Communicating the Business Value of Zero Trust

Release Candidate

cloud security alliance®

This is a Release Candidate version and is subject to change.

Acknowledgements

The CSA Zero Trust 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 (ZT) 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.

Lead Author(s)

Jason Garbis
Alex Sharpe

Contributors

Elier Cruz
Josh Woodruff
Saif Azwar
Rohini Sulatycki
Erik Johnson
Jonathan Flack
Christopher Steffen
Joseph Roblee
Megha Kalsi
Andrea Knoblauch
Nelson Spessard Jr
Lars Ruddigkeit
Dr. Ron Martin
Heverin Joy Williams
Rajesh Murthy
Don O'Neil
Akin Isinkaye

Reviewers

Michael Roza
Osama Salah

CSA Staff

Erik Johnson

Table of Contents

Abstract

Zero Trust is a major industry trend that is being adopted and promoted by security teams within many organizations around the globe, and for good reasons; it delivers improved security and can also reduce cost and improve business efficiency and agility. However, Zero Trust is also an industry buzzword that can be confusing and is often misunderstood. Business leaders and non-security professionals are key stakeholders, budget holders, and gatekeepers in any organization's journey to Zero Trust that can make the difference between successful and failed Zero Trust initiatives. This is because adopting Zero Trust as an organizational strategy fundamentally requires change, support, and investment of significant time, effort, and money across the enterprise. Therefore, security teams need to be able to communicate the concept and value of Zero Trust to non-technical or non-security audiences, all the way up to the Board of Directors. We believe that the Information Security (InfoSec) industry has not sufficiently enabled security practitioners to clearly, succinctly, and directly communicate the *business value* that a Zero Trust strategy can bring. The goal of this CSA guidance is to fill that gap.

Target Audience

The primary audience for this document is InfoSec professionals and practitioners who are looking to present the value and business impact of adopting Zero Trust to business leaders and key stakeholders within their organization.

The secondary audience is non-technical, non-security stakeholders within an organization. This whitepaper contains some technical concepts, but is intended to be understood by a non-technical audience.

Objectives

This document seeks to provide InfoSec professionals with the knowledge and mindset to effectively communicate and present **why** their organization should invest in implementing a Zero Trust security strategy. These communications are intended to be presented to internal stakeholders: people in roles such as non security-focused IT and enterprise architects, finance and budgeting teams, line of business managers, application owners, members of the C-Suite executives, (e.g., CEO, COO, CFO) and board members.

This whitepaper aims to enable security professionals to present the value and business impact[1] of adopting Zero Trust to business leaders and key stakeholders within their organization and subsequently, to convince their organization of the urgency for and need to invest in a Zero Trust initiative.

1. What is Zero Trust?

Zero Trust is a cybersecurity strategy based on a few core principles which, while simple, can have a significantly beneficial impact on organizations' architectures, approaches, and operations. The United States' NSTAC Report to the President on Zero Trust and Trusted Identity Management, states that "Zero Trust is 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, a user 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."

According to the Zero Trust Architecture (SP 800-207) document published by the United States National Institute of Standards and Technology (NIST):

> "Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established."

That NIST document also states that Zero Trust "is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level." It also includes seven core tenets of Zero Trust, included here for reference:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioral and environmental attributes.

[1] Some international efforts use the term "consequences." ISO 31000, Risk management – Guidelines is an example.

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications, and uses it to improve its security posture.

Overall, Zero Trust is a sharp contrast to traditional, trust-based "castle and moat" physical network perimeter security architectures, which are ineffective in the current era of cloud computing, remote workforces, and a heightened threat landscape.

Sophisticated threat actors are increasingly adept at exploiting exposed technical or human vulnerabilities in our modern, highly distributed enterprise networks, which often heavily leverage Internet connectivity. Successful cyberattacks generally exploit trust in some manner. This makes "trust," whether implicit or explicit, a dangerous vulnerability that must be mitigated. With Zero Trust, all network packets are untrusted and treated identically with every other packet flowing through the system. The trust level is defined as essentially zero, hence the term Zero Trust. Note that this approach is centered on removing trust from digital systems, not from people, relationships, or cultures.

Zero Trust is a holistic cybersecurity strategy that encompasses cloud/multi-cloud, internal and external partner/stakeholder user (organizational and BYOD) endpoints, on-prem and hybrid systems, and includes IT, OT, and IoT. Zero Trust is not a product (although Zero Trust-based security infrastructures can be implemented utilizing many different products), nor does Zero Trust require organizations to rip and replace existing security infrastructure. Zero Trust drives an architectural approach to information security that aligns resources and controls to facilitate least-privilege access, ensuring that every network packet is treated as untrusted, and that the system enforces a default-deny model across the layers of the stack.

The Zero Trust approach is a conscious and deliberate strategy that drives the organization's selection and deployment of technology infrastructure across the domains of identity, device, network, application, and data, as securely as possible. The conscious decision to embrace Zero Trust reflects a recognition of the evolving threat landscape and the need for a more robust and resilient security posture, and in taking a risk-based approach to authorizing access. Implementing Zero Trust involves dynamic context, stringent access controls, continuous verification, monitoring activity, and strict enforcement of security policies.

By consciously adopting the Zero Trust approach, organizations aim to minimize the risk of data breaches and unauthorized access by assuming a more cautious and skeptical stance towards network traffic, and activities performed by both human users and non-person identities.

Zero Trust is in the early stages of being widely adopted by enterprises, and is a mandatory part of the new U.S. Federal Government's cybersecurity strategy. As such, we anticipate continued interest in, and need for, guidance on how to successfully adopt Zero Trust within organizations.

2. Misconceptions About Zero Trust

Zero Trust is a strategy, not something you just buy and configure, or develop and implement. As a strategy, it can and should inform your thinking, decision-making, prioritization, and measurement of IT and security projects. Adopting this strategy means that your organization's architecture will be updated and evolve into a Zero Trust architecture. Approached properly, *Zero Trust drives your selection and deployment of technology infrastructure*, across the domains of identity, device, network, application and data, and the cross-cutting areas of visibility and analytics, automation and orchestration, and governance.

Zero Trust is not a silver bullet for preventing data breaches. While most breaches involve thousands of data records, breaches that result in the loss of millions of records incur exponentially higher costs. Vigilance and careful governance are essential to effectively reduce the risks associated with:

- phishing
- business email compromise
- vulnerabilities in third-party software
- stolen or compromised credentials
- malicious insiders
- cloud misconfiguration
- social engineering
- physical security compromise
- accidental data loss
- lost devices

These are the major sources of data breaches that must be addressed when implementing Zero Trust.

