To What Extent Should We Trust "Zero Trust Architecture"?

By: Logan Aboudara and Matt Maledon

HYPOTHESIS

“Despite adoption challenges, recent advancements make Zero Trust Architecture (ZTA) a smart investment, reducing long-term security costs.”

ZTA, or Zero Trust Architecture, is a new cybersecurity framework designed to reduce the risk of security breaches and hacker entry into networks that emphasizes “zero trust” for any access point. While its efficacy is widely known and proven, its proliferation has been stifled by a few key factors, including the complexity and cost of implementation, integration with existing systems, and a shortage of skilled cybersecurity professionals.

In the following paper, we argue that due to more recent research showing advancements in ZTA implementation, companies should invest in ZTA architecture on account of the fact that the implementation of ZTA will decrease overall security costs in the long run for the majority of businesses.

Background on ZTA

Zero Trust Architecture emerged in response to the growing inadequacies of traditional perimeter-based security models, which relied on the assumption that internal networks were inherently trustworthy. Perimeter-based security models, similar to a “castle and moat”, relied on securing the outermost points of access to a network by utilizing firewalls and VPNs to control access to the “inside”. While perimeter based security models served the general public well for decades, they have been proven ineffective due to the fact that an intruder who is able to breach the outermost wall (cross the moat, say) thus has access to the entire network, especially dangerous for larger companies.

In comes Zero Trust Architecture (interchangeable with “ZTA” in this paper). Introduced as a concept by Forrester Research in 2010, ZTA was built on the principle of "never trust, always verify." Over the years, the architecture has evolved alongside advancements in cloud computing, remote work, and the rise of sophisticated cyber threats. By the mid-2010s, major organizations and government agencies began adopting ZTA to secure dynamic and decentralized environments. Zero Trust is essentially a cybersecurity model designed to eliminate implicit trust inherent in perimeter-based security models. It does so through rigorous verification at every access point within the network. Unlike perimeter-based models, Zero Trust emphasizes core principles such as Identity and Access Management (IAM), which assigns every user, device, and data element a distinct identity. IAM solutions authenticate these identities and grant access strictly based on their specific roles within the network, ensuring no interaction is trusted without verification. So, for instance, it isn’t as though my device in the Legal department and Jessica’s in the Sales department each have a password that bypasses the outermost firewall to give us both equal access to the company network, we each must pass an initial identity screening and subsequent ones whenever we want to access information or files not necessarily accounted for in the first identity screening.

Micro-segmentation further strengthens security by dividing the network into isolated zones, limiting attackers' lateral movement. This segmentation, akin to compartmentalizing a submarine, uses tools like firewalls to contain breaches within specific network segments, reducing the scope of potential damage, thus explaining the increase in identity verification inherent in ZTA. Another selling point of ZTA is Least Privilege Access. In other words, access is granted based on specific needs and roles, limiting potential damage if a credential is compromised.

Additionally, Zero Trust relies on continuous authentication, which surpasses traditional static credentials by continuously verifying the identity and trustworthiness of users, devices, and applications throughout a session. Thus, ZTA requires constant verification of users, devices, and activity, offering a clear picture of who is accessing what. This is bolstered by multifactor authentication and regular device updates to maintain integrity. The principle of least privilege access ensures that users and devices receive only the permissions necessary for their tasks, minimizing vulnerabilities from over-permissioned accounts. A pivotal innovation in Zero Trust is the decoupling of security from infrastructure, which replaces legacy systems with flexible, software-driven solutions. Today, ZTA stands as a cornerstone in modern cybersecurity strategies, driven by regulatory mandates and the increasing need to mitigate breaches.

