Supply Chain as Kill Chain

Security in the Era of Zero Trust

Craig Gibson

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by
Trend Micro Research

Written by
Craig Gibson
Trend Micro

Stock image used under license from Shutterstock.com

For Raimund Genes (1963-2017)

Contents

Zero Trust is an “always-on everywhere” approach to security. It is a contrast to traditional legacy trust models in which security is “sometimes present in some cases.” Legacy trust models were a low-cost, high-value approach to increasing an attacker’s efforts, but in an era of attacker automation and supply chain compromise, that is no longer true. Legacy trust models are broken by this combination of automation and supply chain attack.

A reader could have the following three main takeaways from this Zero Trust paper:

1. **Data hygiene**. Zero Trust highlights sources of low-credibility data, providing insights on where investment can reduce automation costs and labor. Zero Trust-derived data hygiene reduces the risk of Decision Contamination (a kind of fake news consumed by executives and AI). It also supports decisions of increased accuracy made with less data, which has the effect of reducing cloud storage and processing costs.
2. **Supply chain security**. By knowing the identity risk of internal, external, human, and device resources, “internal” and “external” data supply chains can be handled identically and transparently. The incidental benefit of this approach is that the use of common global identifiers (federated identities) makes it easier to sell into other very large enterprises such as federation members (interoperability is cheaper when common unique identifiers are used). These include governments and their suppliers.
3. **Omnichannel and next-generation retail**. Omnichannel is the concept of “all channels, one experience.” Customers engage with your enterprise, rather than with individual services or departments. When bringing these together there are many opportunities for cost savings, but also fraud and cybercrime. These gaps can be secured using Zero Trust for traditional purchases as well as mobile online shopping. These gaps can be secured whether the purchase is made by humans with phones or by roaming autonomous cars and can be configured to meet unified integrity demands between billing and data networks. This omnichannel unity can also be used in meeting compliance requirements.

Zero Trust could be thought of as the reverse of traditional manual security models. It is “opt-out-like” instead of “opt-in-like.” In traditional models, enterprise security risk is assigned by staff with little or no central guidance by identity architects. Identity registrations, rights and privilege assignment, inventory management, incident management, and investigations are all typically performed without enterprise business, identity, security, and architect guidance and are therefore fragmented. Often, the staff responsible for these functions do not have any insight into the business-relevance, enterprise risk, or potential revenue loss related to the powers they give these identities. When blocking, traditional security functions are done because of this “best effort” work, and risk actually increases within the enterprise as the likelihood of revenue-impacting, false-positives increases (such as Cart Abandonment). These false positives either increase the chance of production network outages (and other failures) or increase the number of senior staff needed to apply judgment in fixing these.

In counterpoint, Zero Trust involves identity risk management and continuous assessment. This means the security insights that come from Zero Trust are far more accurate than traditional IT security models. By being more accurate, they can be more automated, less manual, and less heavily staffed. They also are less likely to interrupt revenue. Since confidence in the accuracy of data means you need less data to make the same decision, processing and storage costs related to the cloud can be reduced. This always-on continuous assessment method of Zero Trust could be thought of as a mandatory, "opt-out-like" model.

There are deep consequences and benefits to this reversal.

By being able to assert a security context everywhere all the time, the overall quality of data and its transactions (Data Hygiene) are credibly known. With this heightened confidence in the integrity of the enterprise and its risk, greater responsibility can be given to automation functions. Less reliance is necessary on the human judgement normally needed to "fix" and "check" and "approve" automated functions (which are of course manual as soon as a human is involved). This reliance increases accuracy of decisions based on automated processes. The number of senior qualified staff is reduced, along with the effort needed to find and retain them.

The ability to assert data hygiene allows the assertion of Identity Risk at scale. Identity Risk is the ability to determine that an identity (which might be an identity you have never seen before such as a new customer) and its behaviors are permitted to perform a transaction within the accepted risk of a business context. These business contexts are ones in which the business considers the security risk to be acceptable, such as a small risk performed by a large customer (a large source of revenue). This application of business security identity risk means that the security insights derived from Zero Trust are business relevant. The business-relevance of these security insights bridges the traditional difference between Chief-of-Information-Security (CISO)-type risk (based on prevention) and Chief-Risk-Officer (CRO)-type risk (based on revenue enablement). In this way, the application of Zero Trust Risk Insights opens the door for CISOs to elevate themselves to Board-level visibility.

In a data hygiene program, costs go down when you store and process less information of a higher quality. Data hygiene improvements benefit from more accurate identity signals (business context "stories"). With better signals, less information is necessary to make decisions of similar accuracy to those made using substantial amounts of less accurate data. These decisions are also made more quickly and require less (or no) human oversight. When Zero Trust risk insights are used, enterprise cloud costs go down for both processing costs and storage costs. Additionally, these reduce cloud network load, meaning less hardware is necessary and capital expenditures (CAPEX) are reduced.

With data that is both cleaner and rigorously controlled, a class of otherwise undetectable attacks can be prevented. A group these is called Decision Contamination. These use gaps in data control ("dirty data") to manipulate outcomes. Examples of these include fraud, low-and-slow attacks, boiling-the-frog attacks, telemetry contamination, initial subscription frauds, roaming attacks, insider threats, executive flight risk, and others.

While decisions involving dirty data can be manipulated, with enough dirty data even Board-level decisions can be manipulated in nearly undetectable ways for years at a time.

Applications of Zero Trust include Attack Surface Mapping (ASM). These ASM cases could be thought of as any of the following:

1. *Hit.* This requires quickly calculating a cyberattack "hit" (how bad are we hurt?).
2. *Near miss.* If we were hit, how bad could it have been? Should we add this to our plan?
3. *High impact.* This means identifying the top 10 risks for investment planning.
4. *Prediction.* This means proactive risk mapping for new business cases (if we do this, how badly could it hurt if we are hit?).
5. *ASM scanning.* Out of all the potential attack surfaces now and in the measurable future, which are the ones we need to navigate around?

Decision Contamination prevention (when executed in a Zero Trust deployment) can be applied to entire classes of business and business enablers as means of increasing automation potential and reducing cloud costs. As confidence rises in the use of Attack Surface Management, more services can be automated, outsourced, and or offshored with associated cost reductions. Securing decisions is one means of protecting the emerging technology called *Semantic Computing*, a 6G-era technology reliant on extremely scalable automation and operationalized AI. AI is of course especially vulnerable to manipulation through decision contamination as it is incapable of human judgement.

As an example, some uses of Zero Trust prevention of decision contamination could include:

1. Supply chain security tied to vendor risk management and/or government software bill of materials (SBOM)
2. Reduced manipulation of boards of directors via falsified data
3. Leveraging Identity Federation Alliances and cost reduction partnerships
4. Omnichannel and next-generation retail effects on reduced Cart Abandonment
5. Procurement – Vendor Comparison and "virtual bakeoff," Vendor Consolidation
6. Data sovereignty – Dynamic rules for autonomous vehicle cross-border travel
7. 6G telecommunication and Zero Trust
8. Election tampering prevention and tracking
9. National identity and federated services
10. Autonomous vehicle security and fleet management

As the sophistication of state- and near-state level attacks escalates and cost of these attacks falls, smaller and smaller threat actor groups can mount state-level attacks from within the internal supply chain (e.g., work from home) or pose as secure vendor components. Zero Trust is a way to achieve enterprise attack surface visibility capable of seeing the entire scope of a multifront attack.

A Note to Executives and Boards of Directors

These requirements will be eased by the adoption of Zero Trust through the enterprise. In fact, Zero Trust is well-suited to making these complex reporting and compliance requirements into a simple, automated risk scorecard-type report combined with deeply improved insights.

When executives make shareholder-facing statements, including statements made to the public, the accuracy of these statements must be unassailably correct. Historically, the accuracy of these statements was based on the quality of executive oversight and therefore trust in the integrity of data used in reporting.

This trust is increasingly misplaced.

As the sophistication of data-level security breaches escalates, the accuracy of financial reporting is limited by the quality of the data the reports are based on, which in turn is limited by the quality of information security. This security assures the integrity of both financial records and the activities they attempt to measure. Ensuring this end-to-end integrity is a type of executive responsibility called "Fiduciary Duty." Information security is a critical requirement of being able to meet the demands of fiduciary duty. Failure to credibly assert fiduciary responsibility is itself "Breach of Fiduciary Duty," considered a type of fraud in some jurisdictions.

Many countries have recognized that this integrity is bound to their nation's economic health and therefore national security.

For these reasons, the USA Biden Administration has formed a board (the Cyber Safety Review Board) composed of senators and private industry, probing the information security failures of large organizations and their leadership. This board accountability is a template for other countries to follow.

