Zero Trust Core Principles

A White Paper by:

Tuhinshubhra Ghosh, Technology Consultant, DXC Technology
Nikhil Kumar, President, Applied Technology Solutions
Sai Mohan Sakuru, Principal Consultant, Wipro
Patrick Shirazi, Managing Enterprise Architect, Capgemini
Mark Simos, Lead Cybersecurity Architect, Microsoft
Altaz Valani, Director of Insights Research, Security Compass
Anthony Carrato, The Open Group Invited Expert
Stephen Whitlock, The Open Group Invited Expert
Jim Hietala, VP Business Development & Security, The Open Group
John Linford, Security & OTTF Forum Director, The Open Group
Andras Szakal, VP & Chief Technology Officer, The Open Group

April 2021

Zero Trust Core Principles
Document No.: W210

Published by The Open Group, April 2021.
Any comments relating to the material contained in this document may be submitted to:
The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom
or by email to:
ogpubs@opengroup.org

Table of Contents

Boundaryless Information Flow ™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

Threats and technologies are evolving at an ever-increasing rate, requiring organizational flexibility for digitalization, agility, and adaptability. Digital Transformation is bringing change with ever-increasing velocity, complexity, and disruption. Zero Trust is the overarching information security approach for the digital-first enterprise, but it originates in many ways from the work of The Open Group Jericho Forum. Implemented through a comprehensive strategy to secure data/information, applications, infrastructure, and interfaces (APIs and communication patterns), Zero Trust enables organizations to grow and operate in a "trusted" fashion in an "untrusted" (zero trust) network. It allows organizations to adapt security to the needs of business flexibility, agility, and adaptability while retaining the same (and often stronger) security assurances of confidentiality, integrity, and availability for business assets. Above all, Zero Trust reflects a transition from the traditional approach of perimeter-based security to a security operating model that is business-enabling and data-centric.

This document introduces Zero Trust to leaders in Business, Security, and IT. It provides a foundation on the drivers for Zero Trust, their implications, and the role of Zero Trust. In the Digital Age, the necessary seamless flow of data across myriad networks, applications, storages, and other resources introduces the dilemma that it is no longer feasible, or even possible, to consider all elements of the service topology as "trusted". Success in this environment is engendered by the Boundaryless Information Flow™ vision, and the cornerstone for information security for organizational success in this environment is Zero Trust.

Introduction

Context

The world is transitioning to digital-first business models at an exponential rate. Digital Transformation[1] is a priority for many organizations. Threats and technologies are evolving at an ever-increasing pace, requiring agility and adaptability. This need for organizational agility and adaptability is further enhanced by geopolitical changes, disruptive events like the COVID-19 pandemic, the migration to remote work, ever-changing business models, and rapidly evolving relationships in an ecosystem in flux. For the organization, the new Digital Age is characterized by *velocity*, *complexity*, and *disruption*, with the goal of enabling better user experience through simplicity, speed, and ability to support scale.

Traditional, perimeter-based approaches built on legacy models of identity, authentication, and authorization do not meet the needs of a digital business environment. In this modern digital world with ever-evolving threats – such as phishing, social engineering, and particularly insider-threats – organizations must abandon the flawed assumption that networks, both internal and external, are secure. Moreover, the velocity and outside-in nature of a digital-first business model require an Agile approach to securing both partner and customer interactions. Organizations[2] must shift from traditional models to modern, Zero Trust approaches based on asset or data-centric security, policy-driven access controls, modern identity management, and secured zones. These solutions must be simple and cost-effective to develop, implement, transition to, operate, maintain, and evolve.

Defining Zero Trust

Zero Trust – an information security approach that focuses on data/information security, including lifecycle, on any platform or network.

As an information security approach, Zero Trust security capabilities enable organizations to secure data/information, applications, APIs, and any data integrations, on any network, including the cloud, internal networks, and public or untrusted (zero trust) networks.

Zero Trust is implemented through a comprehensive strategy and provides a security framework based on asset or data-centric security, policy-driven controls, modern identity management, and security zones/domains. Zero Trust provides organizational flexibility, agility, and adaptability in addition to the traditional security assurances of confidentiality, integrity, and availability for business assets.

Zero Trust is achieved by leveraging a combination of existing investments and offering new capabilities.

[1] This document relies on The Open Group Digital Practitioner Body of Knowledge™ Standard (see References) for definitions and explanations of terms and concepts related to Digital Transformation, Digital Enterprise, etc.

[2] The terms "organization" and "business" are used interchangeably in this document because some organizations may not be commercial businesses, but all are organizations.

Zero Trust Core Principles

Zero Trust Architecture (ZTA) – the implementation of a Zero Trust security strategy that follows well-defined and assured standards, technical patterns, and guidance for organizations.

Why Zero Trust?

Zero Trust brings security to the users, data/information, applications, APIs, devices, networks, cloud, etc. wherever they are – instead of forcing them onto a "secure" network. In other words, Zero Trust shifts the perceived role of security restricting business to security enabling business.

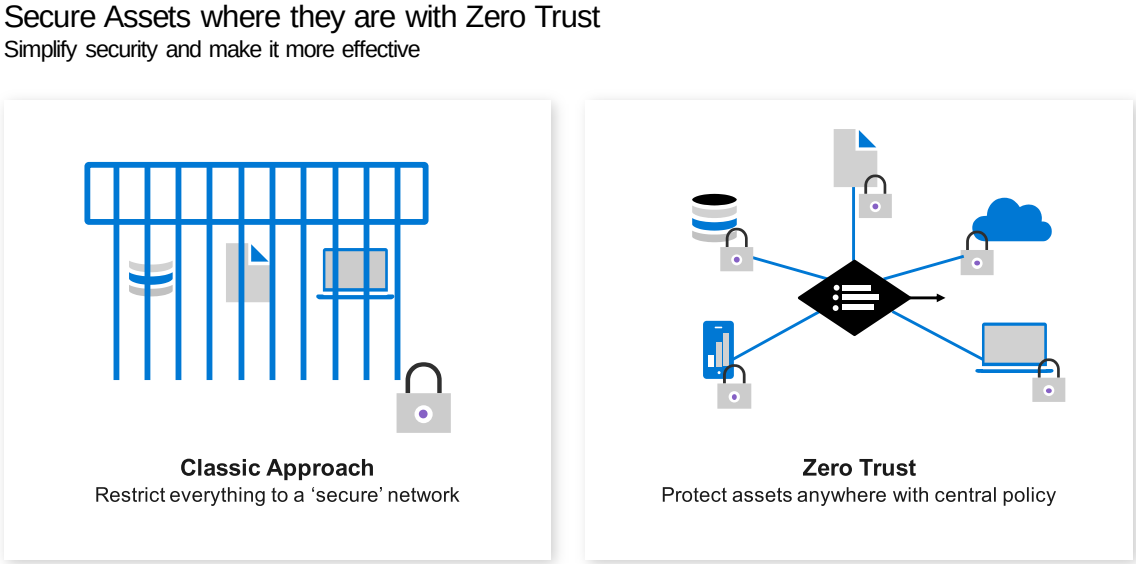

Figure 1: Classic *versus* Zero Trust Approach

Zero Trust enables the continuous journey toward digitization and a digital business model, which will require several intermediate steps before an end state. A Zero Trust security architecture facilitates minimum disruption and greater agility through each intermediate step.

Zero Trust enables rapidly building meaningful and sustainable assurances for business assets and business processes in a modern, digitized environment. It secures business workflows from modern information security threats by securing data/information, applications, APIs, and devices regardless of what network they are on.

Fundamentally, Zero Trust enables organizations to grow and operate in the rapidly changing business models, technologies, regulatory mechanisms, and threats that are the hallmark of the Digital Enterprise.

Zero Trust Core Principles

Zero Trust is not a new silver bullet – many of its underlying concepts (such as de-perimeterization) build on learnings from the Jericho Forum,[3] which have been validated over time. These learnings describe the effective breakdown of the perimeter security model[4] in the 2006-2012 timeframe and the need for new security architectures with a focus on identity and data protection – two key tenets of Zero Trust.

Current technology and business environments have made ZTAs imperative.

How Significant is this Change?

Implementing Zero Trust will be a long-term, incremental, evolutionary journey that will leverage many existing security investments. As an over-arching information security paradigm, it will cause cultural, strategic, and philosophical shifts to people, processes, and technology throughout organizations.

Zero Trust will affect different parts of the organization differently:

- *Business units* will more effectively operate in a compliant manner (whether internal or external) by removing artificial constraints to operating workflows, while enabling organizational agility and entry into new markets
- *Security organizations*, in particular, will undergo a substantial cultural and strategic shift, affecting nearly all aspects of their operations – this will be initially challenging but will result in greater effectiveness, responsiveness, and ability to meet regulatory requirements
- *Technology organizations* will change the way they architect, build, and operate applications and infrastructure – this will be tied closely to any cloud and DevOps initiatives, which may already be in progress

  Zero Trust represents a change in a fundamental assumption (from a safe network to a hostile data and application environment) and will require changes throughout current practices for security, productivity, application development, IT operations, and more.
- *Governance, Risk, and Compliance (GRC) teams* will need to embrace new standards and guidance to ensure that Zero Trust is integrated into the culture of their organizations

  GRC teams will also need to consider existing and new contracts and the way they are written and governed.