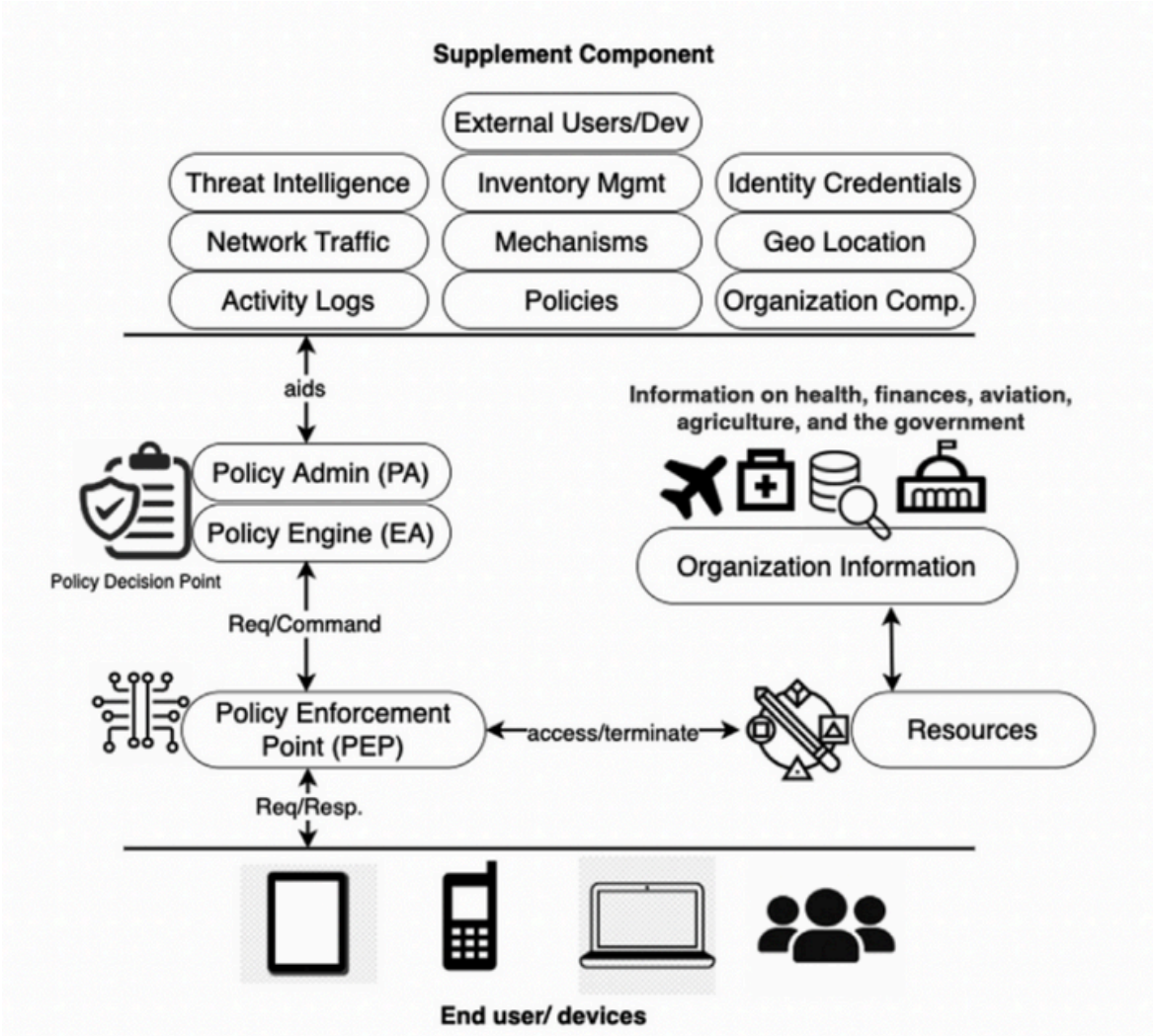

Fig. 2. Detailed architecture of ZTA showing components and their interactions..

The image displayed here is a detailed model of Zero Trust Architecture, including users, information contained by the organization, and the connections between them. Because of ZTA's unique structure, as organizations grow and ebb, ZTA scales to manage more users, devices, and applications without compromising security. Additionally, policies can adapt dynamically to evolving threats and changes in the environment.

The market size value of ZTA in 2021 was USD 22.06 billion. ZTA prospects expect a revenue forecast of USD 59.43 billion by the end of 2028 if more organizations continue to adopt it. The revenue forecast is a **Compound Annual Growth Rate (CAGR) of 15.2% from 2021 to 2028.**

One of the earliest examples of implementation of Zero Trust Architecture was from Google in 2009 in response to Operation Aurora, a massive and multi pronged cyberattack originating in China. Their proprietary Zero Trust system was named BeyondCorp, and it utilized managed devices as centers for authenticating credentials without a specified "border" like most cybersecurity systems were using at the time. Personal devices, or BYOD's, were not given access to BeyondCorp's resources.

REASONS TO IMPLEMENT ZTA

Addressing Implementation Costs

Despite obvious pros to implementing Zero Trust Architecture, many companies have been reluctant to do so for a variety of reasons, including complexity concerns, lack of understanding of the system and philosophy of "Zero Trust", and, most importantly, cost concerns. Most holdouts had concerns that overhauling their existing legacy systems would cost them a fortune.

One estimate puts the benefits of implementing ZTA at around $684k in reduced risk impact over the span of 3-4 years. In fact, ZTA improves organizational compliance by requiring robust forms of authentication from all users. While some "enterprises have reported that the average cost of maintaining compliance runs approximately $10,000 per employee", Zero Trust reduces regulatory compliance expenses by adhering to the highest security compliance standards.

Additionally, according to a study from the scientific journal "Computers and Security", using ZTA is already cheaper than VPN's. In the state of New Jersey, implementing ZTA overhaul to allow for safe remote work and remote courtroom proceedings got an estimated return of $10.7M on investment, which is no small number.

Table 1
ZTA Tools and Current Prices as of 2022.

Tools and Resources	ZTA Component	Unit Cost (u) per Year	ZTA tool cost based on the number of employees in an organization			
			1 - 100	101 - 400	401 - 700	701 - 999
CylancePROTECT for Endpoint Protection Cylance (2022