The relationship of supply chain security and national security is of international effect but has a national impact. An example of this is a malware outbreak affecting the world yet having profound impact on many individual corporations and governments. Governments have begun addressing this supply chain issue as a combination of corporate governance (relying on Zero Trust insights) and supply chain governance (also using Zero Trust attack surface mapping). Zero Trust Architecture is then the binding force between executive responsibility and basing their governance efforts on good supply chain security outcomes.

To address these issues in a dynamic way, the US government is using its buying power to improve companies (and their products) that would like to be government suppliers. USA President Joe Biden has signed a Presidential Executive Order requiring vendors to the US government to have a Zero Trust plan in place in support of a supply chain "nested inventory" called an SBOM. Entities that cannot describe their Zero Trust compliance as well as a nested SBOM inventory of software components cannot sell to the US government, or to their in-scope vendors, or their in-scope vendors, and so on. Rippling from the center out, suppliers will require their suppliers to improve their security posture. Since the corporations of many countries sell to the US government and their suppliers, these requirements roll out across borders as well.[1]

The significance of this change is clear to many world leaders. On May 24, 2022, the leaders of Japan, India, USA, and Australia declared their alignment with many of these principles:

> "To deliver on the Quad Leaders' vision for a free and open Indo-Pacific, we commit to improving the defense of our nations' critical infrastructure by sharing threat information, identifying and evaluating potential risks in supply chains for digitally enabled products and services, and aligning baseline software security standards for government procurement, leveraging our collective purchasing power to improve the broader software development ecosystem so that all users can benefit."[2]

By requiring suppliers to have a Zero Trust plan in place, the opportunity to detect practical attacks inside a network or a supply chain is both much greater, and the business impact of responding to these risks is much lower.

In effect, the ability of executives to assert that they have done an excellent job is being explicitly bound to good information security through the supply chain. Zero Trust in supply chain management, network management, and vendor management then is a means of asserting fiduciary duty.

Soon, the US Securities Exchange Commission (SEC) will review a proposal for board oversight and reporting of information security events. The proposal requires reporting of cybersecurity expertise on their board of directors. It also requires board-level shareholder reporting within *four days* of material security events. This reporting to shareholders will have a predictable effect on share price.

If approved, compliance with the proposed SEC security reporting will have monumental effects on boards of directors. Cybersecurity risk and strategy becomes immediately a persistent board-level issue, with board cybersecurity expertise being coveted. CISOs then have a permanent seat at the table, bringing mandated skills to every board agenda.

These requirements will be eased by the adoption of Zero Trust through the enterprise. In fact, Zero Trust is well-suited to making these complex reporting and compliance requirements a simple, automated risk scorecard-type report combined with deeply improved insights.

1. Strategic Overview

This paper is a forward-looking, exploratory paper that highlights the distinct aspects of Zero Trust. While other papers focus on technology, this paper focuses on the use and value of that technology, focusing on the "why" rather than the "how" of Zero Trust. Given the nature of the piece, this paper can be considered a thought leadership piece for possible use in executive planning, rather than a landscape review of the current state of the industry or a product-centered pitch.

Much of information security today relies on old concepts. A novel approach to containing the damage caused to enterprises is called Zero Trust. This is a new level of maturity in information security, binding security results to improved risk-based decision making supported by Zero Trust Architecture (ZTA).

Four recommendations are described in this paper.

- Changes to executive responsibility and board governance that require the adoption of ZTA
- New government and customer requirements for Supply Chain resiliency, using ZTA
- Use of Zero Trust tools such as operational risk management automation to ease security management, reducing both enterprise risk and the total cost of ownership (TCO) of security
- Use of the simplification effect ZTA has on security management to reduce reliance on difficult-to-retain senior security staff. In turn, this reduces the security skills gap by being able to rely on junior staff and/or offshore staff for even complex incident triage.

While most Zero Trust messages describe it as "never trust, always verify," a better description is "Guilty until proven innocent." All users, devices, and transactions are always considered suspect. There is no trusted safe haven in which a hacker or fraudster can hide from the network's probing eye. By trusting zero entities, transactions, devices, or users, there is no perimeter to get through. There is no hacker saying, "I'm in," because there is no "in."

Instead of perimeters, continuous risk assessment is used to determine the delay imposed on access to resources (called "friction").

Maximum risk means blocking.

Elevated risk means reduced access to resources.

Low risk means full access with monitoring.

There is only more risk or less risk; there is no state of blind trust.

Unlike a traditional trust environment, Zero Trust security context allows security decisions to be more fine-grained than the traditional “block/don’t block” state of either too much security or not enough.

If Zero Trust is implemented correctly, it will not impede business but will reduce cost and risk. In this way, the real drivers of security (money and resources) are served.[3]

1.1 What is ZTA?

Zero Trust Architecture (ZTA) is an enterprise architecture approach for implementing Zero Trust complex business requirements such as operational identity risk management.

This operational risk created by security can be reduced to a minimum level by applying risk context (Zero Trust risk insights) to the security response.

Normally this context is applied because of human judgement, requiring manual processes that defeat the purpose of security automation. Zero Trust does much to correct that, improving the quality of data used in automated response. This creates new opportunities for expensive and difficult-to-hire security personnel to stop repetitive tasks and go back to doing more business-relevant valuable tasks requiring human judgement.

The combination of attack surface discovery, risk assessment, and risk mitigation are used to create these risk insights. Gartner calls this combination Cyber Asset Attack Surface Management (CAASM).

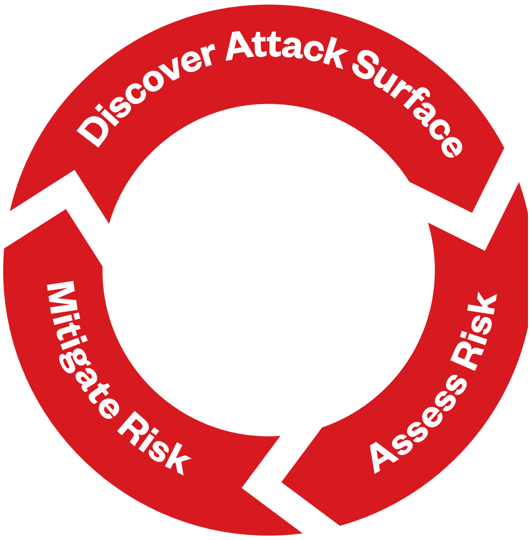

Figure 1. The risk management life cycle

This context-driven approach to reducing the risk created by security can decrease the total actual cost of security, which includes cost of the security product plus its operational and revenue impact. The impact of security can then be further reduced with the use of micro-segmentation to “reduce the blast radius” of security as described in Section 1.2. below.[4]

In applying operationalized risk management to security, security effort can be matched to the value of the asset as closely as possible. The closer the security response is to the risk of the asset, the less the unnecessary cost (risk) the security action will have.

1.2 Reducing the Blast Radius of Security Response

Security is itself a risk, and (pre-Zero Trust) security creates costs by doing its job in a traditional, blunt way that ignores context. An example is that mission-critical functions such as those in a smart factory might be interrupted by non-Zero-Trust security with immediate impact of millions of dollars per minute. Yet another example is of non-Zero-Trust security blocking life-critical telecom or hospital networks, with immediate impact on human life.

When Zero Trust security context is recognized and responded to, the output of the security action is much more accurate *while addressing business priorities* such as revenue, life criticality, and/or mission criticality. What this means is that when business risk priorities are added to systems such as Zero Trust that handle security risk, in effect the Zero Trust system is actually enforcing *business risk reduction through security risk reduction*. This is a profound improvement to traditional security models.

This can be automated by translating the business process algorithms into security process algorithms such as policy enforcement. Business context is then security context. Revenue impact (see Section 1.3 below) can then be built into security response, such as using a “block” response when there will be low revenue impact and a “monitor” when a security response will have high-revenue impact.

With the ability to adopt business priorities into security response, security systems with traditionally high security risk move from being cost centers to actually reducing cost.

1.3 Granularity of Response and Reduction of Security Business Impact

Inaccurate or overactive security is itself a risk and minimizing the scope of an effective security response reduces its negative consequence. By making a security response as accurate and as “tuned” as possible to the specific security context of the incident, the cost of security revenue impact (in the form of blocking and security-generated outages) is reduced. Security impact on business is reduced.