Similar to securing physical assets in an unknown or potentially hostile physical environment (e.g., ATMs), Zero Trust ensures acceptable confidentiality, integrity, and availability assurances for intellectual property, data, and applications. Organizations will be able to reduce risk and enable agility by more seamlessly integrating security controls and architectures, thus limiting the impact of threat events and leading to greater resiliency and efficiency.

[3] These include the Jericho Forum Commandments, the Jericho Forum Identity Commandments, the Trust Ecosystem Guide, and the Need for Data Principles White Paper (see References).

[4] Previous iterations of Zero Trust were often referred to as perimeter-less or a new identity perimeter.

Zero Trust Core Principles

Zero Trust supports modern business scenarios by allowing organizations to move agilely and securely in a modern ecosystem of varying participants (including individuals and organizations), with relations in flux.

Zero Trust Drivers, Requirements, and Capabilities

Zero Trust enables organizations to proactively meet the drivers for the Digital Age. These drivers lead to the requirements and, therefore, the capabilities of Zero Trust, as shown in Figure 2, Figure 3, and Figure 4, respectively.

Zero Trust Drivers

Figure 2 highlights the key drivers. This is not intended as a complete list, for organizations will have their own nuances, and traditional 5-force models first described by Porter (1979)[5] can be used to determine and focus these drivers. However, in general, most organizations engaged in Digital Evolution[6] tend to apply one or (typically) more of these drivers to define their roadmaps.

The scenarios presented in Examples of Zero Trust in the Modern Digital Enterprise (on page 25) apply the drivers, requirements, and capabilities and show their relationships with the Core Principles outlined later in this document.

Figure 2: Zero Trust Key Drivers

[5] How Competitive Forces Shape Strategy, Michael E. Porter – see References.

[6] Digital Evolution refers to the process of continuous Digital Transformation.

Zero Trust Core Principles

- **Evolving Business Models**:
  - Driven by changing business, regulatory, and technical environments
  - Evolution of Digital as the single most disruptive element for organizations and the biggest driver for Zero Trust
  - Outside-in business strategy emphasizing providing value to customers
- **Emerging Partnerships**:
  - Emerging partnerships, relationships, customers, supply chains, and organizational ecosystems; e.g., evolving integration of data and applications with partners
- **Rapidly Changing Technology**:
  - Cloud computing, often hybrid-cloud, and the adoption of Software as a Service (SaaS), serverless computing, edge computing, and microservices
  - Complex communication patterns; e.g., REST, file, streaming, message-oriented, event-driven
  - Artificial Intelligence (AI) and its variants; e.g., Robotic Process Automation (RPA), Machine Learning (ML), Natural Language Processing (NLP), Internet of Things (IoT), Industry 4.0
- **Regulatory, Geopolitical, and Cultural Forces**:
  - Evolving and often lagging regulatory requirements driven by geopolitical forces, cultural forces, and maturation of the Internet
  - Privacy policies, such as California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), Chinese privacy laws
  - Impacts to organizations selling in multiple environments or operating across multiple jurisdictions
- **Disruptive Events**:
  - Events such as 9/11, 2008 Great Recession, or the COVID-19 pandemic
- **Paradigm Shift to Remote Work**:
  - Shifting to remote work, driven by organizational intent and laws
  - Enabling mobility so that individuals can work or collaborate wherever they are
  - Support for families and improved employee productivity
  - Savings in real estate and maintenance
  - Reduced impact on climate change

Zero Trust Core Principles

Zero Trust Requirements

The drivers above help define the requirements to determine the capabilities that a Zero Trust must support. As Figure 3 shows, these requirements tend to disrupt existing processes and models, defining capabilities that must be supported by a modern information security architecture for the Digital Age.

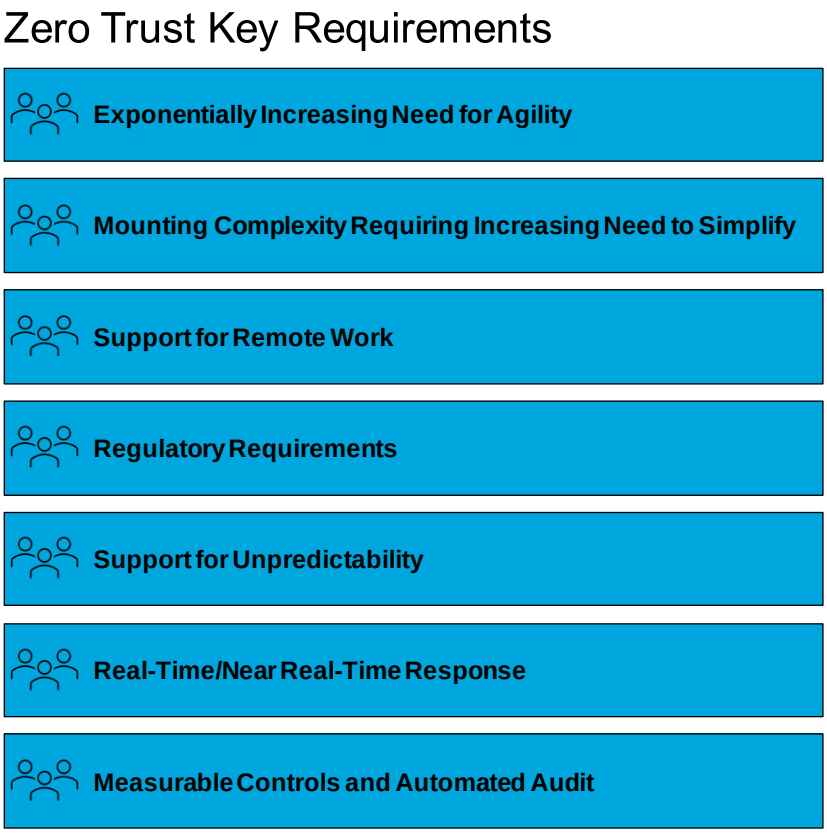

Figure 3: Zero Trust Key Requirements

- **Exponentially Increasing Need for Agility**:
  - Business models are rapidly evolving and must include strategic and tactical planning
  - People organizations must plan for training and working with employees to adapt to continuous change and new capabilities
  - Both business and technology processes must be agile and measurable
  - Technology decisions must consider the rapid rate of change and disruption from ever-evolving technologies
  - Risk models must be able to adapt to the continuous, rapid rate of change
- **Mounting Complexity Requiring Increasing Need to Simplify**:
  - New business models

  - — Organizational ecosystems
  - — Diverse communication patterns
  - — Multiple and diverse data sources, with data becoming more critical for new technologies, such as AI
- **Support for Remote Work**:
  - — Bring Your Own X (BYOX); e.g., device, application
  - — Unpredictable networks
- **Regulatory Requirements**:
  - — New business and technology models driving new regulations, but often with delays between the new models and the new regulations
  - — Rapid and unpredictable geopolitical changes
  - — Local cultural or political changes expressed in jurisprudence (e.g., CCPA, GDPR)
- **Support for Unpredictability**:
  - — Unpredictability driven by disruptive events; e.g., 9/11, 2008 Great Recession, Dodd-Frank Act, Basel III, the COVID-19 pandemic
- **Real-Time/Near Real-Time Response:**
  - — Real-time/near real-time response to new and evolving threats
- **Measurable Controls and Automated Audit**

Zero Trust Core Principles

Zero Trust Capabilities

The Digital Age does not give us the luxury of time to meet the requirements using traditional network-based solutions, or individualized, interface, or per client, vendor, or supplier-level integrations; nor can we predict what changes it will bring. Zero Trust helps prevent lengthy audits in order to meet organizational needs. *Zero Trust provides organizations with a modern information security paradigm able to meet the capabilities that can support those requirements.* Figure 4 describes the key capabilities.

