Defining the Zero Trust Protect Surface

cloud security alliance®

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

Acknowledgments

The CSA Zero Trust Research Working Group

The scope of Zero Trust research and guidance necessarily includes cloud and on-premises environments along with mobile endpoints and applies to the Internet of Things (IoT) and operational technology (OT). The goals of the CSA Zero Trust (ZT) Working Group are to:

> - Collaboratively develop and raise awareness of Zero Trust best practices as a modern, necessary, and cloud-appropriate approach to information security (InfoSec).
> - Provide thought leadership and educate the industry about the strengths and weaknesses of different ZT approaches so organizations can make informed decisions based on their specific needs and priorities.
> - Take a deliberately product- and vendor-neutral approach to architectures and implementation approaches for mature Zero Trust implementations.
> - Take technically sound positions on Zero Trust and make defensible recommendations while remaining product- and vendor-neutral.
> - The working group is composed of 9 different work streams that align with the Zero Trust maturity model and architectural pillars.
> - The lead workstream(s) for this document is **ZT7 - Pillar: Data**, led by Shruti Kulkarni, Krishna Narayanaswamy and Alex Kaluza.

Lead Authors

Shruti Kulkarni
Michael Roza

Contributors

Krishna Narayanaswamy
Shamik Kacker
Erik Johnson

CSA Staff

Erik Johnson
Alex Kaluza
Claire Lehnert
Stephen Lumpe

Reviewers

John Kindervag
Jason Garbis
Chandra Rajagopalan
Bernard Coetzee
Hani Raouda
Heinrich Smit
Jennifer Minella
Steve Guilford
Paul Simmonds
Ivan Djordjevic
Anand Kumar Jha
Gopi Ramamoorthy

Table of Contents

Acknowledgments....3
Abstract....5
Target Audience....5
Introduction to Zero Trust....5
  Document Scope....6
  Business Assets Overview....6
Zero Trust Implementation Process....8
  Overview of the Protect Surface....8
  Prioritizing Iterative Execution of the 5-Step Process....13
  Caution Regarding DAAS Elements Whose Purpose Is Uncertain....14
DAAS Elements Comprising a Protect Surface....14
  Data....15
  Applications and Workloads....16
  Assets: Systems and Devices....17
  Services....18
  NSTAC, CISA Maturity Model and Protect Surfaces....19
Risks and Impacts of Protect Surface Compromises....21
  Applying Data Classifications....24
Attack Surface Versus Protect Surface....25
Looking Ahead, After Protect Surfaces are Defined....26
Conclusion....28
Useful References....29

Abstract

The objective of this document is to provide guidance for iteratively executing the first step in the five step Zero Trust implementation process described in the NSTAC Report to the President on Zero Trust and Trusted Identity Management (pg. 7), originally formulated and socialized by John Kindervag. Separate CSA research documents are being developed to elaborate detailed guidance for each of the five steps.

This crucial first step, Defining the Protect Surface, entails identifying the organization's Data, Applications, Assets, and Services (DAAS) elements, accompanied by business risk and current security maturity assessments to help with implementation prioritization. The paper focuses on the methodology behind this process, including grouping DAAS elements into a Protect Surface comprising a business information system. Key considerations and concepts are explored, including the interplay between attack and Protect Surfaces and how the CISA Zero Trust Maturity Model V2 can be leveraged for implementation prioritization. This guidance empowers organizations to adopt a repeatable process for navigating the complexities of Zero Trust implementation.

Target Audience

- **Primary Audience**: Zero Trust Architects and Implementation Teams, Chief Information Security Officers, Information Security Managers, IT Security Analysts
- **Secondary Audience**: CxOs (CEOs, CISOs, CFOs, CTOs, CIOs), Privacy and Compliance Officers, IT Auditors and Assessors, Software Developers, Network Security Engineers

Introduction to Zero Trust

The National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Zero Trust and Trusted Identity Management defines Zero Trust (ZT) as *"a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, an entity should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified."*

Traditional, centralized trust-based "castle and moat" physical network perimeter security architectures are ineffective in the current era of decentralized cloud computing and the remote workforce, where few organizational assets and users actually still reside inside the "castle."

Sophisticated threat actors are increasingly adept at exploiting any exposed technical or human vulnerability in modern, highly distributed enterprise networks that often leverage Internet connectivity heavily. Successful cyberattacks generally exploit trust in some manner. This makes "trust" a dangerous vulnerability that should be mitigated and managed. With Zero Trust, all network connections and packets are untrusted and treated identically with every other packet flowing through the system. The trust level is defined as zero, hence the term Zero Trust.

Zero Trust is a holistic enterprise security strategy that encompasses cloud/multi-cloud (all service models), on-premise/hybrid systems, internal and external partner/stakeholder user (organization-managed and BYOD) endpoints, and is inclusive of operational technology (OT), Industrial Control Systems (ICS) and IoT. Consequently, Zero Trust has been compared to a mountain that must be climbed one step at a time, i.e. implemented incrementally and preferably in a risk-based manner. These principles are a common theme in CSA ZT guidance.

Enterprise adoption of Zero Trust is broad and growing. Venture Beat reports that 90% of organizations moving to the cloud are adopting a Zero Trust Strategy[1] while Gartner predicts that 10% of large enterprises will have a mature and measurable Zero Trust program in place by 2026.[2]

Document Scope

The objective of this document is to provide guidance for iteratively executing the first step in the five-step Zero Trust implementation process described in the NSTAC Report to the President on Zero Trust and Trusted Identity Management (pg. 7), originally formulated and socialized by John Kindervag. This document guides navigating the intricacies of incremental Zero Trust implementation principles. It begins with Defining the Protect Surface, a foundational step for a resilient cybersecurity implementation based on a robust understanding of the organizations' business assets. It describes the methodology of identifying, categorizing, and assessing the risk and security maturity associated with an organization's data, applications, assets, and services (DAAS elements), establishing clear criteria for risk-based prioritization. The guide illuminates key considerations, such as the distinction between a Protect Surface and an Attack Surface. The document concludes with significant insights into the second step, "Mapping Transactions Flows," which focuses on understanding how the system works.

Business Assets Overview

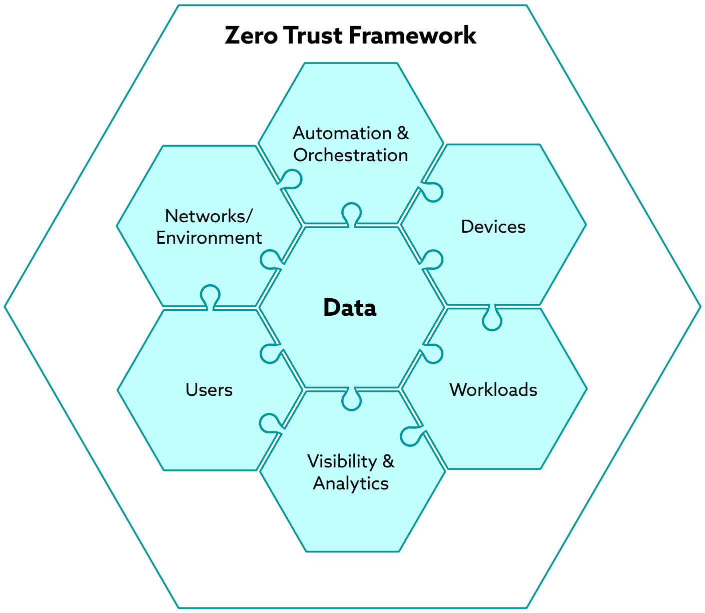
Awareness and adoption of Zero Trust is happening at the same time that enterprises are facing complex data security challenges. Organizations go through IT transformation initiatives where data leaves the confines of private data centers and moves to cloud-hosted environments that are not completely under their direct control. These changes make it essential for organizations to identify and protect their critical business assets and data.

It is also important to note that business assets and data and their sensitivity are relative to organizational context. For example, the financial services sector may define sensitive assets to include cardholder data, bank account data, and financial transactions. An identity provider may define data in terms of identities held in their store. A software product company may define code

[1] https://venturebeat.com/security/why-90-of-enterprises-migrating-to-the-cloud-are-adopting-zero-trust/
[2] https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026

repositories (code base) as their critical assets/data. A chemical industry may define its critical assets as the plant process and the need to protect it from misuse or sabotage.

The illustration below is from the US Department of Defense Zero Trust Reference Architecture. It depicts data as central to the Zero Trust framework since it is integral to all the pillars. However, the Zero Trust framework includes devices, workloads, and services as intersections with data and the elements (for example, the intersection between devices and workloads).



ZT Pillars were identified by the ZT Strategy. These associate to an interlinked group of strategic resources.

Protecting data is at the center of ZT goals and is a part of all other resources.