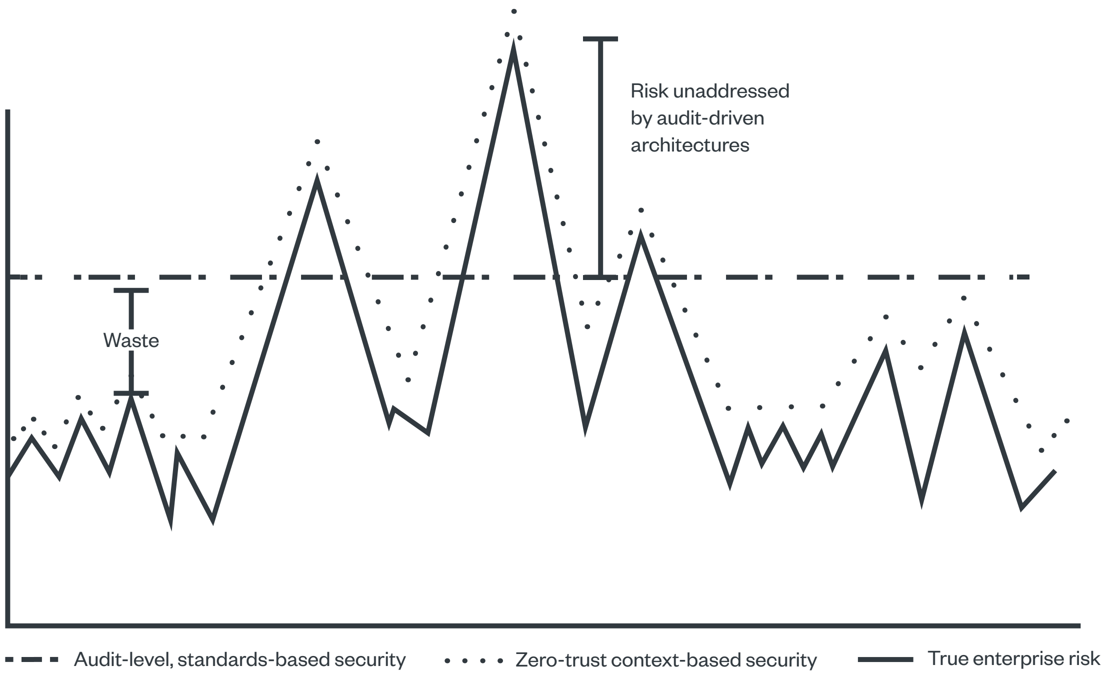

Figure 2. Zero Trust is a means of applying context (risk) to traditional information security.

Additionally, when security telemetry that incident response is based on is made as accurate as possible using context-driven security insights, the response both occurs more quickly and resolved sooner for an overall reduction in total business impact.

This cost reduction can be further reduced using micro-perimeterization, another means of limiting the spread of security incidents.

1.4 Security as Business Enabler

By using security context to adapt to real-world and near-real-time risk, an organization's security posture can dynamically respond to individual large-scale risks (such as supply chain risks) as well as reduce the effect of numerous threats with similar effects (managing risks rather than vulnerabilities). This context-driven risk approach also allows innovative approaches in cost reduction such as fraud risk management at scale across technical domains, management of regulatory risks across jurisdictions (such as privacy and data sovereignty), and even location-dependent risks determined by wireless networks (such as roaming and nomadic networks).[5]

These combined approaches can evolve into use cases for which security reduces risk in supply chain (SBOM), reduces costs in vendor management and addresses the strategic costs of vendor sprawl. Additionally, Zero Trust security improvements for asset inventory accelerate incident response and therefore lessen the impact of security compromise.

2. How Zero Trust Helps Your Organization

Zero Trust is a way to seek and destroy shadow IT and other inefficiencies. It is a way to reduce cost (both OPEX and CAPEX) and therefore enterprise risk. It cleans up enterprise data (data hygiene) by finding systems that are producing higher-than-average data risk. It enables revenue by both reducing the risk of brand-impacting and customer-facing, security-originated outages like blocking critical customer functions such as Operational Technology factory robots. It allows fine-grained control over things like roaming and data sovereignty.

Zero Trust allows many business functions to use a single access method, both improving security and reducing the effort required by a customer to complete a sale.

Zero Trust can also be leveraged in many other use cases, a few of which can be seen in the appendices of this paper.

2.1 Why Attack Surface Mapping is Important to Secure Your Supply Chain

Zero Trust can be considered a means of identifying revenue-impacting chains of vulnerability in the enterprise. Some of these might seem of small impact in isolation, but they have an escalating effect farther down the supply chain that might result in Cascade Failure (one thing breaks another, in series).

These chains can be business processes (representing revenue and therefore business impact), security processes (representing risk and safety), and supply chains (representing risk and revenue). The collection of all these chains are called the attack surface.

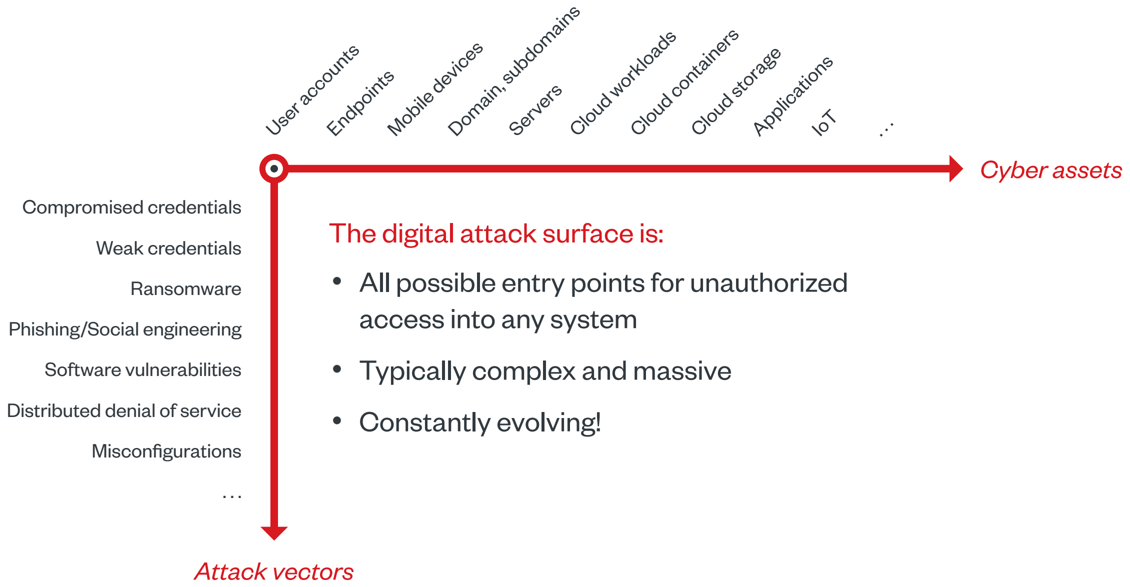

Figure 3. The digital attack surface

During recent high-impact global breaches, the revenue-generating value chain and the risk-generating kill chain are often identical. Supply chains cross multiple vendors and processes, and kill chains represent their own supply chains. Effective supply chain management using Zero Trust is a big step toward proactively finding and breaking potential kill chains. Conforming to the National Security Agency-Defense Information Systems Agency (NSA-DISA) version of Zero Trust in support of an SBOM is a method of moving forward with this. Not only can potential attack surface risk be identified, but the effect of cyberattack near misses can be identified as well.

The European Parliament defines a cyberattack that is a “near miss” as an event which could have compromised the availability, authenticity, integrity of confidentiality of data, or could have caused harm, but was successfully prevented from producing their negative impact.[6]

A comprehensive approach to handling supply-chain-as-kill-chain is Cyber Asset Attack Surface Mapping (CAASM). Using Attack Surface Mapping or CAASM, current, potential, and “near-miss” supply chain attacks can be scanned for (“Kill Chain Mapping”) and preemptively mitigated.

2.2 Supply Chain Attacks and Near Misses

Unplanned gaps in supply chains (whether for data or goods) are normally revenue-impacting. These can include data supply chains such as network or application connectivity. Reducing risk in a live network, detecting cyberattack near-misses, procuring low-risk products in a supply chain, or identifying the risk in an existing supply chain, are all Zero Trust use cases crossing the security perimeter of the enterprise. (See Appendix for more examples of these).

Examples of Supply Chain attack modeling can be found on the MITRE ATT&CK® page on "Supply Chain Compromise," which states that "Adversaries may manipulate software dependencies and development tools prior to receipt by a final consumer for the purpose of data or system compromise."[7] On the page on "Supply Chain Compromise: Compromise Software Dependencies and Development Tools," it also states that "Applications often depend on external software to function properly. Popular open-source projects that are used as dependencies in many applications may be targeted as a means to add malicious code to users of the dependency."[8] Additionally, "Targeting may be specific to a desired victim set or may be distributed to a broad set of consumers but only move on to additional tactics on specific victims."[9]

Examples of digital supply chain attacks include Cryptolocker[10], Petya/NotPetya[11], the SolarWinds[12] attack, and more recently Log4J[13] supply chain attacks. These by their nature break the business model of the victim enterprise and can cost millions or tens of millions of dollars per hour.