Figure 4: Zero Trust Capabilities

- **Adaptive Identity**:
  - Support for multiple classes of consumers and participants, whose roles and identity may evolve to meet rapidly evolving ecosystems and new environments
  - Ease of maintenance and operation while being agile and easy-to-modify
- **Threat Scope Reduction and Risk Avoidance**:
  - Reduced scope of threats to support agility and support complexity

  - Increased complexity and number of communication patterns increasing difficulty of addressing through a data and asset-centric approach

- **Context-Specific, Policy-Enforced Data Security:**
  - Holistic approach that reduces risk of exposed data across full lifecycle by best practices for continuous improvement
- **Separation of Concerns**:
  - Ability to support unpredictable consumers by decoupling security from the underlying resource so that clients of APIs and applications can evolve in a changing digitized environment
- **Real-Time/Near Real-Time Response**:
  - Security Operations Centers (SOCs) with threat and incident response organizations, infrastructure, and processes
- **Automated Audit**:
  - Support for agility and increased complexity without traditional, lengthy processes
- **Policy-Driven Access Control**:
  - Support for adaptive identity, evolving and agile access to resources (e.g., applications, APIs), and unpredictable relationships between consumers and producers
- **Secured Zones**:
  - Adaptive and easily configured zones for data that must be protected, such as fraud, Personally Identifiable Information (PII), and Payment Card Industry (PCI) data

Advantages of a Zero Trust-Driven Future

Zero Trust enables mobility and user choice because people can work anywhere on any (secure) device they choose, using the applications and data they need. This leads to improved organizational productivity, agility, and the ability to proactively support new and evolving capabilities.

Zero Trust improves confidence in the security mechanisms used to protect data and applications, further enabling the business.

Zero Trust provides support for quickly evolving organizational ecosystems, by enabling rapid creation and dissolution of business-to-business relationships.

As Figure 5 shows, in this digitized world, remote work is part of the norm. The digitization of organizations introduces complexity and the need for agility driven by, for example:

- Migration to the cloud
- The need to leverage SaaS providers
- Continued leveraging of legacy assets

Zero Trust Core Principles

- Privacy by design
- Data governance
- Rapidly changing national and global regulations
- Ever-changing organizational relationships in an ecosystem in flux

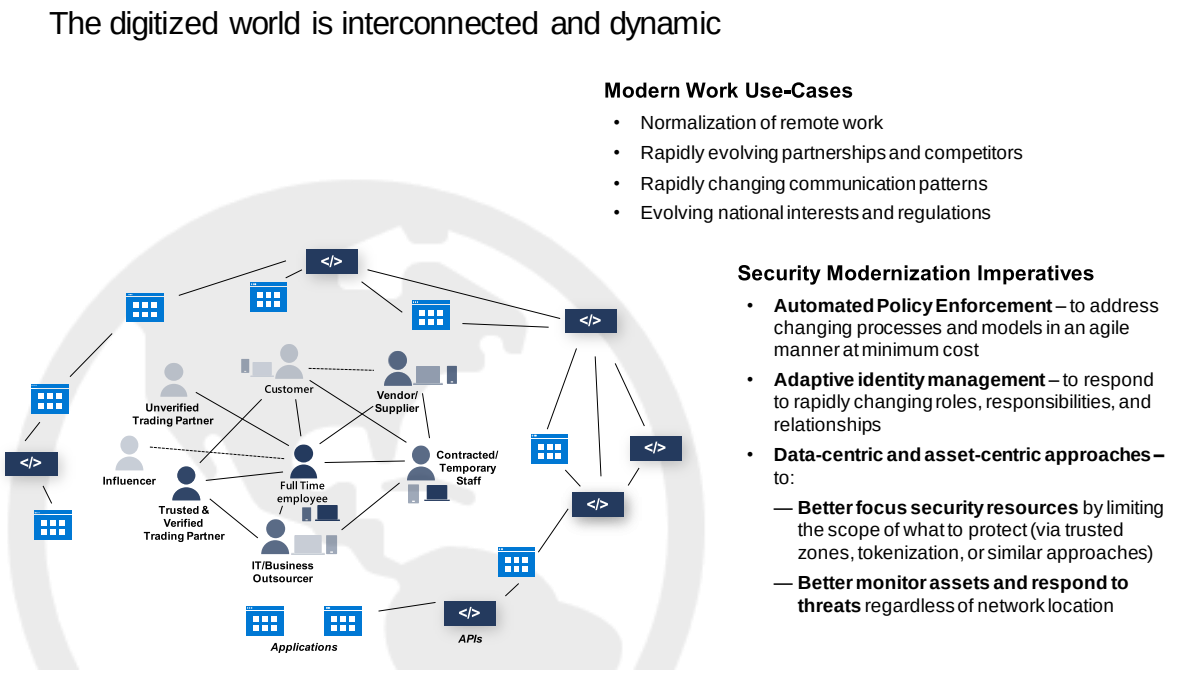

Figure 5: The Digitized World

From a security context, ZTAs enable adapting to the digitized world by simplifying interactions and making them scalable. A ZTA reduces the need for additional security solutions *by starting with an assumption of a compromised network environment*. *This proactive reduction in complexity* reduces security risk, by reducing what has to be protected, and letting resources be better focused on protecting high-value assets (the "crown jewels"). By doing this, operating costs can be managed, and threats can be responded to rapidly, in real-time/near real-time.

The needs of the digitized world are encapsulated in the capabilities that ZTAs must support, as described earlier in Figure 4.

Figure 6 illustrates what that ZTA might look like.

Zero Trust Core Principles

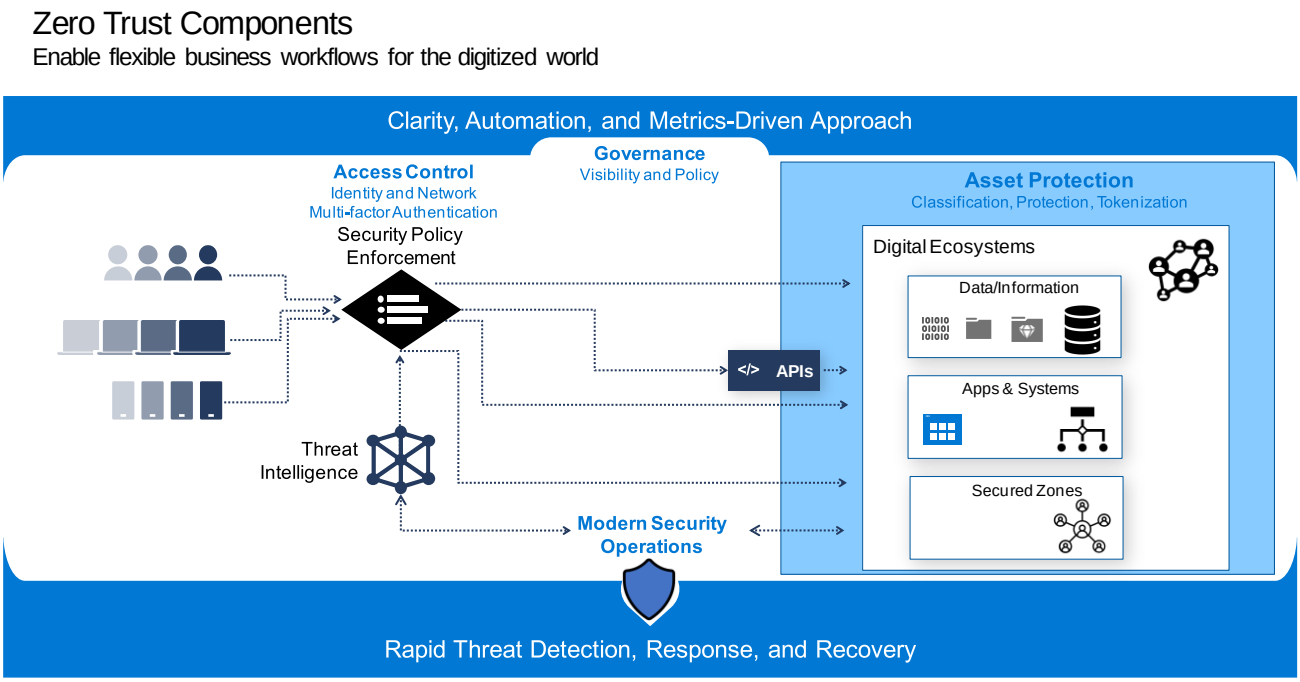

Figure 6: Zero Trust Components

In Figure 6, assets and data/information are grouped into Digital Ecosystems, which can be as granular as needed. Digital Ecosystems are environments either within an organization or across organizational boundaries, potentially involving multiple "partner" entities. Access to assets, data/information, and/or the Digital Ecosystems may be protected by access control at an API (service) level or directly at the asset or data/information. Access control is done through security policy enforcement and is policy-driven, enabling protection of assets and data/information using policies based on – but not limited to – business processes, data classification, asset or data/information (provider), and consumer (user). This allows dynamic and adaptive policy definition and enforcement, providing businesses with the ability to evolve in an agile manner.

Zero Trust identity models support federated identities, common in many organizations, especially in a world of loosely-coupled Digital Ecosystems, through subject (user)-centric digital identity models. Using adaptive policy-based access and tokenizing data using technologies such as format-preserving encryption reduce risk and the threat surface area; these also limit the friction that new technologies bring, in turn reducing the disruption of building new or re-architected platforms and systems. These approaches allow organizations to protect their high-value assets within highly protected, tiered secured zones.

Other key building blocks of Figure 6 are the support of automated audit, leading to agile compliance, and improved visibility and governance. This helps reduce/avoid long-running audits and compliance overhead. Incident management and threat management in a Zero Trust world are done through responsive and near real-time threat management and SOC components, which are tied in with incident management, closing the secure DevOps loop.