Zero Trust is also much more than just technology. There are a huge number of security technologies on the market, addressing specific threats within a defined context. Zero Trust is more about people and process than technology, although technology still plays a role. What is required is a concerted effort to connect these elements to deliver more comprehensive security, through automated policies.

Zero Trust does not have to be difficult, but it does require security and technology teams to establish partnerships with business stakeholders (which is largely the focus of this document). This can represent a culture shift within organizations. It may feel uncomfortable, but when this partnership is established, Zero Trust becomes much simpler and more effective.

3. Guiding Principles for Communicating Business Value

The Guiding Principles document developed by the CSA Zero Trust Working Group includes several principles that can aid in understanding and communicating the business value of Zero Trust.

Beginning with the End in Mind: This encourages one to establish a clear vision of the organization's desired direction and destination at the outset of the Zero Trust journey. Desired outcomes relevant to business value include reducing the cost of compliance, the financial impact of incidents, the complexity of IT and process debt, residual risk, and Total Cost of Ownership (TCO).

Breaches Happen. Acknowledging this fact allows for a shift in mindset from the impossible goal of being 100% secure, to the more achievable goal of instead being resilient. This shift results in three benefits:

- Limiting the blast radius of affected devices when a breach occurs
- Reducing a hacker's ability to perform reconnaissance and move laterally across the enterprise
- Reducing the impact by limiting what assets can be damaged or stolen by a single event

Risk Management: This plays an important role in Zero Trust. Understanding the organization's risk appetite provides a threshold for acceptable risk. The Zero Trust goals listed above aid in reducing Inherent Risk to acceptable levels by implementing controls that reduce Likelihood, Impact, or both. This can help make the organization more resilient and increase agility.

Using risk-based prioritization allows an organization to understand and identify the gaps they must address. The organization can then make an informed decision about where to start – typically it makes sense to start small and focus on quick wins that will begin to bolster their security posture and build momentum for the Zero Trust initiative. Obtaining and maintaining buy-in from leadership is easier when a smaller and lower-stakes protect surface is selected as a pilot so its metrics can be leveraged to highlight the change to the security paradigm and demonstrate business value.

Communicating the business value of Zero Trust will effectively encourage leadership to ensure a proper tone from the top and set the stage for a successful Zero Trust journey.

4. Business Value

4.1 What do we mean by *Business Value*?

This section is intended to introduce readers to core universal business concepts and terms. The foundational vocabulary and conceptual model provided will enable readers to ask more effective questions, understand business drivers, and construct a business-meaningful case for adopting Zero Trust. This section is not intended to be a comprehensive introduction to business or financial management, as there are many other credible resources available for that.

In addition to for-profit businesses, there are many different types of organizations, including not-for-profit organizations, governmental agencies, and regulatory bodies, which are not businesses in the traditional sense. For example, a federal government agency responsible for regulating the banking industry is not a "business," yet it can benefit from Zero Trust. For organizations such as these, the term *business value* should be interpreted to mean contributing to *fulfilling their organizational mission objectives*.

Businesses operate on financial and performance metrics, and have developed a comprehensive set of standard ways to measure these. If your organization is a publicly-traded company, it is required to report on the state of the business publicly. These reports are a must-read for you, as they'll quickly connect you to the organization's metrics and performance, as well as the strategic challenges and opportunities it faces.

While not all of the following measurements are applicable to every organization, this list touches on several common ones you should be familiar with. To understand specifics for your organization, it may be prudent, after performing some basic research, to find a friendly colleague in the finance department, and ask them which financial terms and metrics are most important to your organization[2].

- Revenue: Quarterly, Annual, Annual Recurring Revenue
- Net Income or Earnings
- Margins
- Cost of Revenue and Gross Profit
- Cost of Goods Sold (COGS)
- Cash Flow
- EBITDA (Earnings Before Interest, Taxes, Depreciation, and Amortization)
- Order-to-Cash and Days Sales Outstanding (DSO)
- Balance Sheet health

In addition to those financial reporting metrics, businesses also frequently track:

[2] There are also reputable web references for these terms, including Investopedia Financial Terms Dictionary and Harvey's Hypertextual Finance Glossary

- Stock price and performance, in absolute terms as well as compared to peers
- Compliance with regulatory requirements or voluntary guidelines
- Audits and audit findings
- Reputation and brand value
- Employee productivity
- Operational efficiency

Different roles have different priorities. For example, shareholders tend to be most interested in a healthy stock price and/or reliable dividends. Stakeholders on the other hand, may care more about other metrics, depending on their role.

4.1.2 Business Value and Risk

Businesses also care a great deal about *risk*. The discipline of Risk Management (RM) recognizes four risk treatments: Accept, Avoid, Mitigate, and Transfer[3]. Recent years have shown that neither risk acceptance nor risk avoidance are sufficient. We also know that risk transfer, most commonly in the form of insurance, does not prevent incidents, and is becoming too costly to be practical in many cases. Risk mitigation remains the most effective investment.

Mitigation requires a set of controls (e.g., technical, people, process) which reduces risk to acceptable levels. Like any control, it costs money, consumes resources, and often slows things down. Since Zero Trust is a holistic strategy for the enterprise, a single platform and policy model can form the foundation for other areas such as Privacy, Security, Compliance, and Third-Party Risk Management (TPRM). Zero Trust architectures will enforce multiple controls across infrastructure technologies and layers.

The risk of insider threats can be the most difficult for an organization to manage as it involves valid users with legitimate access (e.g. employees, former employees, contractors, or business associates) who have inside information concerning the organization's security practices, data, and computer systems. The threat may involve fraud, theft of assets, the theft of intellectual property (IP), or even sabotage. Often, incidents from insiders involve the misuse of valid access. Zero Trust, by enforcing the principle of least privilege, reduces insider threat likelihood by requiring the proper identification (authentication) and the validation of access rights (authorization) prior to granting access to an asset. It also limits the impact by constraining lateral movement, and with it, the scope of the impact.

Third-party risk management, sometimes referred to as vendor risk management or supply chain management, is the practice of evaluating and mitigating the risks introduced by vendors (e.g. suppliers, business partners, and members of the supply chain). This process typically begins when the relationship is first formed, and continues throughout the life of the relationship, including when the relationship is closed. A Zero Trust strategy reduces these risks through providing better visibility and controls to minimize the impact of any third party security incidents, and to grant least-privilege access for these parties.

