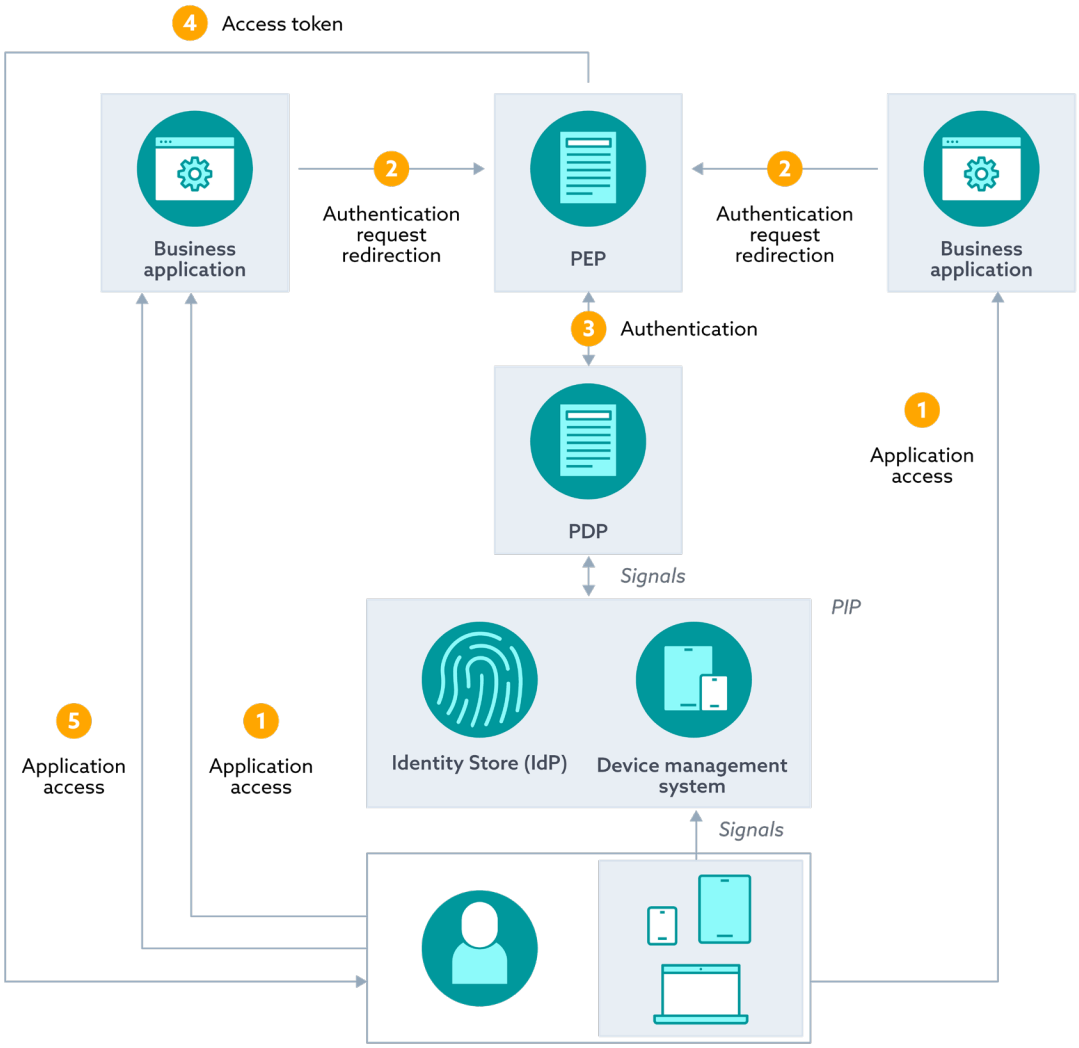

Figure 16: *Validating SaaS Application Access*[26]

A process should also exist in order to ensure that the user identity is mapped to a real user when possible (identity proofing). The accuracy of claims should also be controlled during the lifecycle of the user. When possible, an integration with a public key infrastructure (PKI) should be considered because it can be integrated with the identity system.

8.2 Device & Endpoint Considerations

In a ZT environment, devices and endpoints (e.g., laptops, mobile phones, IoT devices, servers, etc.) also require authentication validation before they can access the resources protected by the ZTA. In addition, the device's security posture (e.g., device hardware and software patch level, the status of installed security software, etc.) should also be validated against an organization's security policies before the device is allowed access to the resources it requests. In more mature implementations, these validation steps are performed continuously, and the device's behavior is also analyzed to identify any unusual activity.

[26] Figure inspired by: NIST. (2020). Zero Trust Architecture (SP 800-207).

Performing a complete and accurate inventory of all devices and endpoints is a highly sought-after goal for most organizations. While some achieve this goal, many large organizations fail primarily due to the vast number and relatively short life cycle of devices deployed in their environments. A mature ZTA deployment will ensure that only properly registered and secured devices can access the organization's resources. This ZTA requirement will help even the largest organizations achieve their device and endpoint inventory data quality goals. Unmanaged devices (e.g., contractor devices, etc.) should also be incorporated in the ZTA design, and solutions leveraging a gateway or VDI should be explored.