By creating secured zones to protect high-value assets, using tokenization to *reduce the threat surface area*, using adaptive, policy-driven access controls to define access control, and tokenizing data, the organization

can *limit incident blast radius*; in other words, the organization localizes the impact of an incident and improves situational awareness. Risk assessment and compliance are made more agile and responsive to evolving business need through automated compliance and audit. Finally, the agile threat management and SOC architectural building blocks enable early, proactive incident detection, response, and avoidance.

Many of these technologies and components exist at varying levels of maturity, though they are rapidly evolving to leverage new tooling and concepts, such as AI. There is a mindset shift, however, in the manner in which they are used to create an agile ZTA for organizations that *brings security to the users, data/information, applications, APIs, devices, networks, cloud, etc. wherever they are*.

Core Principles

When organizations undertake the journey towards a new, enterprise-wide change, a core set of principles[7] provides a succinct, easily shared "North Star" to guide and coalesce the organization.

This set of Core Principles acts as a set of fundamental guidelines for organizations to adopt Zero Trust and implement ZTAs. They focus on factors specific to Zero Trust – linking people, processes, and technology – and should both be used for all new security initiatives and retroactively applied to old security activities.

The Core Principles are grouped into common themes that address different aspects of Zero Trust:

- *Organizational Value and Risk Alignment* principles address key goals for business, IT, and security stakeholders to address overall strategic drivers
- *Guardrails and Governance* principles address compliance, risk, and information security stakeholders to guide the adoption of Zero Trust and ensure sustainability of assurances, addressing:
  - Rapidly evolving compliance and regulatory needs, requiring proactive integration of industry and organizational controls
  - Lagging industry controls and compliance standards, resulting in an expectation to create supplemental organizational controls
  - Increasing complexity and agility requirements that drive the need for rapid, near real-time or real-time audits, requiring automation of data collection, traceability, and processes
- *Technology* principles address the IT organization, information security, and risk and compliance stakeholders and determine technology decisions that underlie the development of a ZTA, including concerns associated with identity, access, and reduced threat surface area
- *Security Controls* principles address security and IT architects to ensure strong foundations of confidentiality, integrity, and availability assurances

All of the elements of the Core Principles must fit within the business strategy and organizational culture. Simple axioms are provided below to aid in communicating and remembering the principles. Guardrails and Governance help bind business goals and technical reality, and these principles are depicted to the side in Figure 7 as they should not impede direct connections between the organizational mission and the technology and security that support it.

[7] These core principles are deliberately not structured as architecture principles; a follow-up document will refine the core principles in this document.

Zero Trust Core Principles

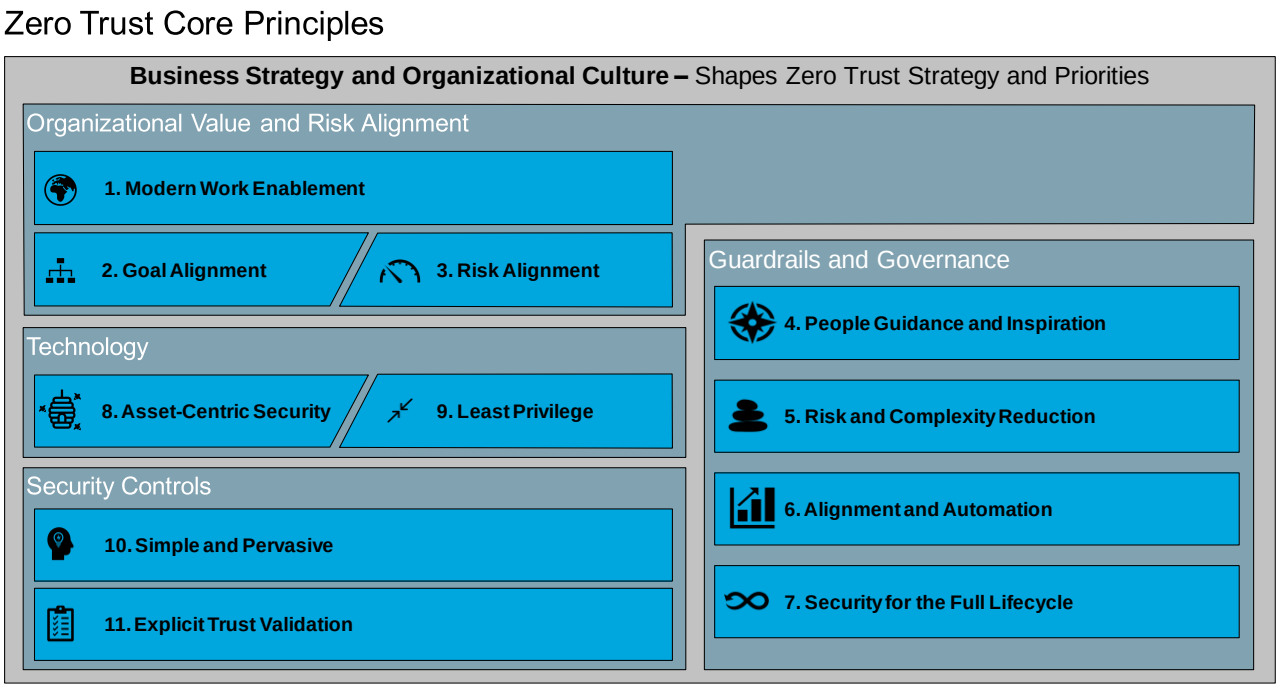

Figure 7: Summary of Zero Trust Core Principles

Organizational Value and Risk Alignment

1. **Modern Work Enablement** – Users[8] in organizational ecosystems must be able to work on any network in any location with the same security assurances, increasing productivity.
2. **Goal Alignment** – Security must align with and enable organization goals within risk tolerance and threshold.
3. **Risk Alignment** – Security risk must be managed and measured consistently using the organization's risk framework and considering organizational risk tolerance and thresholds.

Guardrails and Governance

4. **People Guidance and Inspiration** – Organizational governance frameworks must guide people, process, and technology decisions with clear ownership of decisions, policy, and aspirational visions.
5. **Risk and Complexity Reduction** – Governance must both reduce complexity (i.e., simplify) and reduce threat surface area.
6. **Alignment and Automation** – Policies and security success metrics must map directly to organizational

[8] Users include enterprise users, partners, and any other consumers including intelligent agents, humans, and IoT devices.

mission and risk requirements and should favor automated execution and reporting.

7. **Security for the Full Lifecycle** – Risk analysis and confidentiality, integrity, and availability assurances must be sustained for the lifetime of the data, transaction, or relationship. Asset sensitivity must be reduced where possible (removing sensitive/regulated data, privileges, etc.), and assurances should be provided for the risk of data in use, in-flight, and at rest.

Technology

8. **Asset-Centric Security** – Security must be as close to the assets as possible (i.e., data-centric and application-centric approaches instead of network-centric strategies) to provide a tailored approach that minimizes productivity disruption.
9. **Least Privilege** – Access to systems and data must be granted only as required and removed when no longer required.

Security Controls

10. **Simple and Pervasive** – Security mechanisms must be simple, scalable, and easy to implement and manage throughout the organizational ecosystem (whether internal or external).
11. **Explicit Trust Validation** – Assumptions of integrity and trust level must be explicitly validated against organization risk threshold and tolerance. Assets and/or data systems must be validated before being allowed to interact with anyone/anything else.

Information Security in the Digital Era

Prior sections established an overview of Zero Trust, its key drivers, and the digitally transformed information security world of the future.

This section reviews different aspects of Zero Trust for executives and senior leaders, focusing first on governance, and then Business, Security, and IT viewpoints, and concluding with the practical implications of implementing Zero Trust.

When coupled with prior sections, this section better equips executives and senior leaders to understand the evolving paradigm of Zero Trust and information security in the era of the Digital Enterprise.

Governance, Digital Transformation, and Zero Trust

Any security regime must include governance; otherwise, the policies are simply a set of suggestions. Governance in the context of Zero Trust incorporates business, risk, and technical (IT) perspectives, including CIO and CISO organizations, if those are separate. Governance must address the key characteristics of *velocity, complexity, and disruption*.

In a Zero Trust world, governance must operate in the context of a much higher level of uncertainty than in the past.

Governance must ensure that the implementation and operation of facilities and processes is aligned to the organizational view of risk, including risk tolerance and threshold, while continuing compliance and managing the introduction of new capabilities in a proactive manner.

In the Digital Age, the rapid rise in the number of interfaces and interactions driven by new technologies such as the cloud is coupled with the need for extreme agility. However, traditional audits of partners and interfaces and evolving regulatory requirements (which might often lag changes in the organization's environment) are generally not scalable or able to meet organizational needs for agility and operational efficiency.

