Zero Trust Guidance for Small and Medium-Sized Businesses (SMBs)

Softchoice

cloud CSA security alliance®

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

Acknowledgments

The scope of Zero Trust research and guidance necessarily includes cloud and on-premises environments and mobile endpoints, with applicability to 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 to inform organizations making decisions appropriate to their specific needs and priorities.
- Apply a deliberately product- and vendor-neutral approach to architectures and implementation approaches to mature ZT implementations.

The ZT Working Group is composed of 9 different work streams that align with the Zero Trust maturity model and architectural pillars. The lead workstreams for this document are ZT1&2, Zero Trust as a Philosophy & Guiding Principle, and Organizational Strategy & Governance led by Frank DePaola, Joy Williams, and Maureen Rosado.

Lead Author(s)

Frank DePaola
Mark Fishburn
Larry Kinkaid
Andrea Knoblauch
Aaron Robel
Alex Sharpe
Michael Theriault

Contributors

Sam Aiello
Sue Bergamo
Dr. Chase Cunningham
Kevin Dillaway
Alice Murr

Reviewers

Akintayo Ajayi
Sami Al-Shaher
Srija Allam Reddy
Deepak Antiya
Richard Baker
Daniel Balmer
Songbo Bu
Jonathan Flack
Aditya Garg
Iftikhar Javed
Shamik Kacker
Rahul Kalva
Chad Kliewer
Kimberley Laris
Steven Lorenz
Dr. Ron Martin
Sonia Mishra
Prateek Mittal
Denis Nwanshi
Meghana Parwate
Mithilesh Ramaswamy
Maureen Rosado
Michael Roza
Naveen Rudraradhya Kumar Yeliyyur
Osama Saleh
Paul Simmonds
Amit Singh
Nelson Spessard
Bryant Tow

CSA Staff

Erik Johnson
Stephen Lumpe
Stephen Smith

About the Sponsor

We are a software- and cloud-focused IT solutions provider that equips organizations to be agile and innovative, and people to be engaged, connected, and creative at work. We do this by delivering secure, AI-powered cloud and digital workplace solutions supported by our advanced software asset management methodology and capabilities. Through our customer success framework, we create value for our customers by reducing their IT spending, optimizing their technology, and supporting business-driven innovation. We are a highly engaged, high-performing team that is welcoming, inclusive, and diverse in thought and experience, and are a certified Great Place to Work® in Canada and the United States. To learn more about us, visit www.softchoice.com.

Table of Contents

Abstract

The objective of this document is to provide foundational guidance for Small and Medium-sized Businesses (SMBs) in their journey to evaluate approaches to manage identified risks through the implementation of a Zero Trust strategy to protect their organization. This guidance is aligned with the five-step Zero Trust implementation process described in the NSTAC Report to the President of the United States on Zero Trust and Trusted Identity Management[1] , originally formulated and socialized by John Kindervag. Additional Cloud Security Alliance (CSA) research documents containing more advanced concepts and guidance for building and maturing Zero Trust architectures exist and will continue to be developed as needs are prioritized.

The foundational guidance detailing these evolving principles guide SMBs in adopting Zero Trust as a core cybersecurity strategy. The unique challenges for SMBs are discussed to provide a roadmap for evaluating, implementing, and benefiting from a Zero Trust architecture. As a precursor for SMBs to the CSA Zero Trust Guiding Principles[2] foundational guidance, this document offers relevant context and practical steps tailored for SMBs across the five-step methodology.

Target Audience

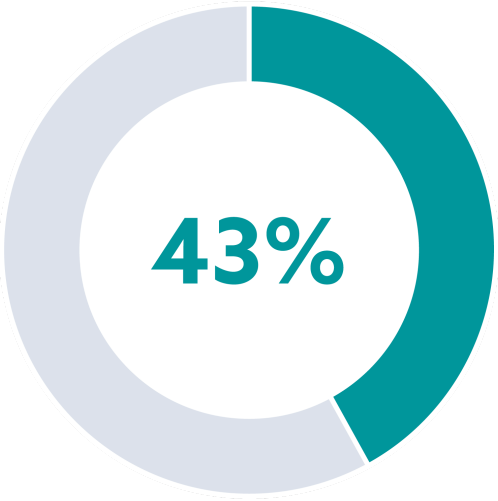
- Primary Audience: SMB Owners, IT/Security Teams, vCISOs, Buyers and Providers of Outsourced/Managed IT and Security Services, Managed Service Providers
- Secondary Audience: Business Managers, SMB Executive/Leadership Team, Office Managers, Administrative Staff, SMB Employees, External IT Auditors and Assessors

Why Should SMBs Be Concerned with Security?