In Zero Trust deployments, the continuous assessment of an inventory of data assets is compared to known and emerging threats. Anywhere or any time there is overlap (for instance with known or emergent CVEs aka Common Vulnerabilities and Exposures), an alert is triggered. This continuous assessment can identify the presence of high-risk vendor modules in your infrastructure immediately, once the risk is known. These can then be de-risked, or otherwise subject to context-driven security decisions such as risk acceptance, throttling, investigation/intelligence monitoring, or other revenue-respecting choices that non-Zero-Trust options cannot capture.

2.3 Biden Executive Order: Zero Trust and SBOM

Recently, the Biden administration issued a Presidential Executive Order. This was later supported with updated requirements, which are expected to be updated again to raise the lowest common denominator security across the US government.

As the US Federal Government enforces this requirement on its suppliers, they will in turn enforce it on their suppliers, and this requirement for Zero Trust and SBOM will ripple throughout the portion of the supply chain serving the US.[14]

By requiring suppliers to have a Zero Trust plan in place, the opportunity to detect practical attacks inside a network or a supply chain is both much greater, and the business impact of responding to these risks is much lower.

In effect, the ability of executives to assert they have done an excellent job is being explicitly bound to good information security through the supply chain. Zero Trust in supply chain management, network management, and vendor management is a means of asserting fiduciary duty.

2.4 Software Bill of Materials (SBOM)

A Software Bill of Materials is a nested inventory of all the software products, their components, and their vendors, across the enterprise. The Biden Executive Order's intent is that vendors provide this to their customers for inclusion in a tool for relating vulnerabilities with at-risk supply chain components. This nested inventory can then be compared to known and emerging vulnerabilities in those components to provide an alertable risk level across all enterprise systems.[15]

When a pattern of activity occurs that might be malicious, detecting it is based on part in knowing the difference between what *should* be happening to your information and software inventory and *what actually is* happening to your information and software inventory.

To do this quickly, you need to have made an inventory of all of the software bills of materials of all the software assets in your enterprise, whether internal or vendor supplied. Since you might have vendors providing parts of your enterprise services, this inventory must contain references to individual vendor components as well as products and services.

This nested inventory (also called a Component Index) is much sought after by incident responders, as it can include contact information, what level of exposure is present in which system, and can be used to create a mapping of the risk represented by the presence of an exploited/exploitable product component. When this information is not readily available, incident responders need time to look for it, which extends the duration, cost, impact, and risk of an incident.

Effective risk management across a multivendor environment with multiple risk profiles is impractical to perform manually at scale. When this is combined with component obsolescence/patching and increasing time investment from hackers, the need for an automated risk management system like Zero Trust is a necessity.

2.5 Zero Trust in USA – DISA NSA vs. NIST

There are several approaches to Zero Trust, one being described by NIST, and another by the DISA NSA Zero Trust Reference Architecture.

There is a relationship between the history and background of Zero Trust and the guidelines that have been recently been made for Zero Trust. The NIST Zero Trust guideline has been published by NIST and many ZTA vendor products were quickly aligned to it with varying degrees of success. Since then, the Biden administration has asserted a Presidential Order that suppliers to the US Federal Government must have a Zero Trust plan. This was later further clarified to assert that the Zero Trust plan should be compliant with the DISA-NSA Zero Trust Reference Architecture, a mature data-centric security architecture document.

The two separate approaches are each best used for different infrastructure security and business risk requirements. The DISA NSA approach is most suited for large critical infrastructure entities, while the standalone NIST approach is most suited for raising the security level of entities closer to the beginning of their security maturity journey.

The NIST approach is an excellent foundation. The DISA-NSA approach is a complementary design element that improves the accuracy of Zero Trust risk management while reducing the cost of infrastructure.

2.6 Zero Trust in USA, Japan, Australia, and India to Be Harmonized

The common drivers behind the USA NSA-DISA Zero Trust approach resonate with the leaders of many countries. The leaders of four countries, Prime Minister Anthony Albanese of Australia, Prime Minister Narendra Modi of India, Prime Minister Fumio Kishida of Japan, and President Joe Biden of the United States came together on May 24, 2022, to issue the following statement:

> "…Improving the defense of our nations' critical infrastructure by sharing threat information, identifying and evaluating potential risks in supply chains for digitally enabled products and services, and aligning baseline software security standards for government procurement, leveraging our collective purchasing power to improve the broader software development ecosystem so that all users can benefit."[16]

While a North American-centric approach to ZTA will emphasize data supply chain integrity issues (assigning responsibility and liability), the Japanese approach seems to center on reducing the consequence of a security incident (impact reduction). Micro-segmentation is a means of "reducing the blast radius" of security events to a smaller segment. Also called micro-perimeterization, this is a means of reducing risk by reducing the spread of infection (if malware) or lateral movement (if a hacker). It is too early to tell if the Japanese approach re-themes into alignment with the American approach after the Quad-Leaders Joint Statement.

2.7 Supply Chain Assurance in the European Union

In the European Union, there is growing legislative support for the adoption of Zero Trust. According to one proposal, strong IT security management, a commitment to adopting a Zero Trust architecture and a strengthened staff cybersecurity awareness program will increase resilience to cyber threats.[17]

Additionally, two policies must be promoted. One policy should promote cybersecurity for subject matter experts (SMEs), consider their needs, and give them both guidance and support, including any guidelines for facing supply chain issues. The other must be a policy that promotes "cyber hygiene" to make up a "baseline set of practices and controls."[18]

These three statements contribute to the same scope profile as the Quad-Leaders Joint Statement and the NSA-DISA ZTA approach.

2.8 China and Supply Chain Assurance Legislation

The Cyberspace Administration of China (CAC) released a draft of the cross-border data transfer agreement called the SCC.[19] This document has an overlap in effect but not scope with the other Zero Trust themes in this paper. In effect, many of these national themes of Zero Trust legislation are deployed not as supply chain security but as privacy legislation. This is a novel approach as Chinese programs for the deployment of national security through National Identity are mature.

By deploying a deeply identity-based version of supply chain security at a national scale, the Chinese deployment of national identity can be used as an extremely dynamic and versatile application of Zero Trust.

A unified USA, NSA, DISA, and SBOM approach is extremely centralized and an entire nation’s identifiable vendors can be cut from US supply chains quickly. In the Chinese approach (heavily reliant on identity, sidechains, and SIM (Subscriber Identity Module) cards, there is an alternative supply chain security approach that could be far faster and effective than the USA-themed approach. A person could speculate that the entire supply chain in 5G/6G would have more in common with a fast-flux botnet than a traditional list-based supply chain security approach. Automated supply chain attacks could defeat the USA NSA DISA approach by being faster than the chain of bureaucratic approvals necessary to block an extremely dynamic attack.

2.9 Complexity as Security Risk

Complexity is a kind of chaos. One of the central themes of supply chain risk is that executives experience one or more of the three risks of architecture sprawl, vendor sprawl, technical debt, and unknown supply chain dependencies. Each of these classes of inefficiency increases the complexity of a revenue-generating technology deployment and therefore increases the likelihood of security breach due to inconsistently enforced security architecture controls. These inefficiencies represent a kind of “noise.”

If an organization makes enough “noise” it is sure to attract “predators.”

Each of these sub-topics can be corrected by a mature Zero Trust deployment. Each has a slightly different theme that bears more explanation.

Architecture Sprawl and Technical Debt

Architecture Sprawl is the concept that planning rigor decreases the "farther" from central planning and enforcement a system is in terms of time, space, logic, business hierarchy, or other dimensions. This means that the cost-reduction capabilities of Enterprise Architecture become less and less effective (more expensive) the less they are enforced. Technical debt is a related concept in which planning activities are "put off until tomorrow," meaning that the effort to fix an architectural problem will become more complex and more expensive the longer the technical debt goes unfixed. Both risks center on not doing enough coordinated and enforced security architecture planning upfront. ZTA highlights these risks by drawing attention to areas of consistent security risk in the enterprise.

Vendor Sprawl and Unknown Supply Chain Dependencies

This is yet another related concept in which multiple vendors are responsible for managing their own cost and complexity. These costs and complexities might be managed effectively by some or all vendors, but these are unlikely to be coordinated across multiple vendors (the customer does not know what is happening within each vendor). Vendor sprawl is amplified by architecture sprawl and technical debt. As a result, the security architecture is inconsistently enforced across vendors. With inconsistent vendor security risk management, Supply Chain dependency and risk will also be unknown. This is highlighted using combined ZTA and SBOM in that high-risk vendors will show up repeatedly in ZTA security risk reports due to SBOM reporting.

Identity Sprawl and Supply Chain Contamination

Identity is a complex topic that many organizations struggle with, in part because even the word "identity" is often used inconsistently/inaccurately within an enterprise. When identity is handled well, it can make the same functions far less expensive due to working as a filter, reducing the amount of data (and types of data) required to make highly automated decisions.

When it comes to identity, *less is more*.