To succeed, a Zero Trust governance model must manage or reduce complexity and the dynamic threat surface, allowing organizations to focus on the remaining, smaller threat surface. Zero Trust governance must also establish best practices and guardrails coupled with meeting existing controls, including fiduciary, regulatory, and business controls, and should *leverage but not depend on* existing controls and organizational risk assessment. A Zero Trust governance model must also provide the guardrails that enforce alignment with the Digital Enterprise priorities of proactive risk management, agility, and speed. Quantitative risk analysis frameworks, such as the Open FAIR™ Body of Knowledge (see References), provide a consistent way to measure, analyze, and discuss risk in a quantified manner, making them especially suited for Zero Trust.

Audit in the World of Zero Trust

Zero Trust requires regular, timely audits to ensure organizations are adequately managing risk. To do this, Zero Trust requires risk and security architecture traceability and the alignment of objectives and measurable results, from strategy to run-book processes. This necessitates a real-time (or near real-time) capability to

assess the security posture of an organization operating in an automated manner – audits extending over long periods of time are no longer actionable.

Dealing with Data and Breaches in the Zero Trust World

The asset which is compromised in case of a breach is data, and a Zero Trust premise is that the organization must be able to operate and grow in a compromised state. It is also reasonable to assume that laws and jurisprudence will lag the changing environment, but also that they will need to be complied with.

In such an environment, ensuring support for prevailing laws and compliance regimes and developing controls for addressing lagging standards become necessary. Security must be shifted as close to the asset (in this case, data) and governance and compliance automated as much as possible. Responses to breaches must be in near real-time. The overall amount of data being exposed must be reduced, thus reducing the loss magnitude and fallout of a breach. Data that must stay sensitive must be treated from a holistic, lifecycle, and access control perspective.

Privacy by Design and Zero Trust

Privacy as a concept and enforced paradigm is rapidly evolving. This rate of change is both jurisdictional and cultural. The disruptive and fiat nature of the manner in which these controls evolve and change leaves organizations very little time to adapt and results in huge expenditures. As a result, ZTAs must plan for "privacy by design" and embed it in all aspects of the architecture. This is inherently a cross-cutting[9] capability with a rapid rate of change and high complexity, so it must be incorporated in a manner *that is adaptive* and business, security, legal, and technology executives must be engaged in determining its implementation.

[9] Cross-cutting concerns are elements of an application or API that are used across multiple parts of the application or API. Examples would be security or logging.

The Business Executive's Perspective

From the perspective of the business executive, there are numerous drivers (as described in Figure 2) to consider, leading to the characteristics of Zero Trust: *velocity, complexity, and disruption*. This includes both the DevSecOps realm and the increasing and increasingly important connections between IT systems and operational technology, both within the organization and with business partners.

Given the profusion of security threats as well as security technologies, there is an increased challenge in measuring security risk and determining where there is Return on Security Investment (ROSI) among the myriad security controls in which investment might be made.

Collectively, these drivers all impact the thinking of business executives as it relates to traditional or legacy security architectures, and ZTAs. From the point of view of business executives, there is increasing interest in ensuring that the organization receives value in terms of reduced risk from security control investments. Additionally, the pace of change drives the need for a focus on ROSI in a timely manner, with a focus on business enablement and operational execution. In short, organizational stakeholders now tend to see investment in terms of the organization being able to support new business models or operate in a changed or evolving business environment. Investment for the sake of meeting compliance controls is no longer a sufficient cause for investment.

Enabling Business by Managing Risk

The goal of Zero Trust is to help business stakeholders manage security risk while enabling their objectives, including both creating new capabilities and supporting existing capabilities in an evolving, digitized environment. As such, any guidance offered in a Zero Trust strategy must align with a typical business-driven risk lifecycle approach. The outcome should be the identification of relevant threats and mitigations as well as a set of recommendations on how best to balance risk and business objectives (typically speed to market or cost).

Zero Trust approaches focus more on risk avoidance, providing a proactive approach to reduce risk wherever possible by bringing security to the users, information, applications, and APIs wherever they are; this contrasts directly with traditional, perimeter-based approaches that focus more on risk mitigation and responding/reacting to threats after they are identified or have occurred. In essence, Zero Trust implementations proactively reduce the amount of data/assets at risk which, in turn, reduces the effort, cost, and time required to maintain and protect data/assets.

People are more comfortable taking business risks when they feel safe – just as a car with better safety features provides assurances for the owner, ZTA enables an organization to move with greater speed and agility.

In some cases, an organization may not have the necessary Zero Trust competencies to enable business needs. It is the responsibility of technical and business leadership to determine how best to address this gap. It may involve hiring more people, training existing people, using a third party, or accepting the risk and insuring against it. As such, a Zero Trust security strategy must place the technical executive at the same table as business executives with discussion taking place in business terms.

Enabling Zero Trust Adoption and Digital Transformation

Digital Transformation requires agility, and organizations must be able to connect, disconnect, and interconnect many assets, both internal and external to the organization. Organizations are fundamentally changing their business models and entering new lines of business, and institutional knowledge garnered over operating in a particular line of business becomes less relevant or even irrelevant in the new business model, business domain, or technical environment. Organizations are also changing culture, processes, structure, and teams rapidly. In most cases, both business and technology teams are going through this evolution. Information security must adapt to this new environment.

Zero Trust provides a way to undergo Digital Transformation[10] securely and, therefore, must be embedded in the organization throughout the transformation process, which in turn implies that organizations proactively incorporate Zero Trust through the journey. The incremental and transformative nature of Zero Trust strategies requires an approach that supports the duality of operation and growth.

In an agile world centered on Digital Transformation, Zero Trust provides two fundamental advantages:

- It reduces the blast radius of an incident and facilitates situational awareness
- It reduces the threat surface area to better focus threat mitigation, based on asset and data-centric approaches

It does this through:

- Strategic business alignment by using capabilities to align security, the business, and technology
- Alignment of security to operational execution of the business and business processes
- Alignment of security and operating models to determine structural funding and operational decision rights, curating governance frameworks
- Mapping of business strategy and vision, through goals, principles, and policies to actionable security guardrails and governance

[10] The Open Group Guide: SOA for Business Technology (see References) can be leveraged to provide a framework for the development of modern Digital Organizations and executing Digital Transformation. This will be developed fully within the context of Zero Trust and ZTAs in a future publication of the Zero Trust Architecture Work Group.

Examples of Zero Trust in the Modern Digital Enterprise

To understand the impact and to concretely connect Zero Trust to typical Digital Transformation initiatives, we have provided some key use-cases (scenarios):

- Scenario 1: Normalization of Remote Work
- Scenario 2: Rapidly Evolving Partnerships and Ecosystems
- Scenario 3: Rapidly Changing Communication Patterns
- Scenario 4: Evolving National Interests and Regulations

Each scenario derives the capabilities of Zero Trust from the key drivers and requirements based on the context in the example scenario to illustrate the use of Core Principles while adopting Zero Trust.

Scenario 1: Normalization of Remote Work

Acme Banking Corp. is a traditional bank that has always primarily engaged with customers face-to-face. Acme Banking Corp. now faces a changed world and several key business drivers:

- *Rapidly changing technology* has allowed competitors to lure their customers away with online banking and peer-to-peer payments
- *Regulatory agencies* have instituted low interest rates, which are damaging the profitability of Acme Banking Corp.
- *The disruptive event* of the COVID-19 pandemic precipitated an unexpected massive *shift to remote work*, requiring Acme Banking Corp. to remotely service customers immediately

As a result of these drivers, Acme Banking Corp. identifies the new requirements it must meet to remain competitive and profitable:

- Acme Banking Corp. must *support remote work* for employees to work from home and use their own devices to do their job (including their banking staff interacting with clients in an online model)
- The *push to agility* requires migrating to a digital world with more online interactions and fewer physical banking centers
- *Managing increasing complexity* is required due to continuously evolving sales and client relationships (and applications) to keep up with competitors and customer preferences
- These changes, together, create a larger threat landscape that necessitates *real-time/near real-time* response and mitigation, particularly around employee access

How does Acme Banking Corp. meet these requirements and maintain security? In this scenario, traditional perimeter-based security models for networks do not work: they are slow to implement, expensive to operationally maintain, and difficult to adapt to rapidly changing business and technical environments. IT and the business need a self-service model to meet operational needs for agility and cost reduction. During this period of disruptive change, Acme Banking Corp. needs to continue operating the business while establishing

new capabilities to meet these needs. *Leadership needs a strategy to support operations and adapt and grow business models – all while maintaining adequate security – with timelines of weeks, not months.*

To accommodate these requirements, Acme Banking Corp. decides to adopt Zero Trust and implement a ZTA. This approach aligns security and technology to business needs and, with capabilities such as data-centricity and adaptive identity, reduces risk and complexity and supports agility. With the Zero Trust capabilities of quantified risk, secured zones, automated audit, and real-time/near real-time response, Acme Banking Corp. knows that not only will it be agile, but it will now also be able to trust that it is providing its customers and the organization with the security that is needed to grow and succeed.