SMBs contribute approximately 40% of global revenue[3] but often encounter significant obstacles in establishing effective cybersecurity measures. Obstacles include limited understanding of business risk tolerance, limited resources for cybersecurity, competing business priorities, development and retention of skilled employees, existing relationships with capable technology partners, and ability to adapt to the rapidly evolving cyber threat landscape. Many SMB owners think cybercriminals only target large corporations, believing they are too small to be a target. However, this misconception can have devastating consequences for SMBs.

[1] NSTAC Report, page 7
[2] CSA Zero Trust Guiding Principles
[3] What are SMBs?

SMB Share of Cyber Attacks (2023)



The impact of a cyberattack on an SMB can be devastating, both financially and reputationally. Recent studies have shown that:

- 43% of cyberattacks last year targeted SMBs with an average cost of $3.31 million USD.[4]
- 41% of small businesses were the victim of an incident in 2023, up 3% from 2022.[5]
- 60% of SMBs go out of business within six months following a direct cyberattack.[6]

SMBs face indirect yet significant impacts from cyber incidents, including the loss of intellectual property, damaged customer trust, and challenges in securing affordable insurance, funding, or lines of credit. These underscore the critical need for robust cybersecurity measures, regardless of business size.

Cybercriminals often attack SMBs as a conduit to broadening the scale and reachability of their attack. A notable real-world example is the 2013 US-based retail giant breach, where attackers gained access via an HVAC vendor, compromising over 40 million credit and debit card accounts. Similarly, a less-publicized incident involved a casino being hacked through a vulnerable internet-connected aquarium. Protecting SMBs is a widely recognized priority to regulators, legislators, and standards bodies.

Attacks against SMBs often include:

- Ransomware: Encrypting data and demanding payment for decryption
- Data Breach (aka Exfiltration): Unauthorized access and theft of sensitive information such as customer or financial records
- Loss of Intellectual Property (IP): Stealing proprietary data, designs, or trade secrets, potentially crippling a business's competitive advantage
- Identity Theft: Misusing credentials to access systems or steal information
- Financial Loss: Fraudulent wire transfers or theft, such as incidents involving Business Email Compromise (BEC) scams
- Operational Outages: Interruptions that prevent delivering services to customers
- Financial Crimes: Leveraging compromised systems for fraud or money laundering
- The Human Element and its Consequences: Cyberattacks occur approximately every 39 seconds, with nearly 95% of breaches attributed to human error

[4] SMB Budget for Cybersecurity
[5] Despite Awareness SMBs Still Highly Vulnerable to Cyber Attacks
[6] 60% of Hacked SMBs are Out of Business 6 Months Later

By 2025, cybercrime-related damages are projected to reach $10.5 trillion USD globally, underscoring the urgency of robust security measures.[7]

SMBs Have Unique Characteristics and Cybersecurity Needs

The value of SMBs is tied to an intense focus on their craft. SMBs benefit from agility and innovation with less bureaucracy. SMBs as a sector are often highly reliant on outsourced IT Managed Service Providers (MSPs) and leverage flexible external security resources like Managed Security Service Providers (MSSPs) and consultants for fractional or remote virtual CISOs (vCISOs).

SMBs are highly susceptible to cyber risk with the impact of an incident potentially being existential. The Small Business Administration (SBA) reports 50% of SMBs have been the victims of at least one cyberattack, with over 60% of those attacked going out of business.[8]

SMBs need to choose providers wisely, as SMBs remain accountable for security posture risks introduced by third-party resources. Clearly defined and coordinated security responsibilities between the SMB and their providers reduce costly security errors under stress. For example, prompt incident response is mandatory in high-risk data industries to minimize community harm. However, its effectiveness relies on intentional coordination with vendors/service providers, making collaboration essential for SMBs in such sectors.

Don't Forget the Basics

As part of developing a Zero Trust strategy, it is recommended to implement certain basic security measures first. It is more important to make progress than include all these elements. While not firm prerequisites, these often serve as the foundational building blocks that a sound Zero Trust strategy can be effectively built upon. The recommendations below are not all-encompassing but represent a list of minimum criteria for an SMB to consider as part of their security architecture. These measures are written in the context of five key constraints that SMBs face:

- Possess little awareness of the real threats to their organization
- Often underestimate the importance of investing in cybersecurity measures
- Lack technical expertise
- Lack proper funding
- Competing business priorities often supersede cybersecurity initiatives

[7] Cybersecurity Statistics 2024
[8] The Impact of Cybersecurity on Small Business

Some basic recommended criteria for an SMB to consider prior to getting started are:

- **Deploy endpoint protection software:** All client and server systems must utilize updated antivirus or endpoint detection and response (EDR) software. Additionally, ensure the software includes automated updating capabilities to simplify maintenance and reduce the risk of human oversight.
- **Patch systems and software applications regularly:** Most operating systems and software applications offer automatic update capabilities, which should be enabled whenever available. If not, SMBs should establish regular processes to install critical updates and patches. Utilizing tools or services to scan the IT environment and identify vulnerabilities with remediation steps is highly recommended. Additionally, operating systems and applications no longer supported by vendors should be upgraded to supported versions to reduce risk where possible. Failing to maintain supported versions and install updates significantly increases the likelihood of compromise.
- **Provide security awareness training to employees:** Human behavior remains one of the largest vulnerabilities in cybersecurity. The 2024 Verizon Data Breach Investigations Report (DBIR) highlights that 68% of data breaches involve the human factor.[9] While not foolproof, it is important for SMBs to provide some level of ongoing security awareness training, if for nothing else than to create a security-aware culture. As threats targeting SMBs continue to evolve, technical controls such as remote browser isolation offer much more effective preventative protection. For less mature organizations, training can serve as a mechanism to minimize the risk of an end-user falling victim. Many budget-friendly security awareness training solutions exist.
- **Perform critical system and data backups regularly:** Data and critical system availability is necessary for any business to function. It is important to perform regular data and system backups at a frequency that can be supported. It is also important to ensure the backup process is resilient from ransomware threats, which often target backups. SMBs should also test to ensure that backups can be restored.
- **Limit access to and adequately protect sensitive data:** SMBs in different industries likely have specific sensitive data types including intellectual property (IP), financial information, personally identifiable information (PII), or software code. Access to this data should be actively managed and granted only when necessary and rescinded when no longer required. Sensitive data should also be encrypted at rest. Internal IT teams or MSPs should enable manageable processes for SMBs to support these best practices.
- **Implement strong password policies with a preference on passwordless:** Passwords have historically been the first line of defense in securing accounts and sensitive information. SMBs should implement a strong password policy that aligns with best practices recommended by the Cybersecurity and Infrastructure Security Agency (CISA).[10] Passkeys and passwordless solutions should be used over passwords whenever possible.
- **Utilize multifactor authentication (MFA) wherever possible:** MFA is an extremely effective control to protect against account takeovers and minimize the risk of unauthorized access.

[9] Verizon DBIR 2024, page 8
[10] CISA Password Guidance

Additionally, MFA can serve as an extremely important building block in an SMB's Zero Trust architecture. MFA should be employed everywhere authenticated access is provided to a critical business system or sensitive organizational data. Re-authenticate using MFA prompts periodically to increase its effectiveness. SMS-based MFA should not be used because of its potential to be compromised. Phishing-resistant MFA should be used where possible.

- **Secure remote access using a virtual private network (VPN) solution:** For SMBs that must grant remote access to on-premises resources, VPN solutions should be utilized. It is important to note that VPNs should be a temporary solution until the SMB can replace the need with a remote access solution that aligns with Zero Trust principles, including explicitly granting access to the resource required and not the whole internal network. Zero Trust Network Access (ZTNA) solutions offer these capabilities.

Please see the Appendix for links to resources providing more detailed guidance.

Introduction to Zero Trust

Zero Trust is a simple approach to information security (InfoSec) that is often misunderstood and overcomplicated. When properly understood, Zero Trust philosophy and strategy are valuable tools that organizations can use to enhance security, increase resilience, and guide digital transformation. These tools can also be applied to AI in a mutually beneficial way: AI can aid with the implementation of a Zero Trust strategy.

Zero Trust is mandated for all Federal Agencies in the United States by Executive Order[11] and is being adopted globally through initiatives such as the Digital Operational Resilience Act (DORA) and the Network and Information Security (NIS2) Directive in the European Union (EU).

Historically, information security relied heavily on technical controls, with security models based on the ability to collect assets and surround them within a controlled physical perimeter. This is no longer the case, especially in a world where work from home, the prevalent use of Wi-Fi, and the expanding use of cloud technologies are the norm. This shift moves security from the perimeter to the data itself, which is imperative as nearly all applications are connected via the internet.

Users were historically presumed to be "trusted" based on their location within the organization's perimeter. Zero Trust upends this concept by requiring verification, irrespective of location, before granting access to an asset and continuously thereafter.