[3] The International Standards Organization (ISO) uses the terms Retain, Avoid, Optimize, Transfer to refer to these same principles in the ISO 31000:2018(en), Risk management – Guidelines

4.2 The Business Value of Information Security

In simple terms, Information Security refers to the protection and safeguarding of a company's digital assets, systems, and data. By implementing effective security measures, a business can minimize unauthorized access, data breaches, and cyberattacks, enabling smooth functioning of its operations, maintaining trust with customers and partners, and avoiding potential financial losses or reputational damage caused by security incidents.

The increasingly prevalent digitization of our businesses and economy has led to InfoSec becoming a primary, as well as board-level, concern within organizations. The World Economic Forum (WEF) states that more than 60% of the Global Domestic Product (GDP) is digital[4], while the National Bureau of Economic Research (NBER) has determined that corporate valuations are mostly driven by intangible assets, which include data and intellectual property (IP)[5]. These assets are increasingly the targets of attacks and breaches, and therefore must be properly secured.

Information Security is based on three primary concepts, **Confidentiality**, **Integrity**, and **Availability**, which together make up what is known as the CIA triad. Security policy, implementation, and the description of security risks are based on these three parameters:

- **Confidentiality** is the concept that those things a company holds as critical to the business, or information that should not be shared, is kept safe and private, and only those with a need to know have access.
- **Integrity** is protection of what the business deems as valuable, to assure it is not tampered with or changed without the knowledge of proper parties. The information, data, or objects maintain their accuracy.
- **Availability** is simply assuring that the object or asset is ready for use when it is needed by the business.

When implemented correctly, InfoSec can and should support the mission of the business. Security supports the business by reducing risks to the overall business by protecting the assets that the business has identified as valuable. The successful implementation of information security has the added benefit of promoting compliance to international and domestic standards and regulations. Compliance with many of these standards and regulations (e.g. HIPAA, GDPR, PCI DSS, and ISO 27000) includes requirements around data protection, proper risk management, limiting access to protected data and processes, and regular training on how to protect this information. All of these things are part of a proper InfoSec program.

---

[4] "Digitalization: a silver bullet", World Economic Forum: https://www.weforum.org/agenda/2022/05/a-digital-silver-bullet-for-the-world/

[5] "Intangible Value", Andrea L. Eisfeldt, Edward Kim & Dimitris Papanikolaou, November 2021, US National Bureau of Economic Research (NBER): https://www.nber.org/papers/w28056

From risk management (RM) and compliance perspectives, IT and OT systems represent a considerable source of risk which must be mitigated by the enforcement of technical or process controls. These controls may be self-defined, or they may be externally imposed on them as with regulatory compliance. Organizations typically have to demonstrate how their controls are operating as intended, through compliance reporting or an audit process.

Zero Trust improves security by ensuring that existing controls are operating as intended, as well as providing an organization with a continuous improvement program that further strengthens those controls. In an environment where trust is not inherent, the security team continuously vets the controls by using a risk framework to monitor, identify, protect, detect, respond and recover from perceived and existing threats. This helps with prioritization as no organization has unlimited resources or unlimited time. Zero Trust forms a foundation for all of your cybersecurity, privacy, and operational resilience (OR) activities.

Zero Trust goes well beyond just improving control effectiveness. As an overarching strategy and architecture, Zero Trust breaks down the barriers between organizations internally, bringing together IT, Security, applications, architecture, and the business under a unified vision for securing assets in line with business goals.

4.3 Making a Business Case for Investment in Zero Trust

In the most general terms, a *Business Case* assists organizational stakeholders in making decisions regarding the viability of a proposed project effort, and its use is considered standard practice throughout private and public sector organizations. A Business Case is typically a documented, structured proposal, prepared to facilitate a selection decision for a proposed investment or project by organizational decision-makers. A Business Case describes the reasons and justification for the investment or project in terms of business process performance, needs and/or problems, and expected benefits. It identifies the high-level requirements that are to be satisfied, and provides an analysis of proposed alternative solutions (with reasons for rejecting or carrying forward each option), assumptions, constraints, a risk-adjusted cost-benefit analysis (CBA), and a preliminary acquisition strategy. It may also include financial metrics such as Return on Investment (ROI), a projected Total Cost of Ownership (TCO), or a Net Present Value (NPV), among others.

There is rarely a sufficient connection between an InfoSec investment and revenue generation to make the calculation of ROI or NPV practical. Instead, InfoSec investments are typically looked at in terms of TCO reduction, or as an enabler to driving business value.

Different organizations have different levels of formality, process, and structure for making decisions, and will have different expectations of the content of a business case. Practitioners should take the time to

learn about how technology, strategy, and IT investment decisions are made inside their organization, and follow the appropriate process and structure.

One consistent aspect of a business case is that it must deliver *business value,* which is the main focus of this document. The following section provides fourteen different ways a Zero Trust initiative can deliver business value. Once you determine the applicable areas, you can quantify them appropriately, and incorporate them into the business case structure required by your organization.

5. The Business Value of Zero Trust

As introduced previously, Zero Trust is an enhanced security and risk management approach that assumes that no identity (person, non-person/machine), device (PC, Mobile, IoT) or workload (server, computing instance, container, or function) can be trusted by default. All access relies on authenticated identities, and the evaluation and assignment of access policies based on contextual information.