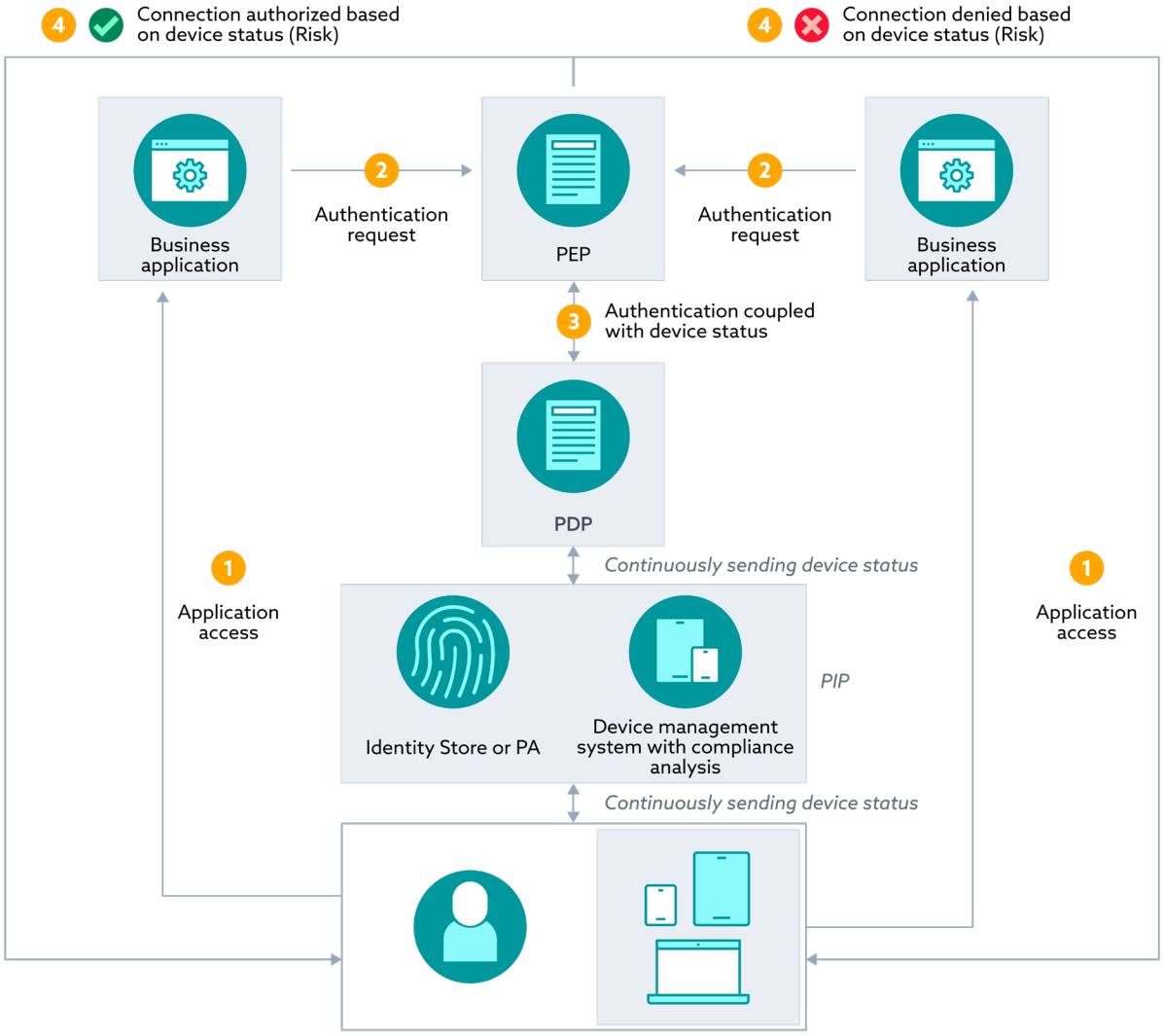

Figure 17: *Access Decisions with Endpoint Risk Analysis*[27]

8.3 Network & Environment Considerations

A typical ZTA implementation will use micro-segmentation coupled with encryption in order to improve the security posture of the network. This means that the data plane used for application/service communication and the control plane used for network communication control should be separated.

[27] Figure inspired by: NIST. (2020). Zero Trust Architecture (SP 800-207).

The decision to allow access to the application is made over the control plane, and the actual application interaction and data exchange with the requesting device occurs via the data plane. To achieve micro-segmentation technology like host-based firewalls, software agents, intelligent routers, or next-generation firewalls can be used. Segmenting traffic based on the data flow (internal data flows vs. external data flows) should also be considered.

8.4 Workload & Application Considerations

All applications should use a centralized authentication, authorization, monitoring, and attributes system. This configuration provides better visibility and enables real-time risk analytics in ZTA. Access authorization should be continuously evaluated and consider real-time risk analytics, which means that the application should adapt to environmental changes. For internally developed applications, security testing should be implemented in all stages of the CI/CD cycle.