Zero Trust leverages long-standing principles like "never trust, always verify," the concept of least privilege, and the practice of segmentation to increase cyber hygiene, reduce the cost and damage from incidents, and promote faster recovery times. By augmenting their existing security practices with Zero

[11] Executive Order on Improving the Nation's Cybersecurity

Trust principles, organizations establish a strong foundation for safeguarding their assets in complex and distributed environments. This proactive approach enhances security posture and minimizes potential risks associated with the evolving threat landscape.

Zero Trust also recognizes that breaches happen. To foster resilience, Zero Trust provides a means to contain the "blast radius" and reduce the impact of any breach while facilitating quick recovery. These same techniques increase the work and investment required by bad actors, further reducing the likelihood of incidents.

CSA's Zero Trust Guiding Principles[12] is an excellent resource, mapping out the underlying themes of Zero Trust. The reader is highly encouraged to review for a deeper understanding and to review suggestions like these:

- Begin with the End in Mind (Business/Mission Objectives)
- Do Not Overcomplicate
- Products Are Not the Priority
- Access Is a Deliberate Act
- Inside Out, Not Outside In
- Breaches Happen
- Understand Your Risk Appetite
- Ensure the Tone from the Top
- Instill a Zero Trust Culture
- Start Small and Focus on Quick Wins
- Continuously Monitor

Lastly, all strong Zero Trust strategies incorporate the understanding of iteration. SMBs should recognize that success relies on iterative enhancements of controls, starting with straightforward implementations that may be incomplete but can achieve substantial, continual progress over time. SMBs should anticipate this and be prepared to continuously improve. Remember, perfection is the enemy of progress[13].

[12] CSA Zero Trust Guiding Principles
[13] Winston Churchill - Where Ideas, Experiences, and Lessons Learned Intersect

Zero Trust Implementation Process – Five Steps

Step 1 – Inventory and Assessment of Assets

In the broader context of the five-step process for Zero Trust implementation, **step 1** is titled Defining Your Protect Surfaces. A protect surface is a business system comprised of critical Data, Applications, Assets, and Services (DAAS) that require safeguarding due to their importance to business operations or susceptibility to cyber threats. This process helps SMBs prioritize their efforts and focus resources on areas that matter most. Detailed guidance exists on the subject for a wide range of private and public sector organizations. In this document, we focus on the key aspects and activities that are pertinent to SMBs, but the detailed guidance may be useful for more complex scenarios.

The process of defining the protect surface centers around inventorying and classifying different types of technology assets. Identify critical business systems and services initially. The list should then be prioritized by highest importance to the organization and lowest current security maturity. The next step in the process is to identify the DAAS elements that comprise each business system. DAAS elements can

include a variety of resources including sensitive pricing information (data), physical infrastructure that drives the business (assets), important business applications (applications), and key technical services such as identity and access management (services). It is important to identify assets that, if compromised, would disrupt business operations. Asset inventory and assessment is about knowing what assets you are responsible for and depend on, the business impact should they be compromised, and their current security maturity as inputs to determining the priority of what should be protected. Critical systems are often the targets of cybercriminals so their protection must be continually reevaluated in order to effectively manage organizational risk.

Understanding each device's vulnerabilities and level of access to sensitive information is critical. Additionally, essential services that organizational applications and assets depend on should be outlined, such as DNS and directory services. Recognize that disruptions to these services can have significant operational impacts. SMBs should focus first on assets that meet the following criteria:

- Criticality: Essential systems for daily business operations and those involved in driving revenue, such as inventory management, ERP, or CRM software
- Sensitivity: Data repositories containing customer information, intellectual property, financial records, or other sensitive organizational data
- Vulnerability: Systems with known security issues or external exposure

Because SMBs are often resource constrained, a recommended strategy to create efficiencies is to further define the protect surface by grouping related DAAS elements and focusing on securing them as a unit. For example, consider a CRM system and its associated customer data as a single protect surface.

Prioritization is also key for SMBs. The most sensitive or highest-risk elements should be prioritized, such as customer data or financial transaction systems. Assess the potential risks and business impact if each protect surface were compromised, considering factors like third-party support costs to recover financial loss, reputational damage, and regulatory penalties. This assessment will guide you in prioritizing which protect surfaces require immediate attention.

SMB IT teams or their MSPs should implement this process iteratively, starting with a pilot protect surface to gain experience. This could involve a less critical system to validate the process while adequately addressing the change management process. The scope can gradually be expanded based on resource availability, budget, priority, and desired risk reduction. SMBs should start where they are and use the resources at their disposal. Large investments should not be required to get started, rather existing tools and technology investments should be leveraged.

The process of maintaining a DAAS inventory should be revisited continuously as these elements may constantly change. SMB leadership teams should be educated and updated throughout the process. Staff should be aware of Zero Trust principles and understand the importance of protect surfaces, recognizing how their actions affect overall security.