With a well-functioning identity enterprise data architecture, the enterprise's data hygiene will improve, the total amount of data stored and processed by the enterprise will be less, and the enterprise's cloud storage and processing OPEX costs will decline. When identity is not defined at the Enterprise Architecture or Business Architecture levels of planning, it causes the enterprise to require much larger amounts of data, processing, and human judgement to make the same decisions. These decisions are also likely to be less accurate since identity design inconsistencies (aka identity sprawl) allow multiple systems to apply different meanings to the same identifiers. When multiple meanings are applied to a single identifier in a single system, those systems suffer *semantic contamination*, reducing the data quality of the entire system and all dependent systems.

An example of such is Customer_Date, which seems like simple application-level identifier. In an enterprise with poor identity data hygiene (a lot of "dirty" identity data), it might have different meanings as shown below. If all of these are placed in the same system, it will be difficult to interpret the amount of semantic contamination in the system's output.

System type	Identifier	"Dirty" meaning	Consequence
System One (Retail billing system)	Customer_Date	The day of customer onboarding	No indication of current value as a customer
System Two (Retail marketing communications system)	Customer_Date	Day marketing mailout sent (instances of the same customer across multiple campaigns)	There are multiple instances that could be used in decision support — One? Some? None?
System Three (Corporate security fraud department)	Customer_Date	The day the customer was permanently blocked for performing massive fraud	Potential for decisions weighted toward high-risk and criminal customers

Table 1. Different types of systems with the Customer_Date identifier and their meanings

Identifiers such as Customer_ID, Customer_Address, System_ID, Phone_Number, and any other sources of identifier can lead to decision contamination when any of the systems have poor data hygiene, and their information enters a common system.

The consequences of this semantic contamination then carry throughout all dependent systems in both the internal and external data supply chain.

The data improvements involved in Zero Trust Architecture include harmonization and federation of identity and identity components, which involves assuring that all identity components and their identifiers have common meaning across systems (identity federation and semantic integrity).

Decision Contamination and Zero Trust Data Hygiene

When semantic contamination has occurred in systems responsible for decision support, the decisions themselves are contaminated. This is a source of inefficiency, impaired automation, and executive misjudgment based on flawed data. This can also be manipulated maliciously by a variety of data contamination attacks. These attacks include fraud, business process compromise, and low-and-slow or boiling-the-frog attacks.

The process of adopting Zero Trust Architecture tends to improve an enterprise's Data Hygiene. High-quality data is heavily qualified and filtered before being introduced into a system. It is checked not just for formatting, but ensuring the meanings of data field identifiers have the same semantic meaning. This is a critical element of supporting accurate decisions.

All decisions made using “dirty data” result in poor decision support and inconsistent results.

2.10 Identity Improvements and Zero Trust

2.10.1 Maintaining Context Across Untrusted Networks

Zero Trust (especially the DISA definition of Zero Trust) relies extremely heavily on a deep understanding of identity. The DISA definition of Zero Trust is the root of Biden’s Executive Order requiring Zero Trust and supply chain security (SBOM). This includes the ability to maintain security context even across untrusted networks, such as when a car or phone moves from network to network (roaming), a laptop is connected to unfamiliar Wi-Fi (called “Nomadic”), or when a customer is new (perimeterless omnichannel). Alignment with this makes customer interaction relatively frictionless, easing the ability to acquire and monetize new customers. For these reasons, Zero Trust is a core element of 6G telecom.

Telecom companies and government entities have a high demand for securing their Data, Assets, Applications, and Services (DAAS) in a coherent and end-to-end way capable of addressing attacks by peer and near-peer state adversaries. This DISA-NSA version of Zero Trust is a response to the arrival of the next-generation advanced persistent threat (APT) attacks by state actors on the data of internal and external supply chains rather than crossing the perimeters of alarm-laden systems. Zero Trust, when deployed this way, can then catch the business process compromises intelligence officers are famous for. Other kinds of Zero Trust deployments such as application-centric approaches common in the market today do not have the deep understanding of operationalized identity to do this.

2.10.2 Leveraging Identity Federation Alliances and Cost Reduction Partnerships

The concept of Identity Federation from a source like the FIDO2 Alliance[20] is a strong option. The ability to harmonize the identities of both enterprise and non-enterprise entities, internal and vendor entities, known and unknown subscribers, and on-site and off-site employees is powerful. Additionally, since multiple organizations use FIDO2, use of this option harmonizes your identities across not only your own systems but also with those of your potential customers who are also FIDO2-harmonized. This cross-federation of FIDO2 members in each other’s supply chain reduces costs for each. The use of FIDO2 makes your identities portable into and interoperable with the systems of other members of the Alliance, and therefore other members might see your enterprise as a more valid partner or supplier. FIDO2 membership then becomes a business enabler.

2.10.3 Omnichannel, Perimeterless Networks, and Reducing Cart Abandonment

Due to cost and scalability, the adoption of several approaches of customer security is becoming popular. The two types of improvement are omnichannel (customer interface and systems reuse) and perimeterless networks (near-frictionless customer onboarding).

When these two are combined in a Zero Trust environment, it has the effect of reducing Cart Abandonment, a large source of risk in retail sectors that includes everything from online retail to online mortgage applications.

Cart Abandonment

Cart Abandonment relates to the retail "shopping cart" in which purchases are collected prior to being paid for. In the case of new customers (arguably the best kind of customer), a source of cart abandonment comes from the frustration a new customer feels at spending time assembling their order (their cart) and then being subjected to a lengthy and cumbersome enrollment process.

Next-Generation Retail and Omnichannel

With the adoption of omnichannel principles (which Zero Trust is thoroughly aligned to) the enrollment can be done once for any product or service provided by the enterprise. Since in both Omnichannel and Zero Trust common identifiers are both shared and harmonized (federated), enrolling in one service a single time means the customer has effectively enrolled in all services. This works epically well when combined with the concept of perimeterless networks.

Perimeterless Networks

In omnichannel, there is the concept of one-time enrollment. In perimeterless networks, the deep identity-risk based surveillance performed can be combined with the risk posed by the enrolled person's attempted activity and how much surveillance has been done already (the person's effective reputation).

If an enrolled person is attempting a purchase of the same low-risk items (groceries for instance) from the same device, location, delivery address, and billing information, there is negligible risk benefit in asking that person for a password as anything but transaction integrity. If the same person (about which you have the same information) attempts to also buy a lawnmower (shipped to the same delivery address), the additional process might only be a photo of the delivery taken by the delivery person to attach a point-in-time to the delivery. This additional step is not to reduce the risk represented by the customer, but the risk represented by the delivery process. The customer has no incentive in this case to abandon his cart because from their point of view the enrollment was transparently identical even though the value of the delivery might have multiplied by three or four times. By reducing the risk-increasing likelihood of cart abandonment, the total overall risk of the transaction goes down to the point where even an expensive lawnmower can be delivered transparently. The increased total revenue of the transaction and increased overall total average revenue across all customers is the Zero Trust Next-Generation Retail win.

2.11 Zero Trust as Internal Registry

Zero Trust has several valuable traits. As an internal registry of software components, it can be a "sole source of truth," managing the integrity of the entire enterprise software deployment. It is an excellent method of detecting shadow IT as well as providing Zero Trust risk insight into the effectiveness (and therefore cost effectiveness) of the enterprise software deployment.

Organizational complexity and the risk represented by it can be mapped using a Software ID (SWID) registry, with an associated security risk and a supply chain risk attached to the registry as security context. This context can be described as security risk insights.

Context-driven security risk insights can be used to greatly reduce the negative impact of obstructive security controls.

Internally developed systems can be a source of risk as both their support cost and obsolescence increase. Zero Trust risk reporting can be used to detect and alert on unacceptable risk, producing prioritized lists of security products with decreasing effectiveness, as well as identifying potential security vendors on whom vendor consolidation efforts can be focused.

2.12 SBOM Vendor Registry and Regulatory Compliance

Auditable and accountable Zero Trust systems can provide easily obtainable evidence of compliance with SBOM, security regulations, and/or industrial audit controls such as the Payment Card Industry Data Security Standard (PCI-DSS). Externally developed systems (including security systems) can be alerted on as sources of risk, but when vendor products are involved, risk can be broken out by vendors. This security vendor risk approach identifies the value presented by each security vendor and allows easy comparison to identify which vendor is the most effective.

Regulatory law technology (RegTech) is an emerging area of great interest. The larger an organization is, the more likely it is to be heavily audited and regulated. The ability to treat supply chain risk and regulatory risk as alertable security risks is an excellent way to reduce the likelihood of multimillion dollar regulatory fines, contract-impacting audit exceptions (failures), and breakdowns in data sovereignty. In effect, applicable rules in standards, regulations, and laws are turned into alertable security requirements.

An important note is that a shareable evidence-grade report greatly reduces evidence, audit, and compliance efforts. It also reduces the chance of auditors “interviewing the new guy” and arriving at unpredictable results. This use of consistent reports allows an enterprise to enter the audit process with confidence in the outcome.