All the resources are bound into the Zero Trust Framework.

Figure 1. US Department of Defense Zero Trust Pillars, Ref: US Department of Defense (DoD) Zero Trust Reference Architecture

Zero Trust Implementation Process

This document provides guidance for completing the first step defined in the 5-step Zero Trust implementation process, as described in the NSTAC Report to the (US) President on Zero Trust and Trusted Identity Management. This foundational reference document, which the CSA Zero Trust research leverages and to which it aligns, depicts the five-step method as an iteratively executed repeatable process in section 2.1.1.

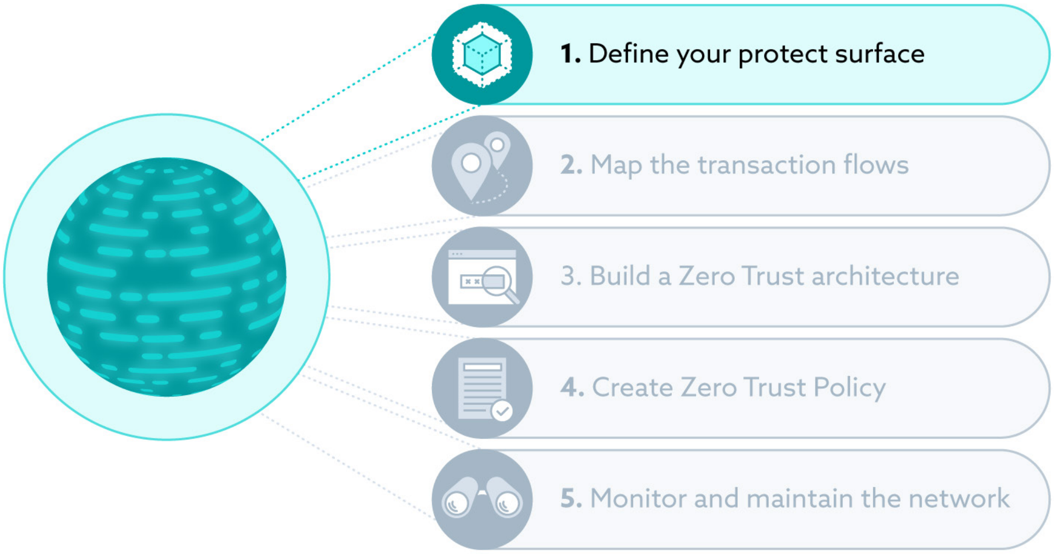

1. Define your protect surface
2. Map the transaction flows
3. Build a Zero Trust architecture
4. Create Zero Trust Policy
5. Monitor and maintain the network

Figure 2. Five-Step Process for Zero Trust Implementation
Ref: NSTAC Report to the (US) President on Zero Trust and Trusted Identity Management

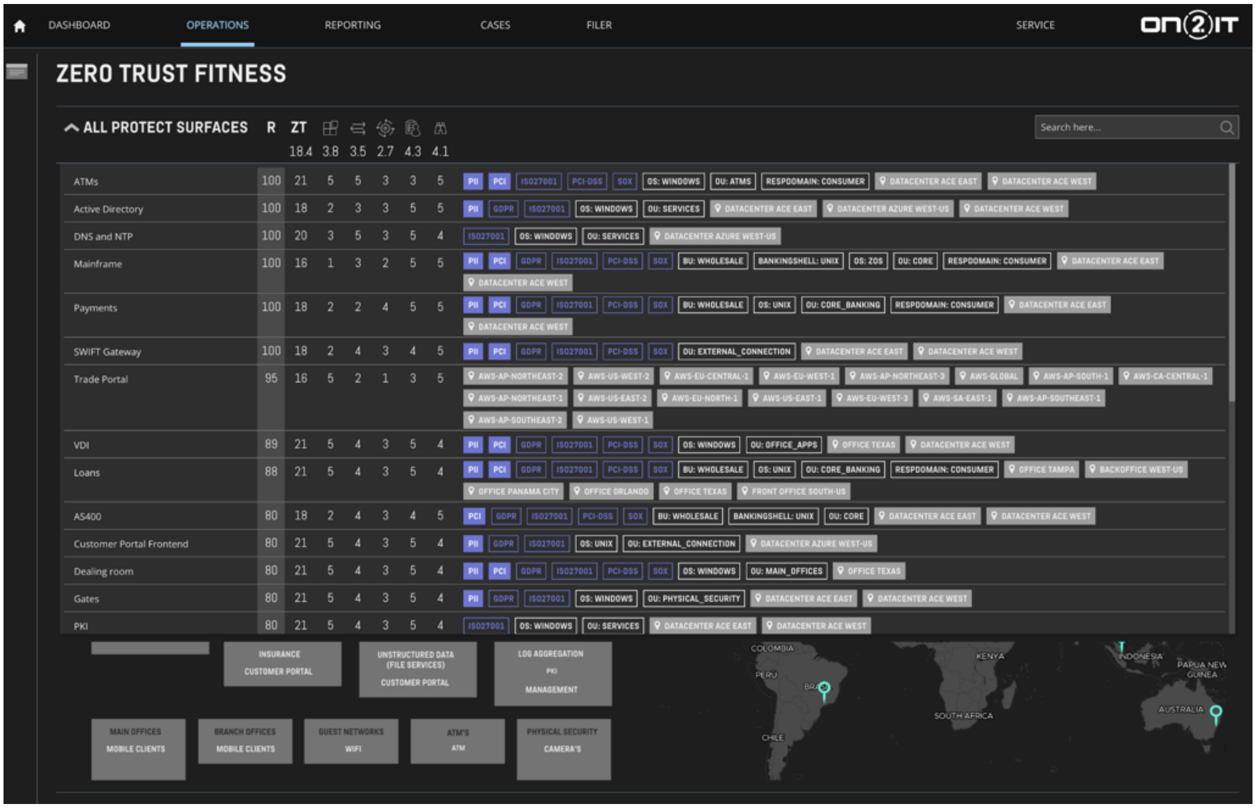
Overview of the Protect Surface

A Protect Surface is the area or portion of an organization's technology environment that the Zero Trust policy implementation protects. Protect Surfaces consist of Data, Applications, Assets, and Services (DAAS), that is, one or more DAAS elements as described in NSTAC report on page 6 in "Table 3: Key Zero Trust Foundational Concepts and Definitions."

Data, Applications, Assets, and Services (DAAS)	The sensitive resources that go into individual protect surfaces. • **Data** - The sensitive data that poses the greatest risk if exfiltrated or misused. • Examples include payment card information, protected health information, personally identifiable information, and intellectual property. • In the government context, this also includes Classified Information, National Security Information, and Controlled Unclassified Information. • **Applications** - The applications that use sensitive data or control critical assets. • **Assets** - The assets, including an organization's information technology (IT), operational technology (OT), or Internet of Things devices. • **Services** - The services an organization most depends on. • Examples include Domain Name System, Dynamic Host Configuration Protocol, Directory Services, Network Time Protocol, and customized Application Programming Interfaces.

The NSTAC report on page 6 in "Table 3: Key Zero Trust Foundational Concepts and Definitions" states that "each Protect Surface contains a single Data, Applications, Assets, and Services (DAAS) element." This definition should not be construed overly literally or prescriptively. Depending on the organization's business environment and requirements, a Protect Surface may contain a set of related DAAS elements comprising a *Business Information System,* such as an application and its data, that should be protected in unison. We believe that the *Business Information System* concept should be the concept around which to organize a set of DAAS elements, transaction flows, enforcement points, and policies. It's essential to choose an appropriate level of granularity for each Protect Surface, so that it is understandable and is one for which it's possible to easily create a related set of transaction flows, architecture elements (enforcement points), and access policies.

Let us illustrate this with examples of business information systems, such as Protect Surfaces for a fictitious financial services organization. Figure 3 shows some examples Protect Surfaces along with related business risk and current ZT security maturity metrics that can be used to help prioritize the next steps in the organization's Zero Trust journey.