Lastly, SMBs should plan for scalability. As an SMB grows or shrinks, the Zero Trust protect surface strategy should be flexible enough to be adapted accordingly. Protect surfaces should be regularly reviewed and updated to stay aligned with the changing business environment and emerging security threats. This methodical approach enables SMBs to establish a practical and affordable Zero Trust protect surface strategy, effectively protecting critical assets without the need for overly complex or costly solutions.

The critical task of asset management and defining protect surfaces requires executive buy-in and a holistic prioritized approach. Budget and in-house expertise can be barriers to success, therefore MSPs can be leveraged to extend the capabilities and expertise of the SMB. SMBs should start small and take manageable steps towards progress. Taking and documenting these steps can demonstrate due diligence as a competitive advantage when providing products and services to other organizations.

Step 2 – Understand How Your Technology Drives Your Business

In the broader context of the five-step process for Zero Trust implementation, **step 2** is called Mapping the Transaction Flows. This consists of mapping the dependencies and interactions between systems, data, and resources. This is a critical step, which results in a deep understanding of both technology dependencies and core business processes.

To map transaction flows, SMBs should revisit the prioritized list of protect surfaces identified in Step 1. These protect surfaces encompass DAAS that are crucial to the organization's operations. Begin by selecting a critical business system to analyze. For example, an SMB offering residential construction services would identify components such as a web hosting platform for a website, accounting software, and computer-aided design (CAD) software as part of its protect surface. The more time an SMB or their MSPs spend prioritizing and understanding the analysis of interactions, the more effective they will be in defining Zero Trust controls for each subsystem.

Once the SMB has defined the protect surface, they should validate their findings by engaging with other business stakeholders to ensure all elements are accounted for. This collaborative approach ensures no critical elements are overlooked and aligns cybersecurity efforts with business needs and priorities. These elements might include data such as product designs, applications such as CAD applications, assets like servers hosting the applications, and services including credit card payment applications.

The SMB should then identify the users interacting with the protect surface. This involves understanding all internal and external stakeholders, including internal employees, external customers, partners, and third-party service providers. Use resources such as identity management systems, customer databases, and even discussions with the Human Resources (HR) team and business functional leaders to identify different user types and gather relevant user interaction information.

Next, identify dependencies and interactions within and outside the protect surface. This involves analyzing interconnected systems, backend databases, network infrastructure, and dependencies on specific workflows. For example, a regional bank might interact with external financial institutions, external auditors and consultants, and internal systems like Active Directory. Document how these systems exchange data or rely on shared resources. This step helps in identifying all interactions with the protect surface. A practical approach is to use available resources such as network diagrams, architecture diagrams, and data flow diagrams. SMBs and their MSPs should review these documents to visualize the network topology, software system structure, and data flows, which will help in identifying entry and exit points, services, and processes that handle transactions. Additionally, leveraging scanning and monitoring tools can provide real-time insights into transaction flows.

Once you have gathered all this information, map the detailed transaction flows by correlating data from the various relevant sources to create a visual representation to improve understanding, and review these flows with relevant stakeholders within the business for clarity and accuracy.

Finally, validate and refine the protect surface based on the documentation maps. Use this mapping to assess the risk and security maturity of each protect surface. Understanding and correlating the risk and maturity will help to more effectively prioritize. Consider factors such as regulatory compliance requirements and perceived risk appetite of the SMB. Adjust and enhance your protect surface definitions and protections to ensure they are comprehensive enough and adaptable to evolving threats. This step helps in fine-tuning the Zero Trust architecture to include true relevance and business context from the SMB.

Step 3 – Design Your Zero Trust Approach

In the broader context of the five-step process for Zero Trust implementation, **step 3** is called Build a Zero Trust Architecture. In this step, SMBs and their MSPs will begin to formalize a design of their Zero Trust architecture. This incorporates elements from Steps 1 and 2, business context gathered along the way, as well as basic security measures described earlier in this document in the Don't Forget the Basics section.

The scope of the design to be implemented should encompass executive commitment and a security policy that is married to the organization's goals. When security objectives are aligned with organizational business goals, it is much easier to garner the necessary support for the investments required to support a Zero Trust strategy. The scope must also include context from every function of the SMB including HR, Sales, Marketing, Customer Service, Finance, and Legal. Additionally, external parties, contractors, and consultants who have access to sensitive business data and systems would need to be incorporated into the design scope. Zero trust is about protecting critical DAAS, so considering risks and benefits of a Zero Trust strategy for all parties is critical, not just for SMB employees.