Whenever possible, applications should also be integrated into the monitoring system in order to send internal insights (e.g., from which country a user is accessing the application, the type of device or browser if possible) and be accessible without VPN.

8.5 Data Considerations

An organization's data classification policy should codify the required data security controls and processes used for each of the data classes defined by the organization. These security controls can include secure encryption (at rest and in transit) and network segmentation for highly sensitive data to simply read-only access for publicly available data. The processes outlined by the policy should include how entities gain access to the data (leveraging least privilege principles) and what steps are required to properly dispose of the data when its end-of-life has been reached.

8.6 Visibility & Analytics Capability Considerations

As mentioned in the introduction of this unit, visibility and analytics is one of the important functions needed in a ZT architecture and helps support the pillars noted above. When optimally deployed, this function increases security by the following three means:

- Leveraging UEBA to continually evaluate the user's behavior against a baseline of previous activity to identify any unusual action
- Running regular device posture assessments to ensure the device being used to access the application or data is properly configured and secured
- Monitoring application health and security by leveraging systems and sensors external to the application

The feedback from these visibility and analytics capabilities should be directed towards the PEP so it can make real-time decisions about granting and revoking access to the requested application and data.

8.7 Automation & Orchestration Capability Considerations

Automation and orchestration should be used to support every pillar. When optimally deployed, this function increases security by:

- Taking advantage of automation by using infrastructure-as-code to deploy network and environment configurations and consolidating with the CI/CD pipeline
- Orchestrating and automating the identity lifecycle, including dynamic user identity and group membership, JIT access to applications and data, and revoking access when required

8.8 Governance Capability Considerations

In a ZTA deployment, governance is the most important function because it ensures that business, risk, and IT perspectives are aligned. Governance helps to define ZTA policies; for example, to access and process data, a device must be encrypted. From a non-technical perspective, governance should also manage and reduce complexity. In order to do that, the focus should be on the protect surface, with governance policies enforced by the PEP.

8.9 Examples of Zero Trust Architecture

From a practical perspective, several reliable sources can serve as a model for defining the target architecture to meet the organization's specific business objectives. A good reference is the NIST SP 800-207.

There are two important items to note. First, every situation is unique with its own business objectives and constraints. These sources are templates designed to inspire and guide you in developing an architecture that fits your needs and meets your objectives. Second, more sophisticated enterprises may have a suite of target architectures. For example, in the case of equipment and devices on a manufacturing floor, an organization may design a different architecture for them than the one it uses for core IT functions.

In essence, ZTA approach variations typically fall into one of the following three categories:

1. **ZTA using enhanced identity governance:** As the name implies, at its core, ZTA is driven by identity and rooted in the proper governance of the access privileges and entitlements for specific assets.
2. **ZTA using micro-segmentation:** This approach is based on the logical segmentation of the network. The organization uses devices such as next generation firewalls (NGFWs) or gateways to act as a PEP and enforce the logical boundaries of the protect surface. This approach assumes that a fully functioning enhanced identity governance program is enforced. It also assumes the organization updates access rules to accommodate changes in business objectives, threats, context, user behavior, and other factors. Micro-segmentation has the added advantage of limiting the impact radius in the event of an incident.
3. **ZTA using network infrastructure and software-defined perimeters (SDPs):** This approach focuses on the network architecture to achieve ZTA. The SDP approach uses the PDP as a

network controller (SDP controller) to restrict visibility of the asset and which entities can interact with the resources part of the protect surface. This approach was developed by CSA. The specific details can be found in the training modules entitled *Introduction to SDP*[28], *Key Features & Technologies of SDP*[29], and *Architectures & Components of SDP*[30].

As NIST highlights, each approach varies based on the specific situation. NIST specifically addresses components and the source of truth for the organization's policy rules.

A full ZT solution will eventually include elements of all three approaches. The selection of the starting point depends on the considerations mentioned previously, including the maturity of the organization, business objectives, technology strategy, use cases, etc. We described/discussed/outlined how these conceptual architectures are geared/crafted to inspire the design of the architecture for your specific situation. NIST lists the following variations:

- Device agent / gateway-based deployment
- Enclave-based deployment
- Resource portal-based deployment
- Device application sandboxing.

Additional discussion can be found in *Architectures and Components of SDP*. These variations are described in more detail and are also compared with the SDP architecture deployment variations in that module.

Conclusion

This module covered the planning activities and considerations for an organization moving to ZT. Learners were instructed on how to identify ZT stakeholders, prioritize and scope a ZT implementation, carry out a gap analysis, map out the protect and attack surfaces, and define the ZT technology policies. Lastly, critical considerations for planning for a target architecture were described in the context of ZT's main pillars and functions.

Glossary

Please refer to our Cloud Security Glossary, a comprehensive glossary that combines all the glossaries created by CSA Working Groups and research contributors into one place.

[28] Cloud Security Alliance. (2022.) Introduction to Software-Defined Perimeter.
[29] Cloud Security Alliance. (2022.) Key Features & Technologies of Software-Defined Perimeter.
[30] Cloud Security Alliance. (2022.) Architectures & Components of Software-Defined Perimeter.