ZERO TRUST FITNESS

ALL PROTECT SURFACES	R	ZT 18.4	3.8	3.5	2.7	4.3	4.1	
ATMs	100	21	5	5	3	3	5	PII PCI ISO27001 PCI-DSS SOX OS: WINDOWS OU: ATMS RESPDOMAIN: CONSUMER DATACENTER ACE EAST DATACENTER ACE WEST
Active Directory	100	18	2	3	3	5	5	PII GDPR ISO27001 OS: WINDOWS OU: SERVICES DATACENTER ACE EAST DATACENTER AZURE WEST-US DATACENTER ACE WEST
DNS and NTP	100	20	3	5	3	5	4	ISO27001 OS: WINDOWS OU: SERVICES DATACENTER AZURE WEST-US
Mainframe	100	16	1	3	2	5	5	PII PCI GDPR ISO27001 PCI-DSS SOX BU: WHOLESALE BANKINGSHELL: UNIX OS: ZOS OU: CORE RESPDOMAIN: CONSUMER DATACENTER ACE EAST DATACENTER ACE WEST
Payments	100	18	2	2	4	5	5	PII PCI GDPR ISO27001 PCI-DSS SOX BU: WHOLESALE OS: UNIX OU: CORE_BANKING RESPDOMAIN: CONSUMER DATACENTER ACE EAST DATACENTER ACE WEST
SWIFT Gateway	100	18	2	4	3	4	5	PII PCI GDPR ISO27001 PCI-DSS SOX OU: EXTERNAL_CONNECTION DATACENTER ACE EAST DATACENTER ACE WEST
Trade Portal	95	16	5	2	1	3	5	AWS-AP-NORTHEAST-2 AWS-US-WEST-2 AWS-EU-CENTRAL-1 AWS-EU-WEST-1 AWS-AP-NORTHEAST-3 AWS-GLOBAL AWS-AP-SOUTH-1 AWS-CA-CENTRAL-1 AWS-AP-NORTHEAST-1 AWS-US-EAST-2 AWS-EU-NORTH-1 AWS-US-EAST-1 AWS-EU-WEST-3 AWS-SA-EAST-1 AWS-AP-SOUTHEAST-1 AWS-AP-SOUTHEAST-2 AWS-US-WEST-1
VDI	89	21	5	4	3	5	4	PII PCI GDPR ISO27001 PCI-DSS SOX OS: WINDOWS OU: OFFICE_APPS OFFICE TEXAS DATACENTER ACE WEST
Loans	88	21	5	4	3	5	4	PII PCI GDPR ISO27001 PCI-DSS SOX BU: WHOLESALE OS: UNIX OU: CORE_BANKING RESPDOMAIN: CONSUMER OFFICE TAMPA BACKOFFICE WEST-US OFFICE PANAMA CITY OFFICE ORLANDO OFFICE TEXAS FRONT OFFICE SOUTH-US
AS400	80	18	2	4	3	4	5	PCI GDPR ISO27001 PCI-DSS SOX BU: WHOLESALE BANKINGSHELL: UNIX OU: CORE DATACENTER ACE EAST DATACENTER ACE WEST
Customer Portal Frontend	80	21	5	4	3	5	4	PII GDPR ISO27001 OS: UNIX OU: EXTERNAL_CONNECTION DATACENTER AZURE WEST-US
Dealing room	80	21	5	4	3	5	4	PII PCI GDPR ISO27001 PCI-DSS SOX OS: WINDOWS OU: MAIN_OFFICES OFFICE TEXAS
Gates	80	21	5	4	3	5	4	PII GDPR ISO27001 OS: WINDOWS OU: PHYSICAL_SECURITY DATACENTER ACE EAST DATACENTER ACE WEST
PKI	80	21	5	4	3	5	4	ISO27001 OS: WINDOWS OU: SERVICES DATACENTER ACE EAST DATACENTER ACE WEST

Figure 3. Protect Surfaces for a fictitious financial organization in the ON2IT demonstration system. Ref: On2IT Zero Trust Implementation Methodology Presentation to the CSA ZT workgroup 2/27/23

Business information systems often contain multiple related DAAS elements. One element is often considered the primary element from a business and risk perspective. For the purpose of this document and CSA ZT implementation guidance in general, we are equating business information systems with Protect Surfaces. Not every business information system will have constituent elements for each DAAS element type (columns). Some large and complex business information systems may be broken into subsystems that are comprised of distinct DAAS elements that are systematically related Protect Surfaces for zero-trust implementation purposes. This is especially applicable when subsystems contain disparate technology at different risk levels. For example, OT smart metering systems that are part of a larger service monitoring and billing business system could be considered a distinct subsystem. Table 1 below describes another set of sample Protect Surfaces.

Sample Protect Surfaces					
#	**Business Information System**	**Data**	**Applications**	**Assets**	**Services (Supporting)**
1	CRM system	Customer data Data on company products, services, contacts, resources and events for customer use	CRM application (SaaS)	CRM SaaS CSP's CRM Servers	Customer and Organizational Identity Services, DNS
2	Document repository	Files and metadata	Sharepoint Online	Microsoft infrastructure	Identity-as-a-Service (Azure Active Directory)
3	Payment System application	Data for cardholder data acquisition and payment processing	The web application that manages cardholder data and processes payments	Server hosting the database that has cardholder data persisted in it	External credit card payment processing services, DNS
4	Industrial Control System	Control, sensor and process data used to manage chemical processes in a chemical plant	Production chemical process control application	Chemical plant sensors and PLCs	Heating, Ventilation, and Air Conditioning (HVAC)
5	Smart energy metering and billing system	Electrical consumption and customer data	Customer monitoring and billing system	A smart meter that consumes energy signals to support system monitoring and customer billing	Smart meter wireless network

Table 1: Sample Protect Surfaces

An organization's digital presence and operations, including all data, applications, assets, and services, should be protected from potential threats, whether deployed in private, public, hybrid cloud, on-premise environments, or some combination thereof.

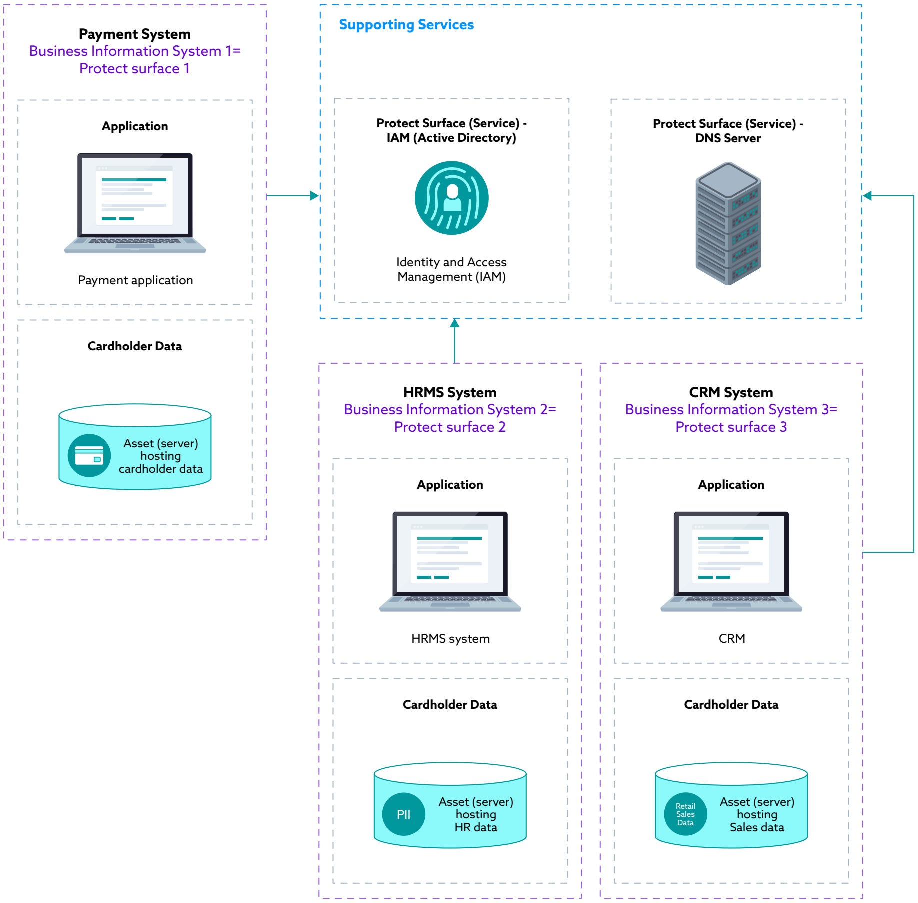

Payment System
Business Information System 1= Protect surface 1
Application
Payment application
Cardholder Data
Asset (server) hosting cardholder data
Supporting Services
Protect Surface (Service) - IAM (Active Directory)
Identity and Access Management (IAM)
Protect Surface (Service) - DNS Server
HRMS System
Business Information System 2= Protect surface 2
Application
HRMS system
Cardholder Data
PII
Asset (server) hosting HR data
CRM System
Business Information System 3= Protect surface 3
Application
CRM
Cardholder Data
Retail Sales Data
Asset (server) hosting Sales data

Figure 4. Protect Surfaces for another fictitious organization

Figure 4 illustrates several Protect Surfaces defined for an organization, all of which interface with each other.