As development of the Zero Trust approach begins, it is important to understand that Zero Trust architecture is not product dependent, in that a properly implemented Zero Trust architecture should allow for any technology to be used as long as it fits the requirements of the control and should be flexible enough to allow for vendor/technology changes in the future, if implemented properly.

The goal for an SMB is to design their Zero Trust architecture based on the scope and goals defined in Step 2. The SMB needs to identify and select the appropriate technologies, solutions, and vendors that will enable them to implement the Zero Trust principles and components in their environment. The SMB also needs to define and document the policies, rules, and workflows that will govern the behavior and interactions of their users, devices, and applications.

A key consideration is that an SMB should not focus on spending exorbitant amounts of money when getting started but instead should focus on fully utilizing their existing technology investments. Additionally, it is recommended to consider other technology or business initiatives beyond Zero Trust to determine if there could be a strategic benefit in aligning them. To get started, the SMB or their MSPs should consider the following questions:

- What are the core components and capabilities of your Zero Trust architecture (e.g., identity and access management, device management, network segmentation, data protection, threat detection and response)?
- How will you implement and integrate them into your environment to ensure alignment with organizational requirements (e.g., cloud-based, on-premises, hybrid)?
- What are the best practices and standards that you will follow to ensure the security, reliability, and interoperability of your Zero Trust architecture (e.g., encryption, authentication, authorization, logging, monitoring)?
- What are control capabilities that will enforce access and permissions of your users, devices, and applications, and where will they be placed in your design (e.g., least-privilege, role-based access control, attribute-based access control, context-aware, dynamic)?
- What are the workflows and processes that you will implement to manage and maintain your Zero Trust architecture (e.g., user/device/application provisioning, deprovisioning, auditing, updating)?

Oftentimes, if an SMB has already invested in technologies such as multifactor authentication (MFA), extending MFA to every system where critical DAAS are accessed could serve as a very foundational building block to achieving a ZT use case. Some MFA platforms can also be extended to be more dynamic in nature and can be used to mature the processes the SMB has established when deploying MFA within their organization.
MSPs can help the SMB design their Zero Trust architecture by using tools and methods such as architecture diagrams, use cases, user stories, and test cases. The US Critical & Infrastructure Security Agency (CISA) Zero Trust Maturity Model publication[14] can also be utilized for a practical framework to assess and improve the Zero Trust maturity level.

[14] US Government - Cybersecurity & Infrastructure Security Agency Zero Trust Maturity Model

Another useful resource is US NIST Special Publication 1800-35[15], which goes into depth on the possible architectures and technologies that can be used to implement a Zero Trust architecture. While this document is more geared towards enterprises, it provides comprehensive guidance on the foundations of different architecture possibilities that can be adopted in SMBs.

Step 4 – Implement Your Design

In the broader context of the five-step process for Zero Trust implementation, **step 4** is called Create Zero Trust Policies. Having designed the Zero Trust processes in the previous step, the next step is to begin implementing. In this step, the SMB should focus on creating policies that provide granular rules allowing traffic to access the resource in the protect surface.

This step involves creating Zero Trust security policies and processes that ensure only the right people or resources have the right access to the right data and services across the SMB's environment, which might include on-premises and public/private cloud environments. The SMB should plan to start small and focus on achieving manageable, quick wins. Many SMBs can become overwhelmed at the thought of achieving complex Zero Trust outcomes, but an inherent benefit is that the scope can be as small as you need it to be.

It is important to reiterate the importance of understanding the sensitivity to cost and complexity for many SMBs. As new ZT use cases are achieved, it is highly advisable to revisit the possibility of leveraging existing investments in tools and technologies. When an SMB combines the approach of starting small with using existing tools and technology, achieving ZT outcomes begins to appear achievable and less daunting.

A simple approach to evaluating the return on investment is to compare the costs related to time and technology investments needed to implement a ZT architecture against the financial business impact if critical DAAS were to be negatively impacted by a cybersecurity incident for a prolonged period of time. Leading an SMBs business leadership through an exercise such as a tabletop exercise that uncovers these impacts can be very impactful.

As an SMB begins to consider what ZT outcomes to prioritize, use the data created during the previous steps as key inputs. For example, reviewing the asset data identified in **step 1** and understanding its criticality to your business serves as a critical consideration when prioritizing. Coupling this asset knowledge with the understanding of critical processes that drive the business, which are uncovered by mapping transaction flows in **step 2**, can significantly help an SMB understand where to focus.