With this vision in mind, as Acme Banking Corp. adopts Zero Trust, it can now:

- Respond to *rapidly evolving consumer needs* and business relationships, leveraging the Zero Trust capability of *adaptive identity*, primarily applying Core Principle 1: Modern Work Enablement
- Identify, respond to, and mitigate threats as they arrive – instead of afterwards – preventing losses from occurring and minimizing losses that do occur, by leveraging the Zero Trust capability of *real-time/near real-time response*, primarily applying Core Principle 2: Goal Alignment
- Report compliance to their regulators using the Zero Trust capabilities of quantitative risk through industry standard risk frameworks and automated audit, primarily applying Core Principle 3: Risk Alignment
- Maintain productivity by allowing employees to *work from home, using their own devices*, through the Zero Trust capability of *threat scope reduction and risk avoidance*, primarily applying Core Principle 5: Risk and Complexity Reduction
- Take a *holistic approach* and *reduce exposing data during its lifecycle* while protecting customers' PII, by leveraging the Zero Trust capability of *context-specific, policy-enforced data security*, primarily applying Core Principle 7: Security for the Full Lifecycle

As with any long-term change, there will be quick wins and incremental progress along the way, along with a significant change in organizational culture. Leaders of Acme Banking Corp. recognize this and proactively communicate why the change is needed and what is expected to help people manage expectations and rapidly plan for and execute on this new approach. Throughout this journey, Acme Banking Corp. plans to leverage Core Principle 9: Least Privilege as well as Core Principle 4: People Guidance and Inspiration to facilitate ease of adoption and cultural shifts.

Scenario 2: Rapidly Evolving Partnerships and Ecosystems

Acme Retail Corp. is a traditional retail company that relies on a large brick-and-mortar operation. However, Acme Retail Corp. now faces a changed world and several new business drivers:

- *Evolving business models* have shifted most retail business to online, and the majority of competitors operate both online and brick-and-mortar stores; this trend accelerated significantly during *the disruptive event* of the COVID-19 quarantine
- *Rapidly changing technology* has resulted in sales now being promoted through influencers and trading partners

- Transition to a complex, new ecosystem of suppliers, partners, and new sales channels, where *relationships are constantly and rapidly evolving*; today's competitor might be tomorrow's partner and the day after's vendor

To adapt to this new digital world, Acme Retail Corp. decides to adopt a digital-first business model and shift its business operations online. It also decides to private label some of its capabilities and engage online third-party sellers. The evolving business environment and new business models necessitate new supply chains and marketing and sales channels, resulting in a proliferation of suppliers and marketing and sales partners – effectively a new business ecosystem, often in flux and continuously evolving.

During this transition, Acme Retail Corp. must be able to continue operations while evolving new capabilities and adopting new business models. Acme Retail Corp.'s Digital Transformation results in new requirements:

- Acme Retail Corp. must *rapidly become more agile* and allow roles and the business ecosystem to evolve rapidly as it undergoes this urgent Digital Transformation
- Influencers, new, smaller vendors, and third-party sales channels have varying levels of security capability, requiring *real-time/near real-time response to new and evolving threats*
- As *complexity increases from the new business model and organizational ecosystem*, Acme Retail Corp. must allow organizations to evolve and in fact have one or more of the relationships concurrently, allowing for proliferation of communication channels

How does Acme Retail Corp. meet these requirements and maintain security? In the new digital environment, traditional identity models and complex federated identity systems no longer work. To easily execute and operate new and evolving relationships, Acme Retail Corp. must develop an agile security strategy that rapidly and easily identifies risks and mitigations. *Long timelines from complex security processes are no longer an option that Acme Retail Corp. can afford – agility, timeliness, self-service, and operational efficiency all define success.*

To rapidly adapt to these changes while providing appropriate security measures, Acme Retail Corp. decides to adopt a Zero Trust approach and implement a ZTA. Acme Retail Corp. can now leverage Zero Trust capabilities to:

- Fluidly establish and change relationships by leveraging the Zero Trust capability of *threat scope reduction and risk avoidance*

  By utilizing rapid, trustworthy risk assessments that can be easily conducted and are attestable and quantifiable, Acme Retail Corp. can establish new relationships and business models. Acme Retail Corp. achieves this by quantitatively analyzing risk within the context of organizational risk appetite by adopting a quantitative risk analysis framework such as the Open FAIR Body of Knowledge, primarily applying Core Principle 3: Risk Alignment.

- Enable faster interface creation, audit, and partner relationship establishment by leveraging the Zero Trust capability of *context-specific, policy-enforced data security*

  It achieves this by using a *simple* data classification system, coupled with data tokenization to reduce the volume of sensitive data, and encryption to protect the remaining sensitive data, primarily applying Core Principle 5: Risk and Complexity Reduction.

- Easily meet compliance and governance requirements by leveraging the Zero Trust capability of *automated audit* to allow continuous compliance and monitoring in real time

  Acme Retail Corp. achieves this by the real-time capture and quantification of logs for new cloud services and applications for online shopping, primarily applying Core Principle 6: Alignment and Automation.

- Support rapidly changing roles and access controls by leveraging the Zero Trust capabilities of *adaptive identity management* and *policy-driven access controls*, primarily applying Core Principle 7: Security for the Full Lifecycle

- Enable proactive real-time/near real-time threat detection, alert notification, incident management, and recovery by leveraging the Zero Trust capability of *real-time/near real-time response*

  Acme Retail Corp. achieves this by setting up a new cloud-based security analytics infrastructure that integrates threat intelligence and automated threat response and by establishing a modern SOC that prioritizes events and alerts based on asset sensitivity, which allows for further *threat scope reduction and risk avoidance*, primarily applying Core Principle 8: Asset-Centric Security.

As Acme Retail Corp. moves forward with its Digital Transformation, its adoption of a Zero Trust approach allows Acme Retail Corp. to now prioritize its assets and the protection of them within its risk appetite. It is now empowered to enter new business domains and pivot as needed without concern for security slowing them down or being ignored as a source of business risk.

Scenario 3: Rapidly Changing Communication Patterns

Acme Healthcare Corp. is a healthcare organization that operates many hospitals. Acme Healthcare Corp. has a diverse enterprise estate that includes many legacy applications and devices that protect the lives and health of their patients, but also faces a changed world and powerful new business drivers:

- Organizations of all types are migrating to the cloud due to the rapidly evolving business ecosystem that is driven by *rapidly changing technologies*, evolving regulations, and business models

- The *disruptive event* of the COVID-19 pandemic has driven a push towards telemedicine, further causing new platforms to be moved to the cloud

  The pandemic has also precipitated the need for rapid integration of new clients, staff, and partners: providers and out-of-state hospital systems become engaged, and governmental agencies need access. The new HR system is SaaS-based.

Acme Healthcare Corp. must now share data across an ecosystem composed of its legacy, on-premise systems, a hybrid cloud environment involving multiple cloud vendors, and, due to the industry-wide adoption of cloud technologies, a heavily API-centric architecture. New partners, vendors, and cloud-based, API-based vendor solutions increase the interactions by orders of magnitude. *In practice, this means multiple teams with extensive interdependencies are accompanied by a proliferation of interfaces and their interdependencies as well as a rapid increase in communication channels.* New business capabilities involve the orchestration or composition of data, often from many diverse sources. This, in turn, leads to interactions involving different and ever-evolving communication patterns: synchronous (real-time), asynchronous, event-driven, file/batch-based, streaming, etc.

Zero Trust Core Principles

As a result of these drivers, Acme Healthcare Corp. identifies new requirements it must meet to remain competitive and profitable:

- Acme Healthcare Corp. must *handle exponentially increasing complexity*

  Addressing each interface/pattern individually with the same level of due diligence would be impossible. It would slow down the business and put the organization at risk. There are too many dependencies: different teams working on different APIs work with different priorities and speed, and testing these interfaces and dealing with continuous change make the task next to impossible.

- *Unpredictability and disruptive events* must be supported in all circumstances; if not, patient mortality will increase

How does Acme Healthcare Corp. meet these requirements and maintain security? Traditional approaches of interface-by-interface risk assessment, reviews, encryption, etc., are not feasible. Dependencies limit the value of encrypting each interface – even if it is possible. The growing complexity and dependencies make traditional approaches unfeasible. Who a consumer might be can no longer be predicted well in advance, and the supporting approach must plan for that aspect. During this period of disruptive change, Acme Healthcare Corp. needs to continue operating the business while establishing new capabilities to meet these needs. *Leadership needs a strategy to support operations and adapt and grow business models, all while maintaining adequate security, with timelines of weeks, not months.*

To accommodate these requirements, Acme Healthcare Corp. adopts Zero Trust and implements a ZTA. Adopting Zero Trust will enable Acme Healthcare Corp. to add new members in the ecosystem and send data seamlessly with minimal friction, unhindered by communication channel or pattern. Adopting Zero Trust means Acme Healthcare Corp. can now:

- Reduce the number of at-risk interfaces carrying high-risk data, thereby significantly reducing complexity, increasing agility, and enabling the easy exchange of data between interfaces

  Acme Healthcare Corp. achieves this by leveraging the Zero Trust capabilities of threat scope reduction and risk avoidance and data-centricity (as opposed to network-centricity) and using approaches such as tokenization and format preserving encryption, primarily applying Core Principle 8: Asset-Centric Security.