- Protect Surface 1 consists of an application and a database that process cardholder data and is the primary, high-risk business information system for this organization because any compromise of this data will directly impact the customers, which could lead to regulatory fines, legal fees, and reputational issues.
- Protect Surface 2 consists of an HRMS application, which is an internal-facing business information system with privacy requirements.
- Protect Surface 3 consists of CRM, which is an internal-facing and external-facing business information system with commercial requirements.
- The DNS server (supporting service) constitutes an important Protect Surface, as any compromise of its operation can result in widespread service outages and disruptions
- Identity and Access Management (IAM) constitutes an important Protect Surface, as any

> compromise of its security can lead to unauthorized access, data breaches, and system vulnerabilities.

Figure 4 illustrates how Protect Surfaces interface with each other because of the inter-relationship between the various business information systems and support services.

Additionally, many organizations depend on external data feeds for their business. Data, such as stock market and geolocation data, is often provided by suppliers for consumption by end users or organizations. The organization is responsible for securing the data feed and ensuring the correct data is consumed reliably and securely from the designated supplier. This is part of data discovery and is relevant for mapping transaction flows and understanding how the business information system works.

Organizational data may be data hosted by an external business service provider such as Payroll service. In such a scenario, the data is still owned by the organization but is in the custody of the external business service provider who is responsible for securing the data and their service (which is a Protect Surface in its own right) in accordance with contractual and regulatory requirements, for which the owning organization remains accountable and liable.

Prioritizing Iterative Execution of the 5-Step Process

The .organization should comprehensively identify and document all their Protect Surfaces, including the associated risk and criticality to the organization of each business information system. Once the organization's set of Protect Surfaces are documented, they should be analyzed and prioritized for iterative implementation based on risk, criticality, and current level of security maturity for the execution of the Zero Trust process in the organization's journey.

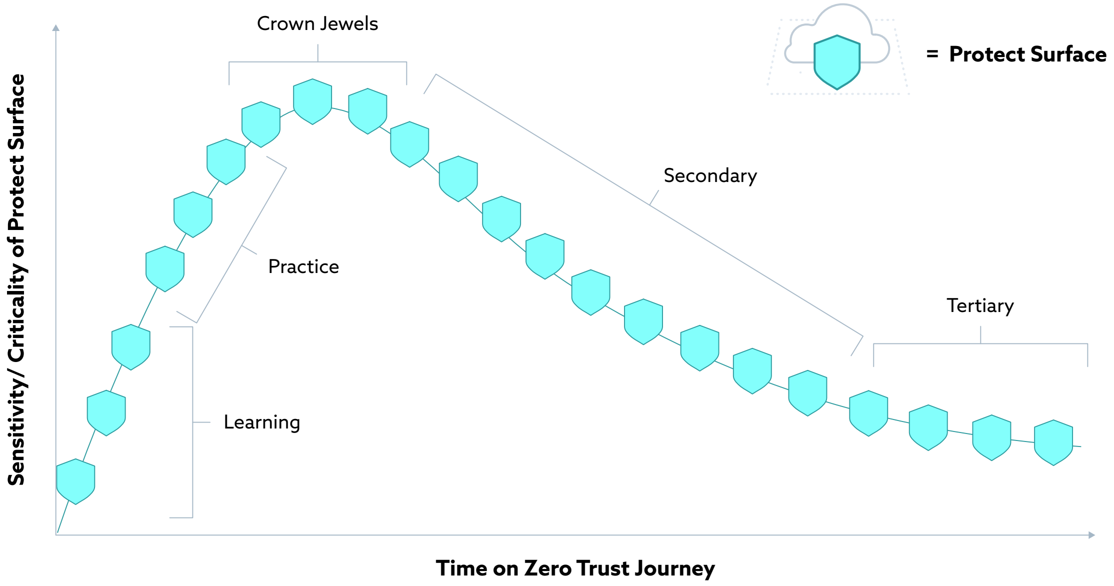


Figure 5. [The Zero Trust Learning Curve: Deploying Zero Trust One Step at a Time](), John Kindervag/ Palo Alto

Figure 5 illustrates that the organization may opt to choose a strategy of implementing a simple Protect Surface or two as test cases to gain some experience before commencing the Zero-Trust journey in earnest with critical business systems, or "crown jewels." Starting with simpler Protect Surfaces can allow valuable insights to be gained safely and then applied to more complex and higher-risk Protect Surfaces. Especially during the initial phases of their Zero-Trust journey, organizations are advised to implement one Protect Surface at a time. This iterative approach ensures that lessons learned from each implementation can be applied systematically to subsequent Protect Surfaces, facilitating a more informed and effective overall implementation.

Caution Regarding DAAS Elements Whose Purpose Is Uncertain

During the initial discovery phase, organizations may encounter DAAS elements whose purpose is unclear, for which there is a lack of institutional knowledge, or that appear to lack alignment with organizational goals. In these cases, caution is advised in resisting the temptation to disable or remove them immediately. These elements may play an important role in the organization's business operations and could cause disruptions if abruptly removed.

Instead, proceed through the subsequent Zero Trust implementation steps (especially 2 and 3), carefully evaluating these questionable elements to understand their function and impact better. Only once you have a comprehensive grasp of the organization's DAAS landscape and transaction flows and have validated the role of these elements can you make fully informed decisions regarding their removal or modification.

DAAS Elements Comprising a Protect Surface

Identifying the DAAS elements to be protected and understanding their business value and risk classification, along with the transactions in which those elements participate, enables organizations to define their Zero Trust Protect Surfaces. Using NSTAC's definition of Protect Surface, the following components form a part of the DAAS elements:

> - Data
> - Applications
> - Assets
> - Services

Data

Data is sensitive because it generally has regulatory or statutory implications, is valuable intellectual property, or has other significant value. Exfiltration or compromise of sensitive data can adversely impact an organization.

Data cannot exist in a vacuum. Data needs a "house" to live in (for example, a database server, file server, word processor, spreadsheet, etc.); the "house" (popularly referred to as an asset) needs to be secured. Securing data from breaches translates to securing the assets that host the data. Focusing on just data would mean zooming in on the assets that host the data, but this does not mean that applications and services should not be secured. If done so, it may translate to a disconnect between the data an application serves/consumes and the services underpinning the application.

Impact of a compromise:

Data, if compromised or exfiltrated, can lead to several impacts, including, but not limited to:

- Direct impact on the organization: When an organization's data is compromised, there is a direct impact on the reputation. The regulatory fine, the legal fees it incurs, the loss of intellectual property, the operational impact, and so on.
- Indirect impact on the end user of the service: However, the actual impact is on the end user whose data is compromised. Depending on the data type, this compromise may result in financial fraud for the end user, digital identity takeover, personal harm, etc.
- In between the direct and the indirect impact sit some impacts caused by the supply chain risk materialization, like the compromise of identities in an identity provider store or the introduction of malicious code in a product that customers consume, which typically can be referred to as external Protect Surface - APIs and CI/CD pipeline.

It is crucial as a first step to identify the locations where the data persists and the associated assets, applications, and services.

Types of data:

In order to locate data in the organization, it is important to know the types of data that an organization hosts and the mechanisms to locate this data. Data can be of the following three types.

- Structured data - Structured data is relatively easy to locate. This is because structured data can be parsed and searched. It is typically located in databases but typically accessed through applications. Database or application admins can often access the data directly.
- Semi-structured data - Semi-structured data is relatively challenging to parse. But it can still be parsed—for example, data in a comma-separated or a tab-separated file.
- Unstructured data - Unstructured data is challenging to parse. For example, data in an image or a Word document can be parsed if the general layout is known.

Now that we know the data types, it is essential to discover the data on the estate. This activity can be performed manually or in an automated fashion. An organization may approach this "big bang" or discover one data category at a time. We recommend the latter, as discovering data in an enterprise is usually a huge effort.

Tools exist to discover unstructured data and semi-structured data. But there are only so many tools to discover structured data, which can be discovered manually by interviewing people who manage applications or assets.

Applications and Workloads

Applications and workloads comprise the collection of software, hardware, and infrastructure that fulfill important business, functional, or operational requirements. Applications often have or include API interfaces, CI/CD pipelines and Web Services, and may be implemented as SaaS services or self-hosted in on premise or cloud IaaS/PaaS environments. All of these aspects and attributes are important metadata that help characterize the protect surface for Zero Trust implementation purposes.

Applications generally have or provide a direct or indirect interface to data, and often interface with supporting services. For example, an application for a shopping cart that allows shoppers to enter/retrieve credit/debit card data and pay for their shopping using payment card services.