From the above steps, the scope, value and cost of protection can be fed back into the organization's security policy and the decision can be made on what should be protected and when based on cost,

[15] US Government - National Institute of Standards & Technology SP 1800-35 Implementing a Zero Trust Architecture

expected risk reduction, impact to the organization and its tolerance to threats. This strongly supports the one-step-at-a-time approach so that as each vulnerability is strengthened, risk is reduced.

Mapping this newfound awareness against existing tools and technologies can quickly help to identify low hanging fruit, which can be a great place to start. Embracing the process in this way can help to simplify the concept of Zero Trust for SMBs, assisting them in envisioning how they can benefit from its outcomes and in developing strong and clear business cases for ongoing organizational support.

Step 5 – Monitor and Maintain Your Environment

In the broader context of the five-step process for Zero Trust implementation, step 5 is called Monitor and Maintain Your Environment. This step addresses monitoring and improving the Zero Trust architecture for an SMB based on the KPIs and metrics defined throughout earlier steps. SMBs should collect and analyze the data and feedback from their Zero Trust architecture components and capabilities. SMBs also need to review and update the policies, rules, and workflows that were implemented for their Zero Trust architecture.

Some questions to consider in this step are:

- How will data and feedback be collected and analyzed from Zero Trust architecture components and capabilities (e.g., logs, alerts, reports, dashboards)?
- How will the performance and effectiveness of a Zero Trust architecture be measured and evaluated against the KPIs and metrics previously defined (e.g., security incidents, data breaches, audit findings, user satisfaction)?
- How will gaps and weaknesses of a Zero Trust architecture be identified and addressed (e.g., root cause analysis, remediation actions, lessons learned)?
- How will an SMB adapt and improve their Zero Trust architecture to the changing needs and expectations of their organization and environment (e.g., feedback loops, continuous improvement, innovation)?

Budget-friendly tools and methods exist that can be helpful such as data analytics, feedback surveys, and performance reviews to help monitor and improve a Zero Trust architecture.

Engaging Service Providers

Given smaller organizations' limited in-house resources, experience, and cybersecurity expertise, delegating to external service providers, such as MSPs, software suppliers, and contractors, has become essential. Effective delegation involves maintaining responsibility while rigorously verifying third parties in the supply chain. CISA has provided a valuable resource by requiring software companies to attest to their suppliers' adherence to secure development practices.[16] This is the Zero Trust thinking that should be applied to verify the security of how all software products and services are developed, operated, and managed.

Selecting the right MSP is critical to addressing an organization's unique needs. Where shortcomings in internal staff and capabilities exist, MSPs can serve as force multipliers for the SMB and help them achieve security maturity without a significant financial investment or internal staffing increases. SMBs should use their networks to determine which MSPs are worth contacting and look for the right combination of capabilities, which might include possessing the best aligned skillset for the technology stack, offer the best aligned support structure, and offer the most competitive pricing. If existing supply chain and procurement processes exist, these can be applied to the procurement of consulting services as well. Key factors to evaluate include the track record of the MSP in handling similar organizations, certifications such as SOC 2 compliance, and transparency in their reporting and monitoring processes.

Framework for Engaging Service Providers for SMBs

- **Due Diligence:** SMBs must conduct thorough due diligence when selecting external service providers.
- **Key Selection Criteria:**
    - **Track Record:** Proven experience in assisting organizations with similar needs and challenges.
    - **Certifications:** Hold relevant industry certifications, such as SOC 2 compliance.
    - **Transparency:** Open and clear communication regarding their reporting and monitoring processes.
- **Capabilities:** Evaluate the skillset, support structure, and pricing of the MSP to ensure alignment with the specific requirements of the SMB.

[16] CISA Secure Software Development Attestation

- **Procurement:** Utilize existing supply chain and procurement processes for consistent and efficient vendor selection.
- **Zero Trust Principle:** Maintain responsibility for security and rigorously verify third-party providers within the supply chain. Ensure the MSP provides consistent reports of Zero Trust program maturity metrics.

Be Aware of Supply Chain Risks

In today's interconnected global business environment, supply chain risks have become significant disruptors, demanding heightened awareness and proactive management. As organizations increasingly rely on external vendors and suppliers, they face greater exposure to cybersecurity threats, disruptions, and other risks stemming from these third-party relationships.

Supply chain risk management (SCRM) is no longer optional, especially for SMBs, as reliance on interconnected supply chains continues to grow. Blindly trusting the security of vendors and suppliers is no longer a viable strategy. SMBs must inventory third-party relationships involving system or network connectivity and implement robust monitoring of these critical environments to mitigate potential risks.