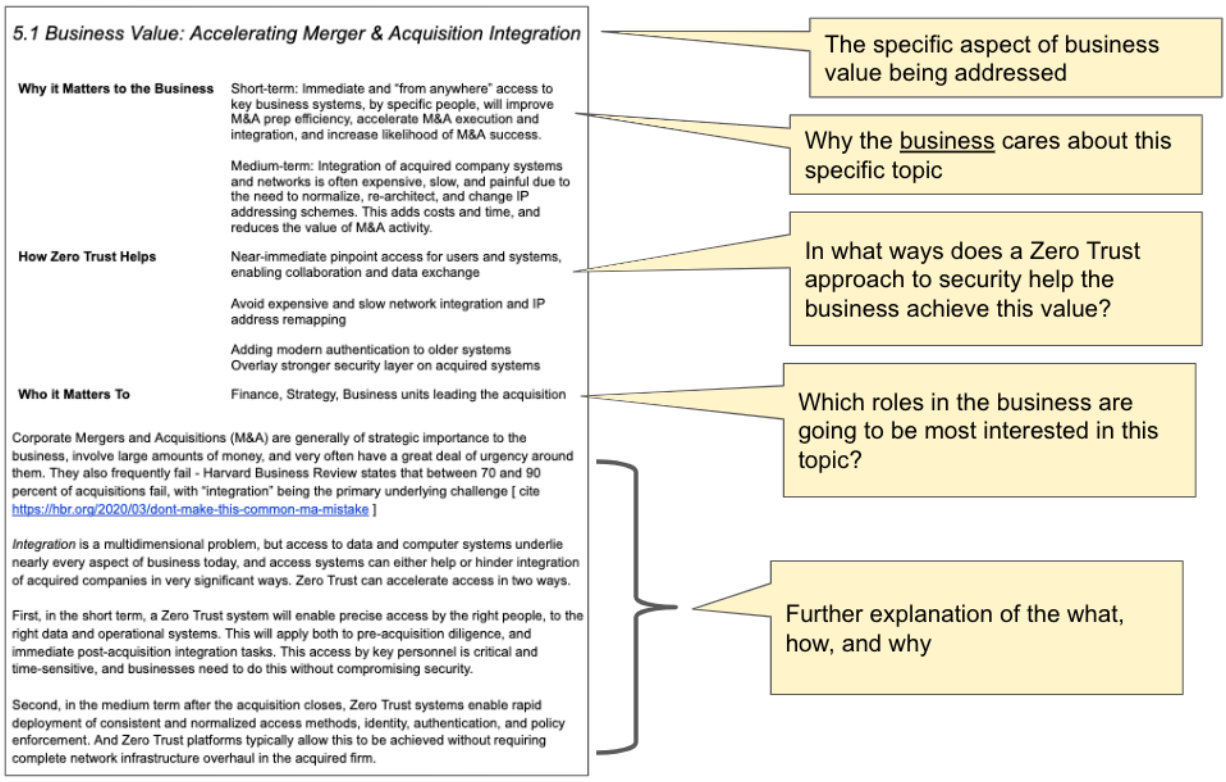
Zero Trust requires an ongoing investment of time, resources, and budget, but in return delivers security, technical, and business benefits. At a high level, Zero Trust delivers business value by providing the following benefits:

- Simplified and streamlined security and IT infrastructure management by centralizing and automating security policies, leading to cost savings and operational efficiency
- Better protection of sensitive data and intellectual property from unauthorized access, increasing the organization's cyber-resilience and reducing the risk of data breaches and financial losses
- Improved regulatory compliance, avoiding potential penalties and maintaining a positive brand reputation
- Reduced time, cost, and effort associated with meeting and reporting on compliance requirements
- Enhanced organizational agility and adaptability to changing business environments, including reengineering business processes
- Increased stakeholder confidence, as customers, partners, and investors can trust the organization's commitment to security and data protection
- Reduced IT and operational costs through infrastructure simplification, centralized policy management, and automation
- Turning IT and Security into a business enabler
- Aligning business and security goals across the entire organization and reducing siloed activities

Zero Trust differs from previous approaches to security, which have promised some or all of these benefits. Specifically, a Zero Trust approach is inherently holistic and must consider and dynamically enforce controls across traditionally siloed systems and layers of the IT and security infrastructure.

Section Format

In order to more easily communicate these high-level goals, we're presenting them in a concise, one-page format. The following diagram provides an example of business value for stakeholders involved in a merger/acquisition scenario.



5.1 Business Value: Cost Reduction and Optimization

Why it Matters to the Business

Reduced total cost of ownership for security, more efficient allocation of resources across business units rather than a siloed approach (CapEx, OpEx, people)

How Zero Trust Helps

Reduced need for legacy security systems, reduced risk of security breaches lowers recovery costs, simplified security architecture and automation improves productivity

Who it Matters To

Executives concerned with cost reduction and risk management (CFO, CISO, CIO), IT and security teams, employees who need secure access to resources for their daily work

Zero Trust allows organizations to consolidate disparate, and redundant, tools and technologies through standardization and simplification of user and device access, such as replacing a remote access tool (e.g. VPN) and an on-premises access tool (e.g. NAC) with a single access tool. This means that businesses can reduce costs associated with purchasing, deploying, and maintaining redundant perimeter-based security solutions. Since they are newer, Zero Trust platforms tend to use generally accepted best practices, existing standards, and widely adopted protocols, which can result in improved interoperability of systems, and may eliminate the need for custom integrations and reduce the number of deployed tools.

Zero Trust can lead to connectivity and bandwidth cost reductions, especially in traditional enterprise IT infrastructures. Organizations can reduce or eliminate the need for expensive private circuits like MPLS and SD-WAN and rely on the internet as their corporate network. This approach removes the dependency on perimeters and enables point-to-point access from each user to each resource, resulting in significant cost savings associated with site-to-site networking or backhauling everything through a data center.

Zero Trust can improve processes, uncovering further cost-saving opportunities. Streamlining security processes by automating access requests and approvals reduces the need for manual intervention, which can result in reduced administrative overhead and increased productivity. Additionally, Zero Trust simplifies security architecture, reducing the complexity and overhead of management as well as the risk of security breaches.

By reducing the likelihood and impact of security breaches, Zero Trust lowers the cost of data breaches both in aggregate, and for individual incidents. It can directly reduce the cost of a data breach by limiting the extent of the breach, thereby minimizing damage and recovery costs. It can also indirectly lower the cost of a data breach by reducing the occurrence of breaches. Additionally, Zero Trust can help businesses reduce insurance overhead due to tightened and more effective security controls.

Provisioning and securing new infrastructure more quickly is also possible with Zero Trust, as businesses can reduce the time and effort required to set up users on new devices and enforce security policies.

5.2 Business Value: Operational Resilience

Why it Matters to the Business

Operational resilience is the ability to deliver operations, including critical operations and core business functions, through disruption from any hazard. Business operations are often wholly dependent on IT technologies and systems, and fragile or unreliable IT infrastructure will have significant and disruptive impacts on a business. Resilience of a businesses operational infrastructure systems must be a critical priority.

How Zero Trust Helps

By default, systems and devices in a Zero Trust architecture are isolated from one another. Only authenticated and authorized identities are permitted to communicate, and are restricted to only authorized protocols.

Zero Trust's fine-grained segmentation reduces the ability of an attacker to perform reconnaissance or move laterally. This smaller *blast radius* of an attack makes the entire system more resilient. Zero Trust platforms also improve preparation for and execution of Business Continuity and Disaster Recovery, by quickly adapting and granting access to changed environments (e.g. DR sites)

Who it Matters To

COO, CEO, CFO, operations teams, lines of business leaders

Zero Trust policies should be based on an *inside-out strategy*, where enterprises make a deliberate shift from asking "What are we trying to defend against?" to "What are we trying to protect?" Policies can then be prioritized based on the asset's value, typically determined, at least in part, based on the service they deliver or the process they support. This creates better alignment with the business and also increases the resilience of the business.