- Applications and workloads provide an interface to data, control, and process business operations, transactions, and services through data acquisition, data processing, data consumption, execution of business process logic, and transmission of signals that control business operations and assets. The application, when processing data, is the workload. The output of the data processing is what the consumer expects - it may include but is not limited to data, an event, or a process. During this transaction, a malicious actor may compromise the application–for example, to exfiltrate data using SQL injection. Hence, protecting the data that consumers of the application input into the application involves securing the application from SQL injection.
- Today's applications often consist of libraries, frameworks, third-party software, and open-source software, which can introduce risks independently. To maintain line-of-sight visibility, a Software Bill of Materials (SBOM) provides a detailed inventory of the software components used in an application, including its dependencies, libraries, frameworks, and other third-party code. An SBOM includes information, such as the component's name, the supplier, the software version, and other unique identifiers. SBOMs can help organizations understand their software supply chains and identify potential security risks. An SBOM can also help identify changes to the software supply chain and vulnerabilities resulting from the changes. Lastly, SBOMs provide a common language for discussing the software supply chain with vendors.
- The business logic organizations create or purchase in the form of applications and workloads, often implemented as cloud services, give life to the data they create, acquire, process, consume and provide to others. This business logic is also critical in allowing us to secure and control access to data since it controls the data access authorization.

> Bringing logic as close to the data as possible allows us to implement granular security and promotes its treatment as another ZT Protect Surface.

Like data, applications may need to be discovered using monitoring and scanning tools to help find them all and collect relevant metadata.

Assets: Systems and Devices

A physical asset is a resource that hosts the data the organization seeks to secure and/or that the organization owns, uses, or performs critical tasks within the enterprise. From a Protect Surface perspective, assets are not limited to servers and workstations. Assets can include endpoint-connected devices as well as infrastructure devices throughout the environment, including IT (information technology), OT (operational technology), IoT (Internet of Things) devices and Industrial Control Systems (ICS). They can include a myriad of physical and virtual devices throughout the organization, such as:

> - Endpoint-connected devices and infrastructure devices, including those within IT (information technology), OT (operational technology), and/or IoT (Internet of Things) devices. These assets may be on-premise within the organization, at remote sites, with remote workers, and/or in cloud environments.
> - Endpoint-connected devices include user-based platforms, such as laptops, servers, smartphones, and headless assets like medical devices, point-of-sale (POS), sensors, printers, elevators, and smart building technology.
> - Manufacturing systems form another set of assets including, but not limited to, industrial robots, plant-control systems, SCADA systems, and so on.
> - Infrastructure assets include networking infrastructure components, both on-premise or in the cloud.
> - Operational technology (OT) are usually programmable systems that interact with their environment and operational equipment. For example, industrial control systems (ICS), building management systems (BMS), and fire control systems. These systems are asset-centric Protect Surfaces, designed for availability and to be used with minimal human intervention. They usually interface with data that helps configure these assets or control their interaction with the environment. For example, the data that controls fluoride levels in a water treatment system. OT may also be a part of critical national infrastructure (CNI), such as electricity grids, fire stations, and water treatment plants.
> - The Internet of Things (IoT) is a type of operational technology. It includes smart home devices, smart wearables, or any network-enabled device that can exchange data and information. IoT devices can form or be part of a Protect Surface. For example, smart televisions should be secured while being configured and used, and could provide an entry point for malicious actors.

Like data, assets may need to be discovered using monitoring and scanning tools to help find them all and collect relevant metadata.

Services

Services usually provide supporting functionality for business information systems, and are also protect surfaces in their own right. Services are often characterized as being part of identity and network/environment pillars, and/or as providing cross-cutting capabilities such as automation, orchestration, visibility, analytics.

Applying business and technical expertise enables organizations to create, manage, and optimize information and business processes. In a modern enterprise, this can be Cloud-based like Software-as-a-Service (SaaS), between applications or an Application Program Interface (API), or for common use like the Domain Name System (DNS). Applications also provide services. For example, a DNS service provides the mappings between IP addresses and hostnames/URLs, without which an end user would need to type out IP addresses on browsers in place of URLs. Services like DNS, DHCP, and SMB provide services for applications and networks. Any impact on confidentiality, integrity, and availability of these services results in an impact on the pillars as well. For example, DNS poisoning may direct an application consumer to a malicious hostname/URL, leading to data / credential exfiltration.

> - Identity and access management provide a channel for human and non-human entities to access assets and for consumers to conduct application transactions. Identity and access management also provide another function of Zero Trust: authentication and authorization before granting access. At this point, it is important to remember that confidentiality, integrity, and, to some extent, data availability can be compromised with identity and access control abuse.
> - The network perimeter is no longer restricted to on-premises and is expanding to include cloud services, network services, secure data and assets, applications, and services. Network and network devices provide perimeter security and network segmentation services. Micro-segmentation and nano-segmentation limit and prevent lateral movement and, in turn, limit access to unauthorized actors - human and non-human entities.
> - Automation and orchestration provide automated policy decisions for any authorizations to access data and automate the enforcement of those policies in real-time.
> - Visibility and analytics provide insight into all access requests made for the data by human and non-human identities. It helps define the Protect Surface by discovering, analyzing, and making visible all components - devices, data, networks, identities, services, etc. and how they are accessible and accessed.
> - Governance provides visibility to enterprise security risks to zero trust principles and manages the risks with support from cybersecurity policies, procedures, and processes within and across pillars

NSTAC, CISA Maturity Model and Protect Surfaces

The [National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Zero Trust and Trusted Identity Management] outlines maturity levels for the Zero Trust implementation process steps in Appendix A with increasing levels of automation corresponding to higher levels of maturity.

	Maturity Stage	Initial (1)	Repeatable (2)	Defined (3)	Managed (4)	Optimized (5)
	Description and Characteristics	The initiative is undocumented and performed on an ad hoc basis with processes undefined. Success depends on individual efforts	The process is documented and is predictably repeatable, using lessons learned in the initial phase	Processes for success have been defined and documented	Processes are monitored and controlled; efficacy is measurable	Focus is on continuous optimization
Step of the Five-Step Process	**1. Define the Protect Surface**	The DAAS element is unknown or discovered manually; data classification is not done or is incomplete	The use of automated tools to discover and classify DAAS elements has begun but is not standardized	Data classification training and processes have been introduced and are maturing: protect surface discovery is becoming automated	New or updated DAAS elements are immediately discovered, classified as assigned to the correct protect surface in an automated manner	Discovery and classification processes are fully automated
	2. Map the Transaction Flows	Flows are conceptualized-based interviews and workshops	Traditional scanning tools and event logs are used to construct approximate flow maps	A flow mapping process is in place; automated tools are beginning to be deployed	Automated tools create precise flow maps; all flow maps are validated with system owners	Transaction flows are automatically mapped across all locations in real time

Figure 6. NSTAC Zero Trust Implementation Maturity Levels

The US Cybersecurity and Infrastructure Security Agency (CISA) leads the USA's effort to understand, manage, and reduce cybersecurity risk by supporting Federal Civilian Executive Branch agencies in evolving and operationalizing cybersecurity programs and capabilities. *CISA's Zero Trust Maturity Model (ZTMM V2)* provides an incremental approach to achieve continued modernization efforts related to Zero Trust within a rapidly evolving environment and technology landscape.[3]

The table below depicts the alignment of the CISA pillars and the Maturity Model as related to Protect Surface (DAAS) elements.

[3] https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Pillar	Surface DAAS Elements	Traditional	Initial	Advanced	Optimal
Data	Data	Limited knowledge of data location	Location of business-critical data known to business processes along with supporting systems.	The location of business-critical data and supporting systems is known and are manually mapped to a Protect Surface.	All data elements in the organization are mapped to a Protect Surface in an automated fashion
Applications and Workloads	Applications	Limited knowledge of application functionality and the supporting services. Missing concept of Protect Surface	Critical business processes are aware of their applications, the supporting services and the data elements.	All business processes are aware of the applications, the supporting services and data elements in their department. Mapping to Protect Surface is a manual process.	All applications, their supporting services and data elements are mapped to Protect Surfaces in an automated fashion.
Devices	Assets	Limited knowledge of assets and the applications running on them. Limited knowledge of data persisted on the assets.	Technical teams manage assets in a proactive way, maintain an inventory of applications, and understand the classification of persisted data. But any concept of Protect Surface is missing.	Assets and applications are inventoried, data persisted on the assets is classified. And are manually mapped to Protect Surfaces.	Businesses and technical teams have worked proactively mapped all assets, applications and data to Protect Surfaces, in an automated fashion.
Networks	Assets	Large perimeter/ macro-segment	Initial isolation of critical workloads	Expanded isolation and placing of Protect Surface manually in micro-segments	Protect Surfaces are automatically placed in distributed micro-segments.

Identity	Services	Implicit trust	Identity and Access management teams are aware of identities that are part of applications, services and assets, but are not aware of access to data.	Awareness of identities that are part of applications, services and assets, data and mapped to Protect Surfaces.	Continuous validation/ context-based access control for the Protect Surfaces.