While comprehensive SCRM programs were once limited to large enterprises due to their cost and complexity, technological advancements have made these initiatives more accessible for businesses of all sizes. Looking ahead, SCRM methodologies are expected to shift toward more data-driven, cost-effective, and efficient approaches, enabling organizations to better safeguard their operations.

Conclusion

Adopting a Zero Trust architecture is becoming vital for all organizations globally because of increasingly complex and destructive cyberattacks crippling businesses worldwide. For the SMB, this is becoming increasingly important because Zero Trust architectures can serve as an enabler for them to achieve more advanced defenses than can be achieved through deploying basic security tools alone. In addition, by following the five-step methodology, SMBs can significantly reduce their susceptibility of being breached, ensure appropriate protection of critical data, and maintain strict control over user access, all resulting in the SMB establishing a more resilient organization as a result. By taking a cost-conscious approach, SMBs can also ensure that they achieve desired outcomes of improved security without breaking the bank.

The five-step methodology starts with identifying which assets SMBs need to prioritize protecting while also assessing their current security posture. Next, the organization should assess their business processes and map them in detail to create knowledge and awareness of which processes are the most

critical. The SMB should then design their Zero Trust architecture, which is often enabled by partnering with a capable MSSP. The MSSP can also be an invaluable resource for addressing the remaining steps, which include implementing the ZT architecture, followed by monitoring and maintaining the Zero Trust environment.

The long-term benefits that Zero trust can provide, including enhanced security and resilience, far outweigh the initial efforts. By embracing a Zero Trust architecture, SMBs can safeguard their operations against sophisticated threats, protect their DAAS appropriately, and establish a heightened degree of business resilience. While it is true that SMBs face a unique set of challenges compared to larger enterprises, by embracing Zero Trust, SMBs can create more robust environments that support their business goals.

Appendix

Glossary

- CSA - Glossary
- CSA - SDP Glossary
- On2IT - Zero Trust Dictionary

References

1. NSTAC - Report to the President on Zero Trust and Trusted Identity Management
2. CSA - Zero Trust Guiding Principles
3. What are SMBs?
4. SMB Budget for Cybersecurity
5. Despite Awareness SMBs Still Highly Vulnerable to Cyber Attacks
6. 60% of Hacked SMBs are Out of Business 6 Months Later
7. Cybersecurity Statistics 2024
8. The Impact of Cybersecurity on Small Business
9. Verizon DBIR 2024
10. CISA Password Guidance
11. Executive Order on Improving the Nation's Cybersecurity
12. CSA Zero Trust Guiding Principles
13. Winston Churchill - Where Ideas, Experiences, and Lessons Learned Intersect
14. US Government - Cybersecurity & Infrastructure Security Agency
15. US Government - National Institute of Standards & Technology SP 1800-35 Implementing a Zero Trust Architecture
16. CISA Secure Software Development Attestation

Useful Resources

1. CSA - ZTAC Resource Hub
2. CSA - Zero Trust for Critical Infrastructure Security
3. NIST - Small Business Cybersecurity Corner
4. NIST - Small Business Information Security: The Fundamentals
5. NIST - Cybersecurity Framework 2.0, Small Business Quick-Start Guide
6. CISA - Cyber Guidance for Small Businesses
7. SBA - Strengthen Your Cybersecurity

8. FTC - Cybersecurity for Small Business
9. FCC - Cybersecurity for Small Businesses
10. CIS Center for Internet Security (cisecurity.org)
11. HBR - The Devastating Business Impacts of a Cyber Breach
12. SEC.gov - The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses
13. Verizon DBIR
14. 35 Alarming Small Business Cybersecurity Statistics for 2024

SMB Resources and Definitions

1. Gartner - Small And Midsize Business (SMB)
2. US Dept. of State - What is a Small Business
3. Census.gov - What is a Small Business?
4. OECD - Enterprises by Business Size
5. Markaaz - SMBs are the Backbone of the Economy
6. Computer Weekly - SMBs Leaning More Heavily on MSPs
7. US Chamber of Commerce - The State of Small Business Now
8. Techround - 60% Of SMEs That Suffer a Cyber Attack Out Of Business Within Six Months
9. CISA - Securing SMB Supply Chains Resource Handbook

Significant SMB Security Incidents

- Code Spaces (2014): This startup providing code hosting services went out of business after a cyberattack destroyed most of its data, including backups.
- VerticalScope (2016): A breach exposed 45 million user accounts from this network of online forums. The lack of multifactor authentication was a key issue.
- Click2Gov (2019): A breach that exposed credit card details impacted hundreds of municipalities using this web payment portal.
- Crystal Valley (2022): This agricultural co-op shut down operations for over a week due to a cyberattack on its systems.