Adopting a Zero Trust framework allows for reduced risk through an overall reduction in ability for malicious actors to traverse the network, and to reduce the effect of ransomware through advanced segmentation and authorization. Properly implemented Zero Trust controls can significantly reduce the blast radius of ransomware or other exploits. This is particularly valuable in protecting critical network infrastructure from network-centric attack risks that often enter from compromised users and VPN connectivity.

From an operations standpoint, due to its proactive nature and effectiveness in minimizing incidents, it reduces risk related to business operations and allows for leaner teams for maintenance. Additionally, it lends to strong business continuity and disaster recovery processes, enabling operational resiliency.

5.3 Business Agility

Why it Matters to the Business

The ability to rapidly respond to market changes and business opportunities is often extremely valuable, and can have an outsized impact on its success. Technologies or approaches that can make a business more nimble can often be very appealing.

How Zero Trust Helps

Strengthening security while improving productivity through simplification and dynamic, real-time policy updates.
Improved prevention and reduction of overhead required to maintain security allows the business to remain ready and focused on seizing business opportunities. Even just freeing up security teams' time in order to collaborate better with the business is valuable.

Who it Matters To

CEO, CPO, CISO, CTO, CIO, COO, Risk, Operational teams

The flexibility to adapt to changing business needs is provided by the Zero Trust model. Access policies can be adjusted automatically to reflect an employee's new responsibilities when they change organizational roles, or when new systems are brought online to address market opportunities. This enables organizations to quickly adapt to changing business needs without compromising security.

The Zero Trust model ensures personnel can securely access corporate resources from anywhere on any device. This facilitates remote work by providing secure access to resources, allowing personnel to easily access the resources they need to do their jobs while maintaining security standards. This also enhances collaboration and innovation by providing secure access to resources across different departments and teams, allowing employees to collaborate more easily and share resources without compromising security, leading to increased productivity.

Zero Trust can simplify the operation of an enterprise security architecture, by providing a unified control plane and policy model, resulting in more efficient system management and user access. This allows organizations to move quickly to pursue business opportunities while managing risk. Additionally, device health, malware status, and changes to security policies are constantly monitored and validated, empowering the organization to execute with confidence and agility.

Furthermore, Zero Trust enables faster adoption of new technologies, such as cloud computing and mobile devices, by providing a comprehensive security framework that can be applied to any environment. By enhancing the organization's security posture and minimizing the risk of security breaches, Zero Trust enables faster and smoother deployment of new applications and services while maintaining stringent security protocols.

5.4 Business Value: Facilitating Compliance

Why it Matters to the Business

Compliance requirements may be imposed on the business by government or industry regulators, or may be willingly adopted by the business in order to improve its standing by obtaining various certifications. In both cases, the organization is required to demonstrate that it's meeting compliance standards. These standards typically dictate various technology and process controls. Compliance reporting is the act of documenting and demonstrating that these controls are in place and effective. Failure to meet compliance requirements can result in fines, which can be significant.

How Zero Trust Helps

Zero Trust systems require positive evaluation of dynamic and context-aware policies. Because these policies are dynamic, they reduce the manual effort required to enforce them. And, because they can be tied to business processes, these systems can often automatically generate compliance reports. Zero Trust systems can reduce the cost and effort of enforcing controls, and of reporting on compliance requirements (creating audit documentation). They also ensure the organization is continuously compliant, not just periodically compliant.

Who it Matters To

Board of Directors, Compliance Team/Chief Compliance Officer, GRC Team, CFO, Application Owners

Meeting and reporting on compliance requirements is often complex, time-consuming, and expensive. Zero Trust will often reduce this overhead in many ways. First, since a Zero Trust system is based on contextual, automated policies, it's easier for them to achieve and remain in compliance. This is because the policies, typically described in meaningful business terms, automatically adapt to changes in identity or device context, ensuring the organization is continuously compliant.

Second, a Zero Trust system's set of controls is typically self-documenting. When policies for in-scope assets are clear and consistently applied, all traffic is encrypted, and all access is logged, evidence collection is less burdensome and takes less time, reducing the organizational burden of the audit itself. That is, a Zero Trust architecture reduces the overhead and "thrashing" that compliance audits cause an organization.

5.5 Business Value: Preserving Reputation and Brand Value

Why it Matters to the Business

In today's world, where cyber threats and data breaches are becoming more prevalent, security has become a critical concern for businesses of all sizes. A data breach can not only result in financial losses but can also lead to reputational damage, affecting a company's brand value and stock price. Therefore, businesses need to take measures to increase security and defend their brand value.

How Zero Trust Helps

A Zero Trust architecture will harden the organization as a target, accelerate threat detection and response, and reduce the impact of successful attacks. These benefits will preserve its reputation and brand value, by lessening the frequency and impact of cyber attacks.

Who it Matters To

There are many stakeholders involved in the security and defense of a business's brand and reputation, including senior management approving budgets, IT leaders deploying security, legal personnel ensuring compliance, and HR for monitoring security protocols. Zero Trust is a useful reference for PR messaging and customer expectations for data protection.

By implementing such measures, businesses can protect their data from unauthorized access, theft, and other cyber threats. Businesses can also invest in security monitoring tools that can detect and respond to threats in real-time. These tools can help businesses to identify and respond to security incidents quickly, minimizing the damage caused by a breach.

In summary, increasing security and defending brand value is a priority for businesses. By implementing a robust Zero Trust cybersecurity architecture, educating employees on best practices, investing in security monitoring tools, and having a crisis management plan in place, businesses can protect their data and reputation from cyber threats.

5.6 Business Value: IT Risk Reduction

Why it Matters to the Business

Managing and treating IT risks is crucial for organizations across various industries to reduce the impact of security incidents that can significantly affect business operations, revenue generation, and business reputation. Reducing IT risks help with protecting sensitive information, maintaining productivity, ensuring uninterrupted service delivery, and meeting compliance and regulation requirements.

How Zero Trust Helps

Organizations need a dynamic and comprehensive approach to enhance security posture and reduce associated risks. Zero Trust Architecture assumes no inherent trust and promotes dynamic, risk-based and strong identity and access controls, context-based and adaptive segmentation, continuous monitoring, and proactive security measures. As a result, Zero Trust promotes a strong security posture, protects critical assets, and safeguards against sophisticated cyber threats.