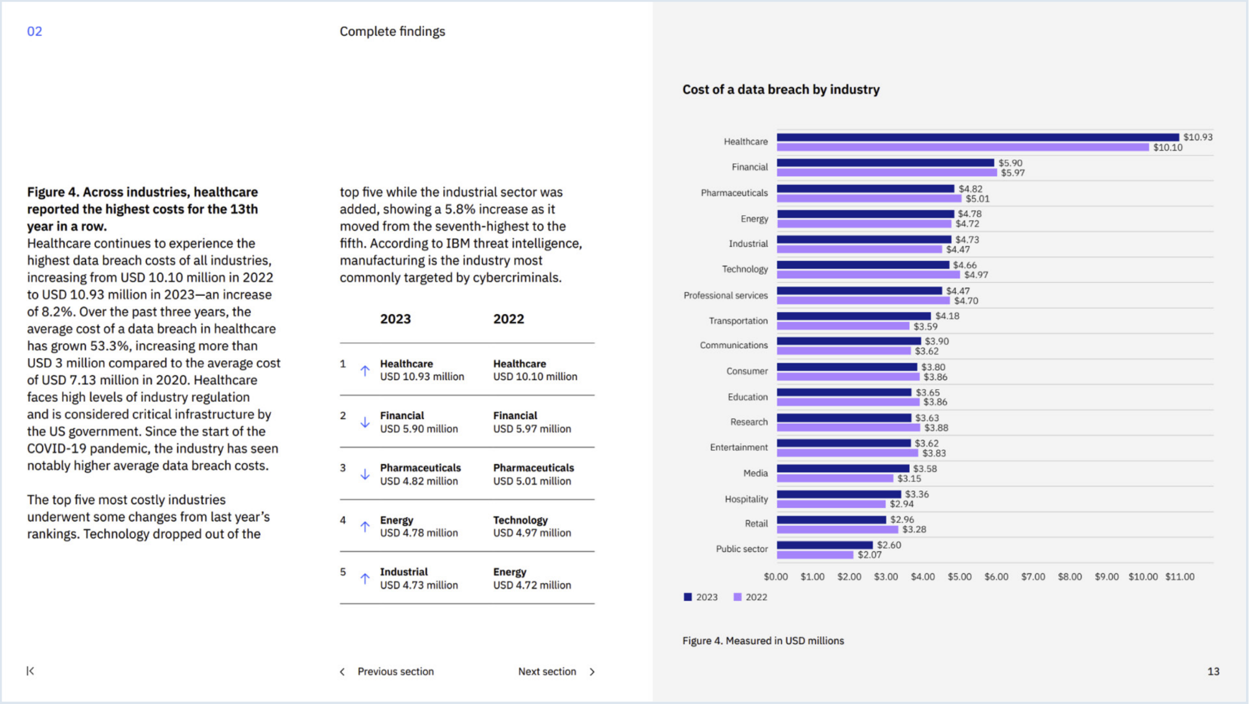
Table 2: Alignment of Zero Trust pillars with CISA maturity levels for the Protect Surface

Risks and Impacts of Protect Surface Compromises

Critical business assets take many forms. For many businesses, it will be their business data and applications. For others, it includes critical infrastructure and operational technology, such as chemical or water treatment plants, or drug production lines that could be at risk of compromise.

Data and information can be monetized - and weaponized - in various ways. That is why data is often the primary target, whether for exfiltration (breaches) and/or encryption by ransomware. Understanding the risks and potential impacts of compromises is an integral part of Step 1 and helps with ZT implementation prioritization. Let's illustrate this with some examples.

The image on the following page is from IBM's Ponemon report (URL). The report documents the cost of a data breach in various industries, depicting the breadth of data breaches. To ensure that such breaches are prevented, organizations secure and protect data.



02 Complete findings

Figure 4. Across industries, healthcare reported the highest costs for the 13th year in a row.
Healthcare continues to experience the highest data breach costs of all industries, increasing from USD 10.10 million in 2022 to USD 10.93 million in 2023—an increase of 8.2%. Over the past three years, the average cost of a data breach in healthcare has grown 53.3%, increasing more than USD 3 million compared to the average cost of USD 7.13 million in 2020. Healthcare faces high levels of industry regulation and is considered critical infrastructure by the US government. Since the start of the COVID-19 pandemic, the industry has seen notably higher average data breach costs.

The top five most costly industries underwent some changes from last year's rankings. Technology dropped out of the top five while the industrial sector was added, showing a 5.8% increase as it moved from the seventh-highest to the fifth. According to IBM threat intelligence, manufacturing is the industry most commonly targeted by cybercriminals.

		2023	2022
1	↑	**Healthcare** USD 10.93 million	**Healthcare** USD 10.10 million
2	↓	**Financial** USD 5.90 million	**Financial** USD 5.97 million
3	↓	**Pharmaceuticals** USD 4.82 million	**Pharmaceuticals** USD 5.01 million
4	↑	**Energy** USD 4.78 million	**Technology** USD 4.97 million
5	↑	**Industrial** USD 4.73 million	**Energy** USD 4.72 million

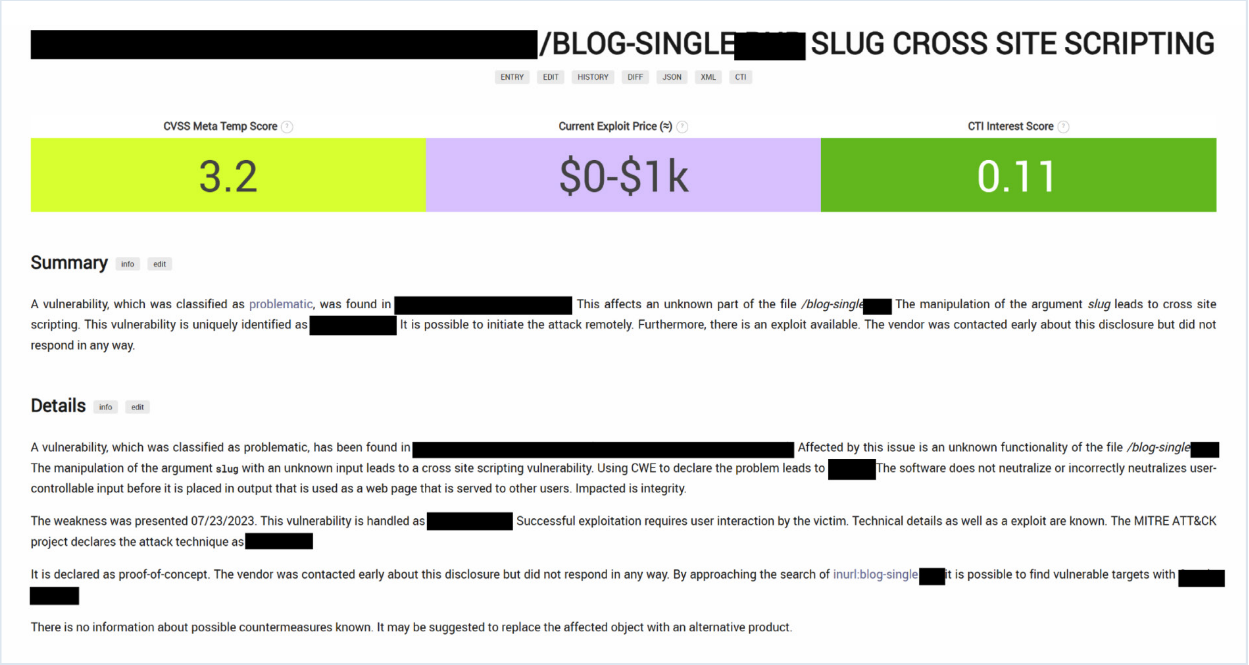
Cost of a data breach by industry

Figure 4. Measured in USD millions

‹ Previous section Next section ›

13

Figure 7: Cost of a Data Breach Report 2023 - Ref: (https://www.ibm.com/reports/data-breach)



[redacted]/BLOG-SINGLE[redacted] SLUG CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.2	$0-$1k	0.11

Summary

A vulnerability, which was classified as problematic, was found in [redacted] This affects an unknown part of the file */blog-single*[redacted] The manipulation of the argument *slug* leads to cross site scripting. This vulnerability is uniquely identified as [redacted] It is possible to initiate the attack remotely. Furthermore, there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as problematic, has been found in [redacted] Affected by this issue is an unknown functionality of the file */blog-single*[redacted] The manipulation of the argument `slug` with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to [redacted] The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. Impacted is integrity.

The weakness was presented 07/23/2023. This vulnerability is handled as [redacted] Successful exploitation requires user interaction by the victim. Technical details as well as a exploit are known. The MITRE ATT&CK project declares the attack technique as [redacted]

It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way. By approaching the search of inurl:blog-single[redacted] it is possible to find vulnerable targets with [redacted]

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Figure 8: Cost of an exploit to carry out a breach, Ref: https://vuldb.com/

The above illustration is from an open-source vulnerability management database. The illustration concerns a vulnerability exploited to exfiltrate data.