2.13 Vendor Risk Management and the SBOM Vendor Registry

When comparing security vendors using Zero Trust risk insights, the least effective security vendors of a particular type can be identified and replaced with the most effective security vendors of that type. In this way, not only does the enterprise security risk decrease (by having better results), but more licensing volume can be bought from a smaller number of vendors (vendor consolidation). This “bulk discount” vendor consolidation approach reduces the total risk of enterprise security while reducing complexity and cost.

3. Risk Management of Human and Machine Identity

Zero Trust security context applies security response based on risk. This risk-based response is a more business-friendly and business-relevant approach that reduces the negative business impact that traditional security responses have.

All security functions come down to identity. "*Who did what to what, when*" is a generic security statement that includes no less than four identity clauses. The accuracy and integrity of this identity statement is dependent on the accuracy and integrity of each of the individual identity clauses in those statements. The accuracy and integrity of the risk represented by the overall statement is based on the overall integrity and accuracy of the entire statement. If every identity clause is accurate, the entirety can be automated with high confidence in the outcomes of the automated risk management process.

A core part of both risk management and asset management centers on identity. Without the ability to identify the difference between assets and/or the difference between those accessing them, there can be no assurance of secure transaction or storage.

Much of modern technical security is based on a decades-old "operator" role. The assumptions of this role came from the concept that a human operator was responsible for all the decisions made by a machine, in the form of responsibility (assigned by giving the operator a metal key) for all the knobs and buttons on an operator's console. A machine was originally incapable of action without a human operator.

This has become increasingly inaccurate over time. Humans and our accounts are often the target of most security detection and enforcement activity, but in the era of computers these accounts do not measure humans. They only measure the activity of the machine that a supposed human was operating. The operator model has increasingly become a design fiction.

The opportunity in a Zero Trust deployment is to accept this "machine as proxy human" security context and apply security rules and surveillance to all devices as if they have a human at the keyboard using a stolen password, or as if malware (or a living hacker) has compromised the machine.

This approach of treating all accounts (human or not) as machine/service accounts creates a lot of architectural flexibility — everything can be treated in a similar fashion whether an unknown device, an unknown user, an unknown network, a known device, a known user, a known network, or any combination regardless how often these change.

This machine-human approach does, however, require harmonized identity telemetry. In 4G and 5G this is conveniently handled by Subscriber Identity Modules (SIM cards) and a few additional on-card credentials. In this way, a SIM-enabled device like a phone, a robot, an autonomous car, a smart factory, a drone cargo ship, or internet of things (IoT) devices can each be handled with Zero Trust as if they have a malicious human behind them. Surveillance then must watch closely and forever to see what that malice might be (security context) and if it requires security action (risk-based response).

Luckily, these large and expensive enterprise risks described above can be fixed. When implementing Software Bill of Materials in a Zero Trust solution, the methods of identifying software apply equally to internally built and customized systems as well. These uniquely identified systems can be baselined for expected behavior, and unexpected behaviors can be alerted on. The concept of Software ID (SWID)[21] can be applied to both internal and vendor software, creating a supply chain component map that is extremely useful to incident responders and other members of the risk management team.

4. Conclusion and Recommendations

The concept of Zero Trust is one of surveillance. A perimeter-based "castle" system checks identity when the perimeter is crossed. A Zero Trust network checks it continuously, cross references it, assesses behavior risk, compares it to potential losses and revenue.

Throughout this paper a reader will have seen:

- Which changes to executive responsibility and board governance require adoption of ZTA
- Which new government and customer requirements to Supply Chain resiliency, using ZTA
- The use of Zero Trust tools such as operational risk management automation to ease security management, reducing both Enterprise Risk and the Total Cost of Ownership of security
- Use of the simplification effect ZTA has on security management to reduce reliance on difficult-to-retain senior security staff. In turn, this reduces the security skills gap by being able to rely on junior staff and/or offshore staff for even complex incident diagnoses.

The core of Zero Trust surveillance is identity, whose integrity is secured using Zero Trust in a way that asserts maximum enterprise functionality and minimum risk.

Zero Trust bases its access on continuous authentication, which requires identity to be very well-thought out and executed in a very elegant way. This elegant design method is a mature formal design method called Enterprise Data Architecture, with its subset being Enterprise Identity architecture. These mature processes enable cost reduction through infrastructure re-use and reduction of operating effort through reduction of complexity.

As the world becomes less stable due to climate change, age, war, supply chain disruption, and resulting aggressive fierce competition for dwindling resources, a more sophisticated, nuanced, and cost-effective approach to security will help the healthiest organizations survive.

Appendices

Appendix 1

TERMINOLOGY – drawn from NIST 800-30, Guide for Conducting Risk Assessments

Risk – A function of the likelihood of a threat event's occurrence and potential adverse impact should the event occur[22]

Threat – Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. Threat events are caused by threat sources.[23]

Vulnerability – A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most information system vulnerabilities can be associated with security controls that have either not been applied (either intentionally or unintentionally) or have been applied but retain some weakness.[24]

Predisposing Condition – A condition that exists in an organization, a mission or business process, enterprise architecture, information system, or environment, which affects (i.e. increases or decreases) the likelihood that threat events, once initiated, result in adverse effects to organizational operations and assets, individuals, other organizations, or the Nation.[25]

Likelihood of Occurrence – A weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).[26]

Impact – The magnitude of harm that can be expected to result from the consequences of unauthorized access or disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.[27]

Appendix 2 - ZERO TRUST USE CASES

USE CASE A – Supply Chain Improvements – Reverse Antivirus as Zero Trust Software Bill of Materials

Antivirus is a list of *bad* hashes that are *never* allowed to act.

Supply chain assurance could be thought of as a list of *good* hashes that are *only* allowed to act. This supply chain assurance method can be thought of as “reverse antivirus” and is an opportunity to reuse existing infrastructure in a way that can be tied to Zero Trust.

Product Maturity Path. The proposed method is initially a registry of vendor self-attestations of SBOM compliance. This can, however, be matured as an operational method extremely similar to antivirus. As an antivirus-like method, it would be downloadable, updatable, a means of locking-in customer loyalty, a way of up-scoping other security functions, etc.

First-Party Data as treasure. As the operator of a registry of the sort described above, a reverse AV feature would be the Root of Trust for supply chain assurance. In this role, a reverse AV feature would have visibility into the activity of all supply chains for all customers. With the application of machine learning and correlation, the security context for any supply chain element, and therefore, any supply chain transaction, can be derived from payments to shipments.

Synergies and Business Architecture Best Practices. It should be noted that this process is extremely like the Know Your Customer (KYC) process used in the banking and finance sector to address money laundering. KYC is used in the assertion of financial supply chain transaction security in the form of Anti-Money-Laundering (AML) controls. Money laundering is a successful class of supply chain attack in which the provenance (criminality) of a money supplier (criminal) is hidden. Similarly, software vendor supply chain attacks rely on hiding the provenance of the vendor components in a supply chain. Software Supply Chain attacks could be thought of as being hidden using “Data Laundering.” The SBOM-Supply Chain product above would have many synergies with this mature financial supply chain assurance practice, and a SBOM product like KYC AML would meet the requirements of many banking audit standards (driving adoption by the banking industry). KYC can be thought of as “context-driven security.”

Forward-Looking Direction. The relationship of 6G telecom, Zero Trust, Supply Chain Security, finance, and electrical power should not be overlooked. In the 6G era (and in current-day preparation for it) the implementation of Zero Trust is mandatory for several sectors as driven by telecom. The use of perimeter-based blocking behaviors is not scalable in fully adopted 5G, and this can be seen in the 6G requirement for Zero Trust. The scalability of DISA-NSA perimeterless Zero Trust is driven using telecom-like “roaming-style” security context.

Improving Context-based security for improvement of Zero Trust. Insights based on SBOM product can feed back into Zero Trust baselining, improving the context-driven security that Zero Trust of the sort large mature customers require. An example of this large mature model is the NSA-DISA Zero Trust reference architecture.

Vendor Consolidation. Intake SDN Security Orchestration Rules into Zero Trust Risk Engine and scan the vendor space for published vulnerabilities, provide alerts based on security context (i.e., “high” might actually be “low” for you, or the reverse). Products as People = handle as Insider Threats.

An important use case is Zero Trust as Supply Chain Vendor Management of both remote workers and cloud assets. The recent Log4j attack could have been identified early and the risk reduced using a Zero Trust vendor management approach. Supply Chains are typically sources of risk since they involve the "Hidden Terminal Problem" in which you cannot see what is happening on the far side of the closest vendor in the supply chain. A "Vendor's vendor" is invisible to your governance and security practices while still being "trusted" vendor traffic.