Who it Matters To

IT risk reduction is critical for various organizational stakeholders, including third parties. Business leaders who are responsible for ensuring the organization's security and mitigating IT risks by investing in risk reduction measures. IT and security teams who are responsible for assessing, implementing, managing and monitoring risk reduction strategies. End users who are on the front lines, and their awareness, actions and willingness to follow and adapt can significantly impact the adoption process of Zero Trust strategies.

Adopting Zero Trust architecture empowers organizations to reduce the likelihood of cybersecurity incidents by implementing stringent access controls and ensures that users and devices are continually authenticated and authorized before accessing resources, minimizing the risk of unauthorized access. It also enables better visibility and response to potential abnormal activity, and the creation and operation of more resilient networks. Additionally, compartmentalizing the network and limiting lateral movement can minimize the blast radius of potential incidents, ensuring that any security breach is contained and its impact is mitigated.

These risk reduction measures strengthen an organization's overall cybersecurity posture, providing increased resilience against evolving threats in the digital landscape.

5.7 Business Value: Secure Adoption of New Technology

Why it Matters to the Business

Flexibility, Cost Reduction, Future Proofing

Secure adoption of new technology is key to staying competitive in a changing landscape and growing revenue

How Zero Trust Helps

Due to its flexibility, a well constructed ZT architecture should be able to integrate new technologies without a major re-architecture and associated cost. Zero Trust is inherently about using a broader set of contextual information to make access decisions.

Who it Matters To

Engineering, Finance, Information Security, Product Owners

The adoption of an architecture based on Zero Trust will lead to a more secure adoption of any new technologies from new clouds, IoT, to AI since ZT focuses on protecting resources (assets including cloud-based assets, services, workflows, network accounts, structured and unstructured data, etc.), rather than just network segments or IP addresses.

For example, new cloud-based services can be easily incorporated into an enterprise's Zero Trust policy model and enforcement points, and tied into their authentication systems. This allows enterprises to quickly use this new technology without sacrificing security or productivity.

5.8 Business Value: Accelerating Business Unit Integration (Merger & Acquisition)

Why it Matters to the Business

Short-term: Immediate and "from anywhere" access to key business systems, by specific people, will improve M&A prep efficiency, accelerate M&A execution and integration, and increase the likelihood of M&A success.

Medium-term: Integration of acquired company systems and networks is often expensive, slow, and painful due to the need to normalize, re-architect, and change IP addressing schemes. This adds costs and time, and reduces the value of M&A activity.

How Zero Trust Helps

Near-immediate pinpoint access for users and systems, enabling collaboration and data exchange.

Avoiding expensive and slow network integration and IP address remapping.

Add modern authentication to older systems,overlay a stronger security layer on acquired systems.

Who it Matters To

Finance, Strategy, Business units leading the acquisition

Corporate Mergers and Acquisitions (M&A) are generally of strategic importance to the business, involve large amounts of money, and very often have a great deal of urgency around them. They also frequently fail - the Harvard Business Review states that between 70 and 90 percent of acquisitions fail, with "integration" being the primary underlying challenge.

Integration is a multidimensional problem, as access to data and computer systems underlie nearly every aspect of business today, and access systems can either help or hinder integration of acquired companies in very significant ways. Zero Trust can accelerate access in two ways.

First, in the short term, a Zero Trust system will enable precise access by the right people (or systems), to the right data and operational systems. This will apply both to pre-acquisition due diligence, and immediate post-acquisition integration tasks. This access by key personnel is critical and time-sensitive, and businesses must do this without compromising security.

Second, in the medium term after the acquisition closes, Zero Trust systems enable rapid deployment of consistent and normalized access methods, identity, authentication, and policy enforcement. And Zero Trust platforms typically allow this to be achieved without requiring a complete network infrastructure overhaul in the acquired firm.

5.9 Business Value: Better Leverage Existing Investments

Why it Matters to the Business

Lower cost of operations and better integration between existing investments, providing better visibility and response to threats.

How Zero Trust Helps

By streamlining controls into fewer platforms and maximizing integration between technologies, Zero Trust can create a streamlined, integrated technology stack with lower cost of operations and higher security efficacy.

Who it Matters To

CISO, CIO, Procurement, CFO, Security Operations

Since Zero Trust architectures leverage best-practices usage of commonly-deployed security infrastructure, organizations do not necessarily need to purchase new technology in order to meet the requirements, as long as the existing technologies in use are able to meet the needs of the control.

For example, existing identity and access platforms can often be used as the starting point, with layering of dynamically triggered Multifactor Authentication (MFA) and other context, such as device health and location, to provide more granular access control. From there, network infrastructure might be reduced, but for organizations with legacy on-premises workloads, current investments can continue to be leveraged as required.

In most organizations, it's likely that there are *some* controls and activities already in place which will fit well into a Zero Trust strategy, and should be expanded to cover a broader scope within the enterprise. By increasing utilization of existing platforms within a holistic Zero Trust policy model, organizations can start to phase out some point products in favor of consolidation to drive more efficiency and lower the cost of operations.

5.10 Improved Visibility & Analytics

Why it Matters to the Business

Improving and enhancing data collection, and turning data into information and knowledge allows the business to make informed security decisions related to risks and the success or failure of these decisions.

How Zero Trust Helps

The collection and reporting of identity and context-enhanced data provides visibility across risk areas and overall impacts specific changes will make to an entire environment. This visibility will also allow for better identification of resource requirements, and processes that a decision may impact.

Who it Matters To

CSO, CIO, COO, CFO

IT, operations, and security teams often struggle with incomplete and outdated asset inventory and utilization information. Zero Trust, because it operates from a default-deny perspective, requires that identities and resources be identified and/or authenticated. This results in a clearer and more accurate picture of infrastructure and assets, as a byproduct of a Zero Trust architecture.

This increased visibility into systems and more accurate inventories allows for better and more accurate access policies as well as improved responses during a security event. For example, during an active security incident, accurate identification of all impacted environments and processes allows for a more timely and complete response. Better visibility into the priority of the systems to be fixed based on business need and the completeness of the response can also be identified and monitored. During the response the security and operational teams can perform additional focus on more vulnerable or business-critical systems.

An accurate and current inventory and visibility into actual usage also assists in the proper sizing of licensing costs both current and projected due to changes in processes. Physical equipment inventories assist with maintenance costs, as well as in infrastructure lifecycle management.