- Improve the user experience and *reduce threat scope and avoid risk* from interfaces by leveraging the Zero Trust capabilities of publishing legacy apps through modern secure methods, *secured trusted zones*, and software-defined networks to protect the remaining interfaces and applications that need high-risk data, primarily applying Core Principle 10: Simple and Pervasive

- Address the rapidly evolving environment and changing ecosystem of partners and employees as well as greatly reduce complexity and improve operational efficiency by ensuring that applications and APIs are built without prior expectations of who the client is (Zero Trust) by decoupling security policy assertions from the application or API

  Acme Healthcare Corp. achieves this by leveraging the Zero Trust capabilities of *separation of concerns*,

adaptive identity management, and policy-driven access control, primarily applying Core Principle 11: Explicit Trust Validation

These actions allow Acme Healthcare Corp. to minimize its risks and add new capabilities, like shared patient history across multiple providers that improve its Stars and HEDIS ratings.[11] New partners, movement to a digital world, and an ability to easily add new business capabilities becomes possible as Zero Trust provides the security that Acme Healthcare Corp. needs for its Digital Transformation journey.

Scenario 4: Evolving National Interests and Regulations

Acme Manufacturing Corp. is a multi-national organization that has supply chains and sales in six different countries – three in the EU, one in Singapore, one in the US, and one in China. These countries have different sets of regulatory controls:

- China requires full governmental access to sensitive data (such as PII, including employee names and date of birth), with no traditional security controls such as encryption
- Singapore has a much higher level of government access to personal data
- The three European countries require strong, individual-centric controls, such as GDPR
- The US follows controls, such as CCPA, with similar individual-centric controls

As a result, Acme Manufacturing Corp. primarily faces the following driver:

- Regulatory requirements differ vastly and are rapidly evolving but lagging

  Acme Manufacturing Corp. must be able to adapt to this rapidly evolving environment and be able to grow and operate while maintaining compliance across the geopolitical regions.

To remain profitable, Acme Manufacturing Corp. decides to adopt a Zero Trust approach and implement a ZTA with the following requirements:

- With applications distributed across multiple countries and platforms, Acme Manufacturing Corp. must be able to *handle a rapidly evolving and increasingly complex* computing environment
- As events in the world continue to develop, Acme Manufacturing Corp. must be able to rapidly adapt to and *meet new and lagging regulatory requirements* throughout the geopolitical regions in which it operates

How does Acme Manufacturing Corp. meet these requirements and maintain security? In this scenario, traditional network-centric approaches no longer work. In some cases, a VPN is no longer an option. Safe Harbor laws[12] no longer apply. To adapt to this rapidly evolving environment, Acme Manufacturing Corp. needs to follow new, non-traditional approaches. *Leadership needs a strategy to support operations and*

[11] Health Star Rating System; see https://en.wikipedia.org/wiki/Health_Star_Rating_System and Healthcare Effectiveness Data and Information Set; see https://en.wikipedia.org/wiki/Healthcare_Effectiveness_Data_and_Information_Set.

[12] See https://en.wikipedia.org/wiki/Safe_harbor_(law).

adapt and grow business models while maintaining adequate security, with accelerated and often unpredictable timelines and regulatory controls.

To meet these new requirements, Acme Manufacturing Corp. decides to adopt a Zero Trust approach and implement a ZTA. This approach allows Acme Manufacturing Corp. to move forward with reduced impact and leverage the Zero Trust goals of enablement and operation in an unpredictable environment. This means Acme Manufacturing Corp. can now:

- Easily meet compliance and governance requirements by leveraging the Zero Trust capability of *automated audit* to allow continuous compliance and monitoring in real time

  Acme Manufacturing Corp. achieves this by the real-time capture and quantification of logs, primarily applying Core Principle 6: Alignment and Automation.

- Reduce the number of at-risk interfaces carrying high-risk data, thereby significantly reducing complexity, increasing agility, and enabling the easy exchange of data between interfaces

  Acme Manufacturing Corp. achieves this by leveraging the Zero Trust capabilities of *threat scope reduction and risk avoidance* and *data-centricity* (as opposed to network-centricity) and using approaches such as tokenization and format preserving encryption, primarily applying Core Principle 8: Asset-Centric Security.

- Secure high-value systems adaptively support changing conditions, and meet compliance needs by leveraging the Zero Trust capabilities of *secured zones, policy-driven access control, separation of concerns* (enabling an API-driven, decoupled privacy by design approach), and *context-specific, policy-enforced data security*, primarily applying Core Principle 7: Security for the Full Lifecycle and Core Principle 10: Simple and Pervasive

As a result, Acme Manufacturing Corp. can now pivot as needed, leveraging Zero Trust as an enabler, both to expand and grow its multi-national footprint and to reduce the friction that it would otherwise face in this changing environment.

Conclusion and Future Directions

Zero Trust builds on groundwork laid by the work of the Jericho Forum and provides a foundation for a modern information security paradigm to meet the needs of organizations in this Digital Age, as they undergo Digital Transformation and operate in a digital environment. This document acts as an introduction to Zero Trust, its drivers, and foundational (Core) Principles.

The Open Group Zero Trust Architecture Work Group will build on these Core Principles to develop additional documents and guidance, including a Reference Model and Architecture, a Zero Trust Practitioner's Guide, and a Zero Trust Business Guide as well as to consider the intersection of IT systems and operational technology.

References

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

- Digital Practitioner Body of Knowledge™ Standard, The Open Group Standard (C196), published by The Open Group, January 2020; refer to: www.opengroup.org/library/c196

  This document is the Digital Practitioner Body of Knowledge™ Standard, a standard of The Open Group, also known as the DPBoK™ Standard. It has been developed by The Open Group Digital Practitioners Work Group (DPWG). This document is intended to assist individuals and organizations who wish to create and manage product offerings with an increasing digital component, or lead their organization through Digital Transformation. It provides guidance for the Digital Practitioner, whether based in a traditional "IT" organization, manufacturing unit, sales, customer support, or embedded in a cutting-edge integrated product team.

- How Competitive Forces Shape Strategy, Michael E. Porter, March 1979, published by Harvard Business Review; refer to: https://hbr.org/1979/03/how-competitive-forces-shape-strategy

- Jericho Forum® Commandments, The Open Group White Paper (W124), published by The Open Group, May 2007; refer to: www.opengroup.org/library/w124

  The Jericho Forum Commandments define the design principles that must be observed when architecting systems for secure operation in de-perimeterized environments. These design principles are grouped within convenient information security areas. The Commandments specifically address those areas and issues of security design principles that are necessary to assure secure de-perimeterized IT operations; they do not include foundation security principles which apply in all IT environments. These Commandments not only provide essential guidance to system architects and designers, but also serve as a benchmark by which the effectiveness of IT security design concepts, solutions, standards, and system architectures can be assessed and measured.

- Jericho Forum® Identity Commandments, The Open Group White Paper (W125), published by The Open Group, May 2011; refer to: www.opengroup.org/library/w125

  The Jericho Forum Identity Commandments define key design principles that need to be observed when planning an identity ecosystem designed to operate on a global, de-perimeterized scale. They build on the design principles defined in the Jericho Forum Commandments.

- The Need for Data Principles, The Open Group White Paper (W143), published by The Open Group, January 2014; refer to: www.opengroup.org/library/w143

  This White Paper explains why our IT industry needs to establish a set of high-quality data principles, and lists a draft base set of Data Principles (in the same vein as the 2007 Jericho Forum Commandments and the 2011 Identity Commandments) as a sound basis for future work to develop them. It acknowledges and outlines key issues that remain to be fully worked through to develop a comprehensive and resilient set of Data Principles, and shares recommended directions on how to develop Data Principles that will stand the test of time as guidance to data management solution developers and also to the customer community needing to assess how effectively data management solutions will satisfy their business needs.

Zero Trust Core Principles

- Trust Ecosystems Guide, The Open Group Guide (G141), published by The Open Group, January 2014; refer to: www.opengroup.org/library/g141

  A trust ecosystem enables emerging data-centric protection features and capabilities – in particular Smart Data (see The Open Group White Paper: Smart Data for Secure Business Collaboration, January 2014 at www.opengroup.org/library/w140) to operate to their optimum potential. The Jericho Forum Commandments, Commandment #8 states that in any environment, secure data is data that remains protected to the required level when outside an entity owner's direct locus of control, and Commandment #9 states that access to data should be controlled by security attributes of the data itself; i.e., data-centric security. In today's cloud computing and other globally distributed environments, we can no longer know where our data might be located or in whose hands it may rest. Operating in a trust ecosystem maintains optimum protection over the data, thereby maintaining its business value as usable as intended but protected from misuse.