A Zero Trust approach to this is to the use of Golden Images[28] verified by repeatable hashes with a vendor's Sidechain[29] Identifier. Sharing subscription access to a global opt-in database of vendors would be a new product opportunity.

A similar approach might be the use of "reverse antivirus" as described above, including SWID as cross references against known vulnerabilities, and alerted on.

USE CASE B – eSIM-Bound National Identity and Data Sovereignty Over a 6G Global Roaming Telecom Network

Recent world events have highlighted issues of nationalism, national instability, and the impact of information operations on a country's population. Several forward-looking nations have been planning for this increasing Cold War-like means of international competition. These countries (including Canada, China, USA, Russia) have begun implementing a Zero-Trust-like model for the Identity-as-a-Service management of their citizens as a means of hardening their nation against these information operations.

In several of these countries Proofs of Concept are underway. In China, the National Identity program is underway in Shenzhen. In the political climate there, it is unnecessary to hide the program (which might be resisted in other countries if more were public). The Chinese national identity program is a very mature and well-thought-out approach which can roll out efficiently despite any potential misgivings of its population. Zero Trust is implemented across both IT and telecom identifiers.

The National Identity program of China is represented here as a supply chain of identity fabric information, using each element in the chain as both an aggregator and a security sensor.

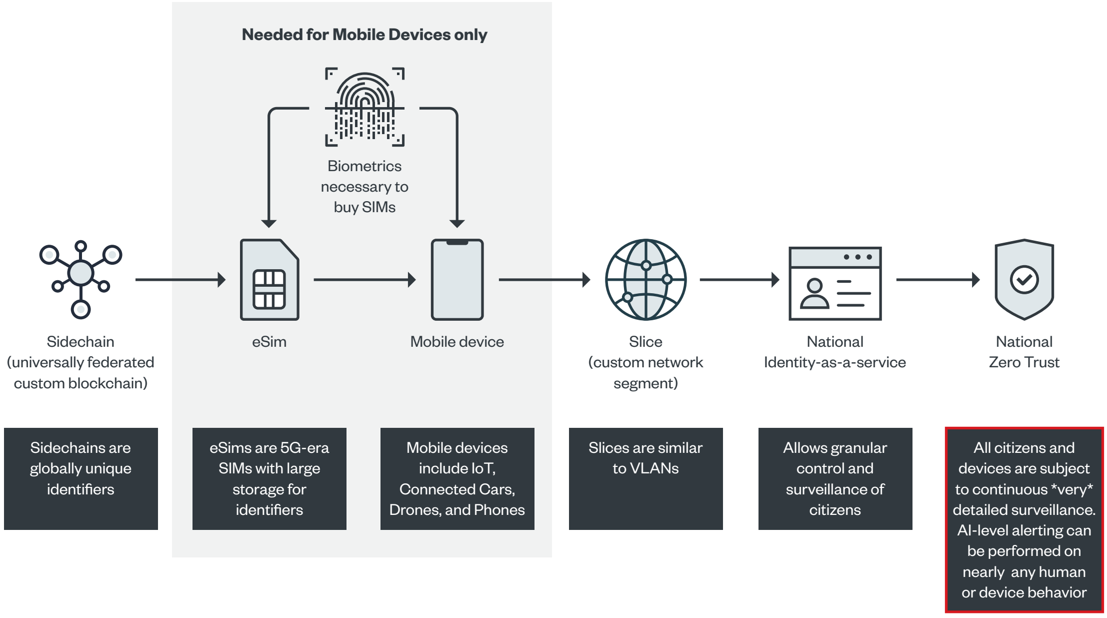
Needed for Mobile Devices only
Biometrics necessary to buy SIMs
Sidechain (universally federated custom blockchain)
eSim
Mobile device
Slice (custom network segment)
National Identity-as-a-service
National Zero Trust
Sidechains are globally unique identifiers
eSims are 5G-era SIMs with large storage for identifiers
Mobile devices include IoT, Connected Cars, Drones, and Phones
Slices are similar to VLANs
Allows granular control and surveillance of citizens
All citizens and devices are subject to continuous *very* detailed surveillance. AI-level alerting can be performed on nearly any human or device behavior

Figure 4. China's National Identity program as a supply chain of identity fabric information

This approach allows offline data sources to be continuously enriched by mobile devices. Since biometrics are required to buy the SIM cards and the devices themselves generate sensor telemetry (including biometrics), there is a powerful ability to combine both types into high-quality artificial intelligence graph databases. These can then be used for the creation of new and more accurate alerts. These can be based on cybercrime, state actor activity, tracking of dissenters, and automated policing. Things like COVID contact tracking can be used transparently to track known associates of criminals, when pushed to all cellphone users in a country.

USE CASE C – Election Tampering Prevention and Tracking

Countries are moving toward a deeper level of traceability in voting that can be solved with a specific version of Zero Trust.

The application of Zero Trust Primacy (and subset Personas) to voting systems can provide

- Integrity to election systems (this person is real, a citizen, and voted only once).
- Binding requirements in some countries that citizens must vote to be eligible for government services.

The above can be provided while being anonymous and secure to both the voter and the upstream system (a feature of Primacy and Personas).

USE CASE D – 6G Zero Trust Compliance

6G Telecom technology already includes Zero Trust as a core feature set in emerging standards.

Zero Trust using Primacy and Personas is scalable (meaning fast and lightweight, reducing CAPEX in terms of total bulk network load of cell towers). For this reason, Zero Trust has been built directly into the proposed 6G standards.

USE CASE E – Omnichannel

The “All Services, One Infrastructure” transformation approach called Omnichannel relies heavily on Identity Federation, a core competence of Zero Trust. When you have multiple means of authenticating there must be lightweight common logging and features. This has the design implication of a common privilege management structure unifying Identity and Access Management (IAM) into a lightweight and scalable identity federation (an Identity Fabric).

Identity fabric must rely on federation to have credible output. The concept of unified IAM is a simple one but complex in execution as many organizations do not have the enterprise data architecture maturity to bridge old and new.

USE CASE F – Data Sovereignty

Data Sovereignty is a specific deployment of Omnichannel, with additional business requirements driven by local law.

Zero Trust implementations can apply filters based on telemetry and encryption using extracted features of local laws. Machine learning has been successful in extracting these requirements at scale, with accuracy higher than human lawyers. Data Sovereignty can then be automated to meet the requirements of individual countries.

USE CASE G – International Identity Card

The blockchain implementation called Sidechains can be used as Globally Federated Canonical Identity, implemented as an eSIM identity persona visible to Zero Trust business, data, application, and network rules. Uses would include global Passport identifiers, global product identifiers (versus counterfeiting), shipment identifiers (versus counterfeiting and hijacking), transaction identifiers (versus fraud and money laundering), counterfeit prevention of retail products, and the tracking of assets likely to be used for illicit purposes (fake vaccines, blood diamonds, firearms, illegal drug precursors, etc.).

USE CASE H – Banking-Energy-Telecom Federation

Electrical consumption of IoT is high and will increase with the adoption of 5G and the ongoing expansion of IoT. Monetizing (and billing for) the increased power consumption of power-hungry electrical devices requires harmonized operational visibility between billing, electrical, and telecom systems.

Exposing these systems and their quite different operational security requirements will require very granular control over how all three families of data architecture interact. The continuous authentication and granular feature security of every device's identity will be necessary. Note that many IoT devices do not have unique identities, but the granular nature of Zero Trust and perimeterless networks allow this identity to be accurately inferred.

Since each system might be attacked from the other, the use of artificial intelligence security gaming algorithms can be used to map the "risk space" of all the systems involved.

In addition, 6G has high demands for speed, billing, and deep control of broadcast electrical power. In the 6G era the use case for the unity of banking, telecom, and power grid requires cross authentication and deep supply chain dependency on each other. Zero Trust Omnichannel is part of this, with Open Banking, Dynamic Grid, and 6G Machine Learning playing large parts.

USE CASE I – "Fake News Firewall" (blocking information operations at scale)

When national identity and Zero Trust are combined, the visibility into a population's activities is deep and profound. The phone call activity, messaging activity, and internet activity can be combined to see activities performed by any emergent group of people.

If a crafted narrative prompts activity by a group and the activity is determined to be against the best interests of the state, the functional equivalent of mass automated censorship can be deployed to prevent the arrival of these crafted narratives from arriving in the minds of vulnerable citizens. In this way the negative activity (burning down 5G cell towers for instance) is also blocked.

The bridge between current fake news prevention and a "fake news firewall" is the escalation of identity risk management into the realm of Signals Intelligence (SIGINT), where the changes to human activity promote an automated response, resulting in automated censorship at scale. Of course, which malicious narratives are censored are dependent on the specific interests of a particular country.

USE CASE J – Vendor Comparison and "Virtual Bakeoff"

Zero Trust does much to bring together harmonized security metrics from multiple sources. This can be used to find and destroy entire classes of risk either proactively or reactively, including risks that come from a vendor's components.