5.11 Improving User Experience

Why it Matters to the Business

User productivity is core to business efficiency, profitability, and competitiveness. Eliminating frustrations and barriers is also a good employee retention strategy.

IT is a critical tool for business user productivity, but is too often a perceived or actual source of friction.

How Zero Trust Helps

Zero Trust can eliminate siloed and outdated access systems, enable the secure adoption of newer technologies, reduce network latency, and avoid security-related downtime

Who it Matters To

All users, CFO, COO, HR, CEO, CIO, Business leaders

Zero Trust improves user experience by enhancing productivity, reducing network latency, increasing agility, and boosting employee satisfaction. It enables users to securely access resources anytime, anywhere, improving productivity and work-life balance. By applying security controls closer to users and resources, access processes can be accelerated, ensuring a seamless and efficient user experience. The adaptive nature of Zero Trust allows organizations to quickly respond to changing business needs and threats, increasing agility and responsiveness. This, in turn, contributes to higher employee satisfaction and retention rates.

Zero Trust's focus on granular access controls improves the accuracy of "need to know" policy decisions. It ensures that users remain fully productive, while minimizing unauthorized access risks, enhancing overall security.

While implementing Zero Trust will often require changes to existing processes, it presents an opportunity to address technical debt and modernize security infrastructure. The long-term benefits of improved security, reduced risk, and enhanced user experience outweigh the temporary inconveniences, making Zero Trust a valuable framework for organizations seeking to optimize their security posture.

5.12 Supporting Strategic Business Initiatives

Why it Matters to the Business

Business initiatives defined as "strategic" are, by definition, essential for businesses to gain a competitive edge, drive growth and profitability, adapt to changes, enhance stakeholder value, and future-proof the organization.

Due to their strategic nature, it's imperative for them to be successful.

How Zero Trust Helps

By establishing a robust security foundation, Zero Trust empowers organizations to embrace innovation, meet regulatory requirements, securely integrate new assets, and foster trusted partnerships.

Who it Matters To

CIO, CFO, COO, CEO, Board of Directors

Zero Trust plays a crucial role in supporting strategic business initiatives by providing a secure foundation for various key areas. First, in the context of digital transformation, Zero Trust enables organizations to confidently embrace new technologies, expand their networks, and facilitate remote work and remote access without compromising security. It ensures that access to resources is granted based on identity and authorization, protecting sensitive data and mitigating the risk of breaches.

In addition, Zero Trust supports strategic business changes to organizational structure, such as mergers, divestitures, or acquisitions, by providing a framework for securely integrating (or separating) disparate networks, systems, and user bases. It allows organizations to enforce consistent access controls, verify identities, and protect sensitive data during the integration process. Similarly, Zero Trust facilitates secure partner collaboration by extending access controls beyond the organization's boundaries. Mechanisms like secure identity federation and access management, enable organizations to collaborate with external parties, share resources, and protect intellectual property.

5.13 Business Value: Reinventing Business Processes

Why it Matters to the Business

Business processes are the core of what businesses do, and using secure technology to reinvent them can result in increased efficiency, better competitive advantage, improved profit margin, more efficient resource optimization, and enhanced customer experience.

How Zero Trust Helps

Zero Trust's model enables secure access by any user to any resource, expanding the possibilities for new and improved business processes, without the location or network-based constraints of traditional IT and security architectures.

Who it Matters To

Executives and business leaders, security professionals, employees, end users and clients, shareholders and investors, regulatory and compliance bodies

The convergence of big data, cloud, and serverless computing has driven the adoption of new technologies, aiming to improve operational efficiency and user experiences. Consequently, many organizations are reviewing their existing business processes and embracing digital transformation. During this process, it is crucial to identify and eliminate unnecessary processes and address any 'dead code' that no longer serves a purpose. This proactive approach significantly reduces the overall attack surface and improves the organization's security posture.

During business process (re)engineering, organizations should diligently evaluate each workflow, access control mechanism, and authentication process to ensure that trust is not automatically granted but continuously verified. Adoption of least privilege access policies and regular monitoring and analyzing of traffic and workflow behavior to detect anomalies. By assessing and evaluating business processes from a Zero Trust perspective, organizations can derive several benefits. First, they significantly improve their security posture by eliminating implicit trust assumptions, scrutinizing access to sensitive information, and reinforcing access controls with granular authorization policies. This, in turn, mitigates the risks of unauthorized access, data breaches, and insider threats. Additionally, organizations enhance regulatory compliance by implementing robust data protection measures and auditable access controls.

Zero Trust empowers organizations to mitigate the risks of transformation initiatives. Organizations often adopt cloud services, embrace machine learning and mobility, and integrate third-party systems and partners throughout this journey. These new digital capabilities expand the attack surface and introduce potential vulnerabilities. However, by implementing Zero Trust, the organization ensures that access to sensitive resources and data is continuously verified and authorized, regardless of the location or device used.

Zero Trust fosters a more agile and flexible approach to transformation. Traditional security models often impede innovation and hinder the adoption of new technologies and processes. With Zero Trust, security becomes an integral part of the transformation strategy, enabling organizations to embrace new technologies, streamline processes, and deliver value to customers while maintaining a robust security posture.

5.14 Business Value: Better Meet Prospective Customer Security Requirements

Why it Matters to the Business

Many organizations are increasingly subject to their customers' requirements, in order to conduct business with them. In particular, enterprises are more frequently imposing stricter cybersecurity requirements on their suppliers, partners and vendors, often under *Third-Party Risk Management* initiatives.

How Zero Trust Helps

Adopting Zero Trust allows organizations to substantially improve their security, and to more easily and effectively demonstrate that they have done so.

This allows the business to more quickly and reliably obtain new customers, retain existing customers, and have easier and cheaper access to capital and cyber insurance.

Who it Matters To

CFO, CRO, CEO

Given the highly interconnected nature of today's digital businesses and the sophistication of malicious actors, many enterprises are beginning to enforce stricter security requirements on their vendors, suppliers, and partners. These are often pursued under initiatives such as *Vendor Risk Management* and *Third-Party Risk Management*. Ultimately, this translates to requiring a higher level of maturity, documentation, and compliance from those third parties. These requirements can be imposed on both potential new suppliers, as well as existing suppliers.

From a supplier perspective, meeting these enhanced security requirements becomes a necessity, and one which must quickly become a business priority, given its direct impact on top line business revenue.

Zero Trust, because it is built upon modern security best practices, will allow these organizations to quickly improve their security, compliance, and documentation, and grow the business' revenue. Any business whose customers are other enterprises is likely already facing these stricter security requirements, or will be in the near future. As a result, this use case is often a good candidate for the security team to leverage to gain support for their Zero Trust project.