In the above example, if data exfiltration was not the objective then cross-site scripting may not have been the focus of the exploit. Any application using the file/blog-single would not be vulnerable.

The above concepts are related to data generated by and for IT systems. However, Operational Technology (OT) and the Internet of Things (IoT) also generate and consume data and often execute important operational functions for the organization which may lead to different types of impact when compromised. For example, such systems can be weaponized. OT and IoT systems differ slightly regarding how and where the data is generated and acquired and what functions the technology performs. With discrete OT and IoT components, the data generation/consumption endpoint is usually located away from the asset that acquires data. For example, a radioactivity detector detects signals from radioactive material. Any compromise of the detector may lead to not detecting radioactive signals, leading to disastrous results when staff are exposed to harmful radiation or when radioactive materials are inadvertently released or smuggled into or out of a facility.

Similarly, in the event of a compromise of an asset that hosts application(s) to control the input of required fluoride level to a water plant, it may lead to poisoned water for the location. This example is shown in the figure below.

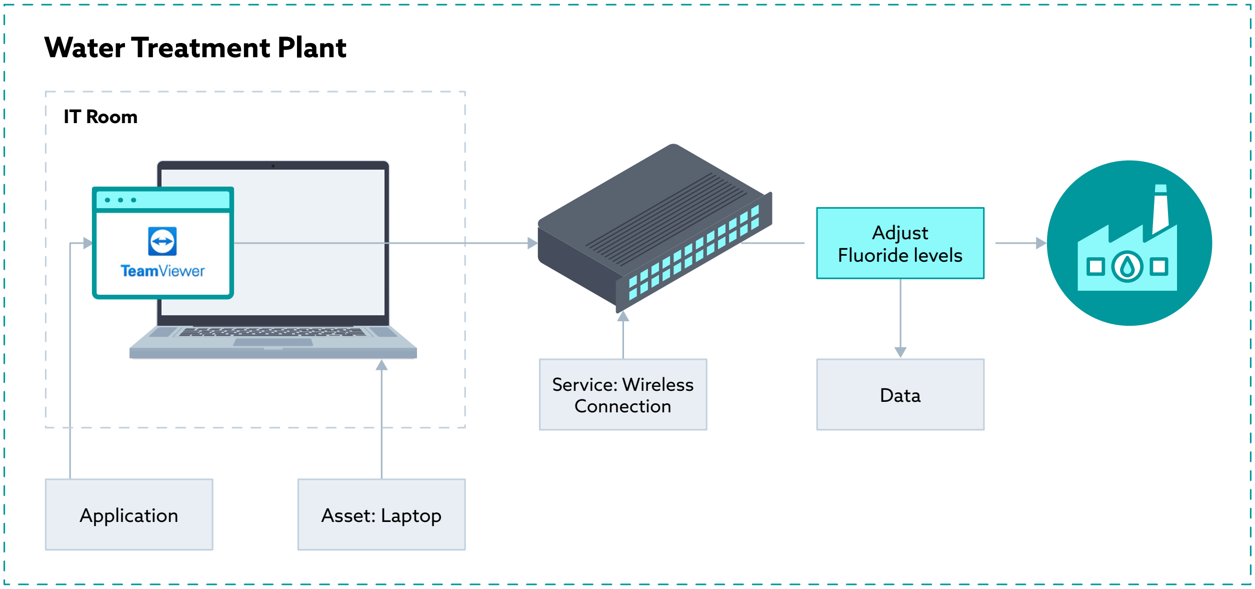


Figure 9: Protect Surface for a Water Treatment Plant

Understanding requirements and potential impacts related to confidentiality, integrity, and availability contribute to identifying and rating the risks related to each Protect Surface. For example, risks of compromising confidential data should be considered, as should the potential impact of a malicious actor (e.g. ransomware) encrypting data without authorization, thereby impacting availability requirements. Similarly, when an unauthorized actor increases or decreases the fluoride components of water in a water treatment plant, integrity (product quality) requirements are impacted. An important way to identify the risks related to a Protect Surface is based on the consideration of confidentiality, integrity, and availability requirements and potential impacts of various potential compromises and outages.

Applying Data Classifications

Data is central to many Protect Surfaces, so the applicable risk depends on the impact of potential data compromises. To ensure that a consistent approach is applied to identifying and classifying risk, data can be grouped into categories that describe the impact in terms of financial loss, reputational loss, or or various other potential impacts. The following are some examples of data classifications.

Data classification based on regulatory and safety requirements:

> a. Example 1
>   1. Radioactive
>   2. Toxic
>   3. Unclassified
>
> b. Example 2
>   1. Hazardous
>   i. Safety of public human property
>   2. Sensitive
>   i. IP, trade secrets
>   3. Regulatory
>   i. Telecom, telemetric, PII, PCI, PHI
>   4. Purposeful classification based on business outcome or value
>   i. Intellectual property

Once data is classified, the ZeroTrust journey depends on how the organization assesses the importance of the applicable Protect Surfaces and addresses the applicable risks in their Zero Trust implementation. NIST SP 800-60 offers some useful guidance related to information classification and identifying related risks.

Attack Surface Versus Protect Surface

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.”

While the Protect Surface is tangible and has a defined boundary, the attack surface is a moving target due to its intangible and ever-changing nature with BYOD, introducing new services, etc. What differentiates the Protect Surface from the attack surface is that the Protect Surface does not change or may have minimal changes with the addition of assets, whereas an attack surface changes frequently, e.g., as new vulnerabilities and attack vectors emerge.

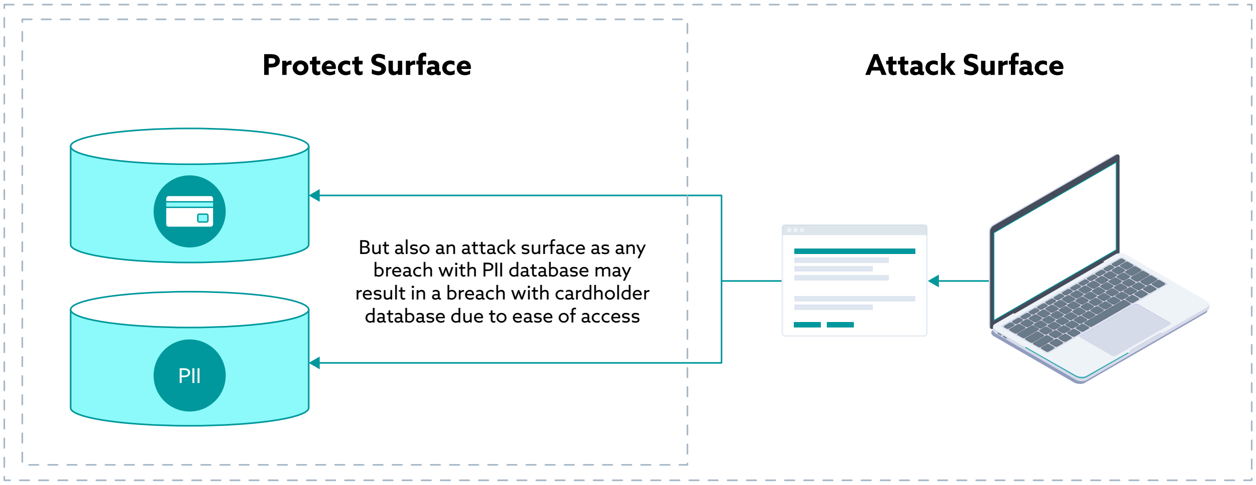

Protect Surface
Attack Surface
PII
But also an attack surface as any breach with PII database may result in a breach with cardholder database due to ease of access

Figure 10: Protect Surface seen in the context of the attack surface

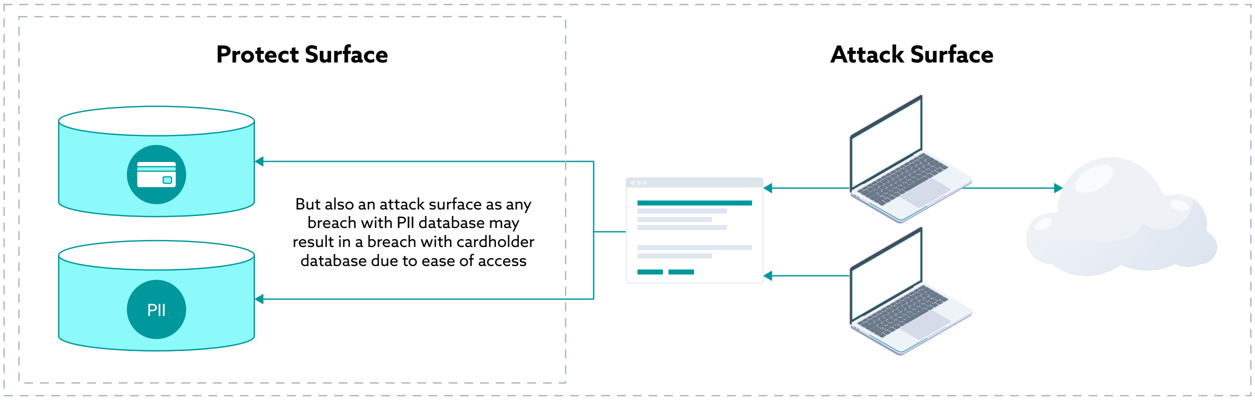

Protect Surface
Attack Surface
PII
But also an attack surface as any breach with PII database may result in a breach with cardholder database due to ease of access

Figure 11: Asset added to the attack surface does not alter the Protect Surface

A Protect Surface gives an inside-out view of a system, whereas an attack surface gives an outside-in view of a system.