Many large enterprises have architecture sprawl (from multiple mergers and acquisitions) that might result in many security vendors in the network with overlap in what their features do. What if an entire vendor is a risk in that their entire feature, product, or product line is less effective (riskier) than another vendor product line already in your network? Comparing the two through audit might not work, since most audits are point-in-time and not real-time analysis based on the trends of logged past real-time performance

A "Bakeoff" is a side-by-side comparison of vendors who have similar features, usually done in a vendor assurance lab prior to awarding a procurement contract. Since this is a component of winning new business, vendors will agree to this since it is normally a condition of competing for contract award.

Bakeoff side-by side comparisons are exceedingly difficult to negotiate by security risk managers once business has been won. For this reason, it would be very convenient to perform a virtual bakeoff, one in which the vendors and their features are compared using a security report using harmonized side-by-side data (such as Zero Trust). In this approach, the performance (risk reduction) of each feature and vendor can be compared. In this way, vendors can be assessed for the return on investment (ROI) of their products, and the best two performers can be vendor-consolidated. Two is the practical minimum for vendors, otherwise there is political leverage lost during future price negotiations.

This and similar approaches can be used for security investment management. Once internal success and credibility are won, larger risk scoping of even non-security vendors can be performed using additional business criteria. In this way, information security that is traditionally thought of as a cost center can "move out of the basement" and be seen as a true contributor to board-level business goals such as those of the CRO.

Zero Trust security risk management can then become a means of performing even non-security risk management of even non-security assets, a scalable and automatable approach to board governance concerns arising out of supply chain and SBOM regulatory accountability considerations.

USE CASE K – Work from Home, Supply Chain, Vendor Management Using Zero Trust

Since work-from-home consultants and employees are effectively part of the supply chain and could be thought of as "vendors," a similar approach can be taken for them, their products, and their devices.

These Zero Trust supply chain approaches support decentralized identity and perimeterless networks when implemented with specific features such as Primacy, making portions of an identity visible to appropriate parties.

References

1 Mark Pomerlau. (Jan. 19, 2022). *C4ISRNET*. "Biden signs memorandum to secure sensitive national security systems." Accessed on Sept. 7, 2022, at https://www.c4isrnet.com/it-networks/2022/01/19/biden-signs-memorandum-to-secure-sensitive-national-security-systems/.

2 The White House. (May 24, 2022). *The White House*. "Quad Joint Leaders' Statement." Accessed on Sept. 7, 2022, at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/.

3 Jack Freund. (Jan. 18, 2021). *ISACA*. "Zero Trust Should Not Equal Zero Business." Accessed on Sept. 7, 2022, at https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-2/zero-trust-should-not-equal-zero-business.

4 Michael Pinhorn. (November/December 2021). *InfoSecurity Professional*. "In Zero, We Trust." Accessed on Sept. 7, 2022, at https://magazines.isc2.org/pages/2021/.

5 PYMNTS. (May 18, 2021). *PYMNTS*. "Biden's Executive Order Brings 'Zero Trust' Policy to Government Agencies." Accessed on Sept. 7, 2022, on https://www.pymnts.com/news/security-and-risk/2021/bidens-executive-order-brings-zero-trust-policy-to-government-agencies/.

6 European Union. (2016). *European Union*. "Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148." Accessed on Sept. 7, 2022, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN.

7 MITRE ATT&CK®. (April 28, 2022). *MITRE ATT&CK*. "Supply Chain Compromise." Accessed on Sept. 7, 2022, at https://attack.mitre.org/techniques/T1195/.

8 MITRE ATT&CK®. (April 28, 2022). *MITRE ATT&CK*. "Supply Chain Compromise: Compromise Software Dependencies and Development Tools." Accessed on Sept. 7, 2022, at https://attack.mitre.org/techniques/T1195/.

9 Venafi. (n.d.). *Venafi*. "Supply Chain Compromise: Compromise Software Supply Chain." Accessed on Sept. 8, 2022, at https://threatmodel.venafi.com/techniques/VT0004/002.

10 Ryan Angelo Certeza. (Oct. 31, 2013). *Trend Micro*. "Ransomware Raises the Stakes With CryptoLocker." Accessed on Sept. 7, 2022, at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3132/ransomware-raises-the-stakes-with-cryptolocker.

11 Trend Micro. (Feb. 18, 2022). *Trend Micro*. "Ukraine Cyberattack 2022: Geopolitical Cybersecurity." Accessed on Sept. 7, 2022, at https://www.trendmicro.com/en_us/research/22/b/ukraine-cyberattack-2022.html.

12 Trend Micro. (Jan. 8, 2021). *Trend Micro*. "Security Alert: Sunburst (SolarWinds) Targeted Attack Detection and Investigation with Trend Micro Products." Accessed on Sept. 7, 2022, at https://success.trendmicro.com/dcx/s/solution/000283368?language=en_US.

13 Trend Micro. (n.d.). *Trend Micro*. "Apache Log4j (Log4Shell) Vulnerability." Accessed on Sept. 7, 2022, at https://www.trendmicro.com/en_us/apache-log4j-vulnerability.html.

14 Shalanda D. Young. (Jan. 26, 2022). *Executive Office of the President Office of Management and Budget*. "Moving the US Government Toward Zero Trust Cybersecurity Principles." Accessed on Sept. 7, 2022, at https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

15 Bill O'Hearn. (Jan. 18, 2022). *AT&T*. "The Security Benefits of a Software Bill of Materials." Accessed on Sept. 7, 2022, at https://about.att.com/innovationblog/2022/security-benefits-software-bill-of-materials.html.

16 Quad Joint Leaders. (May 24, 2022). *The White House*. "Quad Join Leaders' Statement." Accessed on Sept. 7, 2022, at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/.

17 European Parliament. (Nov. 4, 2021). *European Parliament*. "Report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148." Accessed on Sept. 7, 2022, at https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_EN.html.

18 European Parliament. (Nov. 4, 2021). *European Parliament*. "Report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148." Accessed on Sept. 7, 2022, at https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_EN.html.

19 Kate Yin and Gil Zhang. (July 5, 2022). *Lexology*. "China released its 'Standard Contractual Clauses' (SCC) for public consultation." Accessed on Sept. 8, 2022, at https://www.lexology.com/library/detail.aspx?g=2ea3fe56-bc40-4000-aff3-788b18abd868.

20 FIDO Alliance. (n.d.). *FIDO Alliance*. "Alliance Overview." Accessed on Sept. 8, 2022, at https://fidoalliance.org/overview/.

21 National Institute of Standards and Technology (NIST). (n.d.) *NIST*. "Software Identification Tags." Accessed on Sept. 8, 2022, at https://nvd.nist.gov/products/swid#:~:text=The%20International%20Organization%20for%20Standardization%20%28ISO%29%20and%20the,structured%20metadata%20format%20for%20describing%20a%20software%20product.

22 National Institute of Standards and Technology (NIST). (September 2012). *National Institute of Standards and Technology (NIST)*. "Guide for Conducting Risk Assessments." Accessed on Sept. 8, 2022, at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

23 National Institute of Standards and Technology (NIST). (September 2012). *National Institute of Standards and Technology (NIST)*. "Guide for Conducting Risk Assessments." Accessed on Sept. 8, 2022, at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

24 National Institute of Standards and Technology (NIST). (September 2012). *National Institute of Standards and Technology (NIST)*. "Guide for Conducting Risk Assessments." Accessed on Sept. 8, 2022, at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

25 National Institute of Standards and Technology (NIST). (n.d.). *National Institute of Standards and Technology (NIST)*. "Predisposing Condition." Accessed on Sept. 8, 2022, at https://csrc.nist.gov/glossary/term/predisposing_condition.

26 National Institute of Standards and Technology (NIST). (n.d.). *National Institute of Standards and Technology (NIST)*. "likelihood of occurrence." Accessed on Sept. 8, 2022, at https://csrc.nist.gov/glossary/term/likelihood_of_occurrence#:~:text=Definition(s)%3A,or%20a%20set%20of%20vulnerabilities.

27 National Institute of Standards and Technology (NIST). (n.d.). *National Institute of Standards and Technology (NIST)*. "impact." Accessed on Sept. 8, 2022, at https://csrc.nist.gov/glossary/term/impact#:~:text=Definition(s)%3A,information%20or%20information%20system%20availability.

28 Red Hat. (Aug. 31, 2022). *Red Hat*. Accessed on Sept. 8, 2022, at https://www.redhat.com/en/topics/linux/what-is-a-golden-image.

29 Shaan Ray. (Jan. 22, 2018). *Hackernoon*. "What are Sidechains?" Accessed on Sept. 8, 2022, at https://hackernoon.com/what-are-sidechains-1c45ea2daf3.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com