6. Communicating Business Value

In most organizations, the inherent and "obvious" security benefits of Zero Trust will not be sufficient to convince stakeholders to make changes, allocate time, or invest budgets. To best communicate the business value we've discussed throughout this document, we recommend the following.

Know Your Audience

Zero Trust can be transformational to both small and large aspects of a business, and its supporting IT infrastructure and processes. This requires changing things, and many organizations are inherently resistant to change. To overcome this it's important to communicate the business value that this will deliver, which is the primary aim of this whitepaper. Effective communication requires knowing your audience, so it is important to understand the roles, personalities, and motivations of the key stakeholders and decision-makers in your organization. This knowledge will allow you to better tailor your approach, message and content for maximum understanding and support by these audiences.

Know Your Organizational Landscape

Take time to learn how your organization is structured. Who is responsible for which aspects, and how is their success measured? This can help you more easily find current needs, priorities and projects to which you can associate and attach your Zero Trust initiative. Determine who in your organization is responsible for ("owns") which parts of your overall mission, and what that means for them and their team.

Build a Team and Form Alliances

We'll reinforce that Zero Trust cannot be solely a security-led initiative. Security needs to support a business initiative in order to obtain the resources needed to make changes and investments. Work to build alliances with key business and technology stakeholders, and gain executive leadership or even Board of Directors support. Zero Trust needs to be understood and supported across multiple levels throughout the organization in order to have maximum success.

Communication Strategy

Work with your security team to consciously learn how to speak the language of the business, and how to tailor your message to a specific stakeholder audience. Technical or security presentations will fail to impress many people, so understand your audience, and practice with friendly supporters outside of the IT and security organizations.

Plan for the Journey

Acknowledge to all that Zero Trust is not going to be achieved overnight. It will be implemented in phases based on business risk, budget, technical maturity and change tolerance. Prepare everyone for this journey, and plan to deliver some value quickly to build momentum and support.

7. Conclusion

This document provides important background information for a security leader tasked with making the business case for a Zero Trust project. It is intended to help these security leaders justify the implementation of a Zero Trust architecture by connecting it to the business drivers and business values that matter most to their organization. By using one or more of the business values described in this document, and applying them (and adapting them) to the specifics of their organization, security leaders will be able to make a strong case for adopting Zero Trust.

A comprehensive Zero Trust cybersecurity framework approach provides several key business values and benefits. Here are some reasons why adopting a Zero Trust strategy based on best practice tenets is valuable for all organizations:

1. **Risk Mitigation**: Helps identify and assess potential risks to an organization's information assets, including sensitive data, intellectual property, and critical systems. By implementing security controls and best practices across the IT/IOT portfolio, businesses can effectively mitigate specific risks and minimize the likelihood of security breaches, data leaks, and other cyber threats.

2. **Regulatory Compliance**: Many industries and jurisdictions have specific cybersecurity regulations and compliance requirements that organizations must adhere to. A Zero Trust framework helps businesses meet these obligations and demonstrate commitment to data protection and privacy. Compliance with relevant regulations avoids legal and financial penalties and enhances the organization's reputation and credibility among customers and partners.

3. **Business Continuity**: Cybersecurity incidents can disrupt business operations, cause financial losses, and damage an organization's reputation. A strategic approach such as Zero Trust helps businesses to be more aware of the threat landscape, and better able to establish robust incident response plans, disaster recovery procedures, and business continuity strategies. These measures ensure that in the event of a security breach or system failure, the organization can respond promptly, minimize downtime, and resume normal operations with minimal disruption.

4. **Competitive Advantage**: In today's digital landscape, customers and partners prioritize security when choosing who to do business with. Implementing a comprehensive Zero Trust cybersecurity framework allows businesses to demonstrate their commitment to protecting sensitive information and maintaining data integrity. This commitment can differentiate them from competitors and give them a competitive edge, attracting customers who value data privacy and security.

5. **Trust and Customer Confidence**: A strong cybersecurity posture instills trust and confidence among customers, clients, and stakeholders, which allows organizations to demonstrate customer information security. This trust translates into long-term customer relationships, repeat business, a positive brand reputation, and increased customer loyalty.

6. **Cost Savings**: While implementing a Zero Trust cybersecurity framework requires an initial investment, it can lead to long-term cost savings. Proactive security measures, such as risk assessments, security controls, employee training, and vulnerability management, help identify and address security gaps early on, which reduces the potential impact of security incidents and associated costs. Additionally, a dedicated approach can guide efficient resource allocation across business units, helping businesses optimize their cybersecurity investments.

7. **Simplification, Scalability and Flexibility**: Cybersecurity frameworks provide a structured approach to managing cybersecurity risks. They offer guidelines, standards, and best practices that can be tailored to an organization's specific needs, size, and industry. An organization-wide Zero Trust strategy can facilitate this scalability and flexibility, enabling businesses to adapt new security measures in response to evolving threats, ensuring that their cybersecurity practices remain effective and up-to-date. And, by removing security and operational complexity, organizations can obtain improved results.

In summary, a Zero Trust approach to cybersecurity can provide business value by mitigating risks, facilitating regulatory compliance, maintaining business continuity, providing a competitive advantage, building trust and customer confidence, simplifying operations, generating cost savings, and enabling scalability and flexibility in managing cybersecurity risks, threats, and vulnerabilities. Leveraging Zero Trust capabilities can help businesses synchronize, amplify, and connect current and future technology investments to business value. Zero Trust helps organizations break down silos, and unifies cybersecurity, finance, IT, and business leadership perspectives to drive impact and transformational change across core business components: people, processes, and technology.

Appendix – Useful References

The CSA maintains a Resource Hub within the Zero Trust Advancement Center (ZTAC) https://cloudsecurityalliance.org/zt/resources/. Of particular note, the ZTAC Resource Hub and the CSA Zero Trust Circle Community - contain links to the recordings of a number of relevant ZT informational presentations, including several enterprise case study recordings related to communicating business value and obtaining executive, program and budget approvals.

Key resources referenced in this document that are foundational for CSA ZT research include:

- United States' NSTAC Report to the President on Zero Trust and Trusted Identity Management (cisa.gov)
- United States National Institute of Standards and Technology (NIST) Zero Trust Architecture (SP 800-207)
- United States CISA Zero Trust Maturity Model V2

CSA also maintains relevant terminology references:

- Overall CSA Cloud Security Glossary
- CSA Software-Defined Perimeter Glossary