- Open FAIR™ Body of Knowledge:

  — Open Risk Analysis (O-RA) Standard, Version 2.0, The Open Group Standard (C20A), published by The Open Group November 2020; refer to: www.opengroup.org/library/c20a

  This document provides a set of standards for various aspects of information security risk analysis. It was first published in October 2013, and has been revised as a result of feedback from practitioners using the standard and continued development of the Open FAIR taxonomy.

  — Open Risk Taxonomy (O-RT) Standard, Version 3.0, The Open Group Standard (C20B), published by The Open Group November 2020; refer to: www.opengroup.org/library/c20b

  This document defines a taxonomy for the factors that drive information security risk. It was first published in January 2009, and has been revised as a result of feedback from practitioners using the standard and continued development of the Open FAIR taxonomy.

- SOA for Business Technology, The Open Group Guide (G202), published by The Open Group, February 2020; refer to: www.opengroup.org/library/g202

  This document provides best practices and lessons learned to guide the shift of organizations towards a service-oriented way of doing business and improve the successful implementation of business solutions using Service-Oriented Architecture (SOA). The objective is to provide a reference and process model, accompanied by guidance on their use and an illustrative use-case, for evolution to a service-oriented business – a Service-Oriented Enterprise (SOE) – and the associated enabling technical SOA.

Acronyms & Abbreviations

AI	Artificial Intelligence
API	Application Program Interface
BYOX	Bring Your Own X
CCPA	California Consumer Privacy Act
DPWG	Digital Practitioners Work Group
GDPR	General Data Protection Regulation
GRC	Governance, Risk, and Compliance
IoT	Internet of Things
ML	Machine Learning
NLP	Natural Language Processing
O-RA	Open Risk Analysis
O-RT	Open Risk Taxonomy
PCI	Payment Card Industry
PII	Personally Identifiable Information
ROSI	Return on Security Investment
RPA	Robotic Process Automation
SaaS	Software as a Service
SOA	Service-Oriented Architecture
SOC	Security Operations Center
SOE	Service-Oriented Enterprise
ZTA	Zero Trust Architecture

About the Authors

Tuhinshubhra Ghosh, Technology Consultant, DXC Technology

Tuhinshubhra (Tuhin) Ghosh is a Technology Consultant at DXC Technology. Tuhin specifically works as an IoT SME with DXC technology. His responsibilities include leading the development team and providing expertise in specific areas, such as IoT security, data access policies, issue and risk management, audit readiness, and compliance.

Nikhil Kumar, President, Applied Technology Solutions

Nikhil Kumar is the President and Founder of Applied Technology Solutions, Inc. (ApTSi™); he is also a Co-Lead of The Open Group Zero Trust Architecture Work Group, which is a collaboration between The Open Group Security Forum and Architecture Forum. Nikhil is an accomplished industry Digital Transformation and security thought leader. He has led the vision, design, and implementation of solutions covering all aspects of Zero Trust and has been pioneering its vision, including teaching one of the first classes on Zero Trust at university level. In the industry, working from a C-suite and board level to a practitioner level, Nikhil has led the successful vision, design, and implementation of Zero Trust capabilities, with a holistic perspective. This includes technology aspects such as secure trusted zones, tokenization (format preserving encryption), automated audit and multiple authentication/authorization initiatives, process aspects covering risk and compliance regimes and organizational governance, and people aspects, including training, workshops, and setting up Communities of Practices, and adoption from Fortune 50 companies to startups. Nikhil has worked across a diverse set of industries, including finance, healthcare, ed-tech, manufacturing, hospitality, and the utility industry.

Sai Mohan Sakuru, Principal Consultant, Wipro

Sai Mohan Sakuru is the Principal Consultant at Wipro, where he drives the overall cybersecurity portfolio. Sai is a cybersecurity evangelist and a security leader based in the UK. He has vast experience in leading Digital & Process Transformations in IT Infrastructure, Cloud, Process, and Information Security certifications such as ISO 20000, ISO 27001, PCI-DSS, SSAE 16, ISO 22301 deployments for Banking, Financial Services, and Insurance (BFSI), Media, Retail, and Telecom. He previously held roles such as Information Technology Risk & Compliance officer for a media giant in continental Europe. Sai provides thought leadership to clients on risk management, Business Continuity Planning (BCP) and Disaster Recovery (DR), PCI-DSS, data center cyber technology transformations, and cyber resilience strategy, and he advises Fortune 100 clients and works with CISOs, CIOs, and Directors on cyber transformation strategy and initiatives. He is currently working on XDR, Security Intelligence & Analytics, SOAR, Risk Quantification, CCM, and Deception & Zero Trust initiatives.

Patrick Shirazi, Managing Enterprise Architect, Capgemini

Patrick Shirazi is Managing Enterprise Architect at Capgemini. As a security architect, Patrick considers the vital role of endpoint protection in IT solutions. Believing in security by design, Patrick is keen on designing security solutions that utilize the concept of Zero Trust Architecture. Patrick also collaborates with architecture work groups and tries to tailor and apply those standards to real-world problems.

Zero Trust Core Principles

Mark Simos, Lead Cybersecurity Architect, Microsoft

Mark Simos is the Lead Cybersecurity Architect at Microsoft, where he leads the development of cybersecurity best practices and guidance including Zero Trust reference architectures, rapid modernization plans, and similar guidance for Security Operations Centers (SOCs) and related topics. Mark is a passionate advocate for modernizing security practices and technologies using Zero Trust principles. He focuses on helping organizations meet both their cybersecurity and Digital Transformation goals by combining lessons learned from customer cybersecurity incident investigations and experience at Microsoft in operating and protecting hyper-scale cloud services.

Altaz Valani, Director of Insights Research, Security Compass

Altaz Valani is Director of Insights Research at Security Compass; he is also Vice-Chair of The Open Group Security Forum and a Co-Lead of the Zero Trust Architecture Work Group, which is a collaboration between The Open Group Security Forum and Architecture Forum. Altaz sits on several standards working groups, similar to the Zero Trust Architecture Work Group, where security plays a prominent role. He is also a frequent industry collaborator on the topic of balancing business enablement and security risk which are closely tied to the Zero Trust Core Principles described in this document. Altaz is an advocate and evangelist for enabling business priorities and strategies through security.

Anthony Carrato, The Open Group Invited Expert

Anthony (Tony) Carrato is an Invited Expert in The Open Group Security Forum. Prior to retiring from IBM, Tony worked with a number of big data and analytical products and projects, including delivering some of the first big data solutions into production use. Tony is a long-time participant in The Open Group and the Security Forum, where he has been a member of the Steering Committee for several years. He is certified at Level 3 as an IT Architect, through The Open Group and IBM. Tony's involvement in cybersecurity goes back over 20 years.

Stephen Whitlock, The Open Group Invited Expert

Stephen (Steve) Whitlock is an Invited Expert in The Open Group Security Forum. Steve is a retired cybersecurity professional who continues as a volunteer supporting both the US Government and The Open Group. Steve has helped develop international security standards, working with government organizations such as NIST in the US, the European Commission, and the Organisation for Economic Co-operation and Development (OECD), and standards organizations such as the IETF, OASIS, The Open Group, and others. For many years he served on the Jericho Forum Board of Management.

Jim Hietala, VP Business Development & Security, The Open Group

Jim Hietala is Vice-President, Business Development and Security for The Open Group, where he manages the business team, as well as Security and Risk Management programs and standards activities.

Zero Trust Core Principles

John Linford, Security & OTTF Forum Director, The Open Group

John Linford is the Forum Director of The Open Group Security Forum and Open Trusted Technology Forum. John is Open FAIR™ Certified and was the lead author of The Open Group Open FAIR™ Risk Analysis Process Guide (January 2018, www.opengroup.org/library/g180), which describes best practices for applying the Open FAIR risk analysis methodology. John is responsible for enabling the Work Group members to execute their work plan using the available processes and tools in accordance with The Open Group Standards Process.

Andras Szakal, VP & Chief Technology Officer, The Open Group

Andras is Vice-President and Chief Technology Officer for The Open Group. Andras is a recognized expert on Supply Chain Security, Cloud Architecture, and Cybersecurity. He is widely recognized as the driving force behind ISO/IEC 20243, better known as the Open Trusted Technology Provider™ Standard (O-TTPS), and his tireless work to establish recognized professional credentials for technology professionals through the creation of the Open Professions Framework. He holds professional certifications in security (CSSLP), solutions architecture (The Open Group Distinguished Certified Architect (Open CA, Level 3)), and supply chain security (Master Trusted Technology Practitioner (Open CTTP, Level 2)). His experience spans over 30 years of research, telecommunications, global standards contributions, and public sector executive leadership.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 800 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.