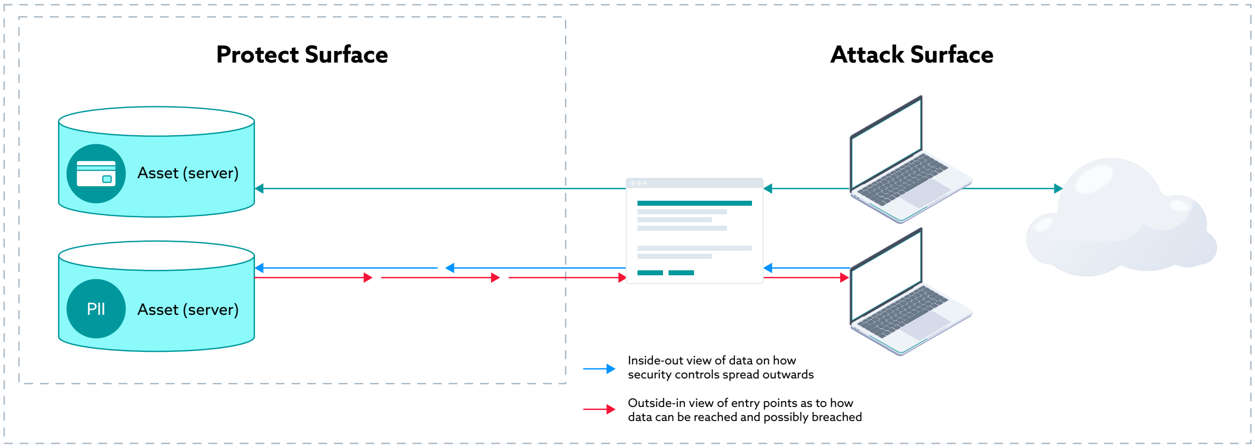

Protect Surface
Attack Surface
Asset (server)
PII
Asset (server)
Inside-out view of data on how security controls spread outwards
Outside-in view of entry points as to how data can be reached and possibly breached

Figure 12: The Protect Surface and attack surface complement and supplement each other

Protect Surface and attack surface complement each other. While Protect Surface helps identify what needs to be protected, an attack surface helps identify how the Protect Surface may get compromised, how attacks might be executed, and to optimally secure the organization's Protect Surface.

Looking Ahead, After Protect Surfaces are Defined

Once the Protect Surfaces have been defined, associated Transaction Flows must be mapped to, from, and within the Protect Surface in step 2 - including developing an understanding of how various DAAS elements interact with other resources on the network. Protect Surfaces align with one or more business processes. Authorized users consume, execute, and manage business processes that should be identified and documented as metadata associated with each Protect Surface. User population and data access information is required for ZT step 2 - Mapping the Transaction Flows. You can understand how the business information system operates by mapping transaction flows. (NSTAC Report to the President on Zero Trust and Trusted Identity Management.) The mapping will also directly inform where to place required controls in steps 3 and 4.

Transactions provide interfaces to data through applications and/or services. Transactions include (but are not limited to) data acquisition, processing, and persistence of data.

Processing of data that requires access includes the following example tasks:

> - Consumers inputting data into an application for shopping, consumers acquiring quotes for insurance products
> - Administrators making changes to banking rate of interest
> - The finance team making payments to suppliers in response to invoices
> - Applications generating events for transactions conducted within the application

The following are two examples of transaction flows:

> - Transactions carried out with the data:
>   - Applications that provide an interface with data help carry out transactions that acquire, process, and persist data.
>   - An OT, such as motion detectors, that acquire data (movements) and convert the data into alerts.
>   - A health application that counts pulse rate and converts into calories burnt in a period of time.
> - Transactions carried out between Protect Surfaces to support data:
>   - Discovery of database server by an application service to persist data, using DNS server.
>   - A database administrator logs into a database server to maintain data using an identity and access management system.
>   - An administrator logging into an administrative console of an IoT-based desk monitoring system to report on occupied desks.
>   - Applications require the support of services that make transactions work as required. For example, discovery of the application via DNS servers, visibility, and analytics for troubleshooting and investigations.

The Zero Trust Network/Environment and Applications/Workloads Working Groups will jointly develop and publish a document covering “Step 2, Mapping the Transaction Flows” in depth.

Overall, understanding and documenting Protect Surfaces within an organization requires a comprehensive approach that involves establishing relationships between Protect Surfaces, what each one does, and its importance to the organization, then implementing appropriate security measures, monitoring for threats and attacks, and responding to incidents promptly and effectively.

Conclusion

Defining the Protect Surface, while only the first step on the Zero-Trust journey, is where the business benefits begin to accrue:

- Improved visibility: Starting on a journey of the definition of Protect Surfaces in an organization leads to discovering data, applications, assets, and services managed within their importance to the organization. The organization can only protect what it sees, and starting on a journey of locating the DAAS elements provides this first level of visibility.
- Improved security: The definition of a Protect Surface facilitates moving security controls closer to the business assets by securing transactions, data, assets, applications, and services.
- Improved compliance: Many regulations and standards (such as HIPAA and General Data Protection Regulation (GDPR) require organizations to implement strong security controls to secure sensitive data. By defining Protect Surfaces, an organization can demonstrate compliance with these requirements with the security controls implemented to secure data.
- Reduced costs: By defining all the critical Protect Surfaces of the organization and implementing required security controls, the organization can reduce data compromise. Thus reducing any primary or secondary costs of a breach.
- Improved business resilience: Understanding the critical Protect Surfaces needed for business operations enables a clear focus, dedicated effort, and robust support in times of failure, enhancing overall business resilience.

This paper defines the Protect Surface and clarifies its components: DAAS elements comprising information systems and the business processes they support. It provides insights into the initiation of the Zero Trust implementation process and the key aspects of defining and protecting surfaces and securing them in subsequent steps. Additionally, the discussion covers DAAS elements, the application of the Maturity Model, and Mapping Transaction flows en route to Zero trust implementation and operation. The paper underscores the broader application of Protect Surfaces beyond just IT systems, encompassing OT and IoT. Readers will find valuable guidance to commence and execute their Zero-Trust journey.

Useful References

NSTAC Report to the President on Zero Trust and Trusted Identity Management

> - Definition of Protect Surface: Refer to Page 6
> - Definition of Attack Surface: Refer to Page 16
> - Appendix A for Protect Surface Maturity Model

CSA Zero Trust Advancement Center

> - CSA Zero Trust Advancement Center

John Kindervag Presentation recordings & blogs

> - ZT Implementation and Guiding Principles Briefing by John Kindervag
>   Passcode: ZTimplement101!
> - ZT Data Protection and Privacy Briefing by John Kindervag
>   Passcode: DataPillar7!
> - Palo Alto Blog with "The Zero Trust Learning Curve"

CISA Maturity Model V2

> - CISA Zero Trust Maturity Model V2

US DoD Reference Architecture & Strategy

> - Department of Defence Zero Trust Reference Architecture
> - Department of Defence Zero Trust Strategy

NIST Special Publications

> - NIST SP 800-207, Zero Trust Architecture
> - A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments
> - Implementing a Zero Trust Architecture figure 1 page 54, 2nd preliminary draft
> - Guide for Mapping Types of Information and Information Systems to Security Categories
> - NIST SP 800-60r2 initial working draft, Guide for Mapping Types of Information and Information Systems to Security Categories (enhanced draft)

IBM Ponemon Report

> - IBM Ponemon Report

Venturebeat

- Venturebeat's report on clouds adopting Zero Trust

Vulnerability Database owned by Pyxyp @https://pyxyp.com/

- Vulnerability Database (vulnDB)

Gartner

- Gartner Report on Zero Trust

DHS LinkedIn Article

- Importance of defining a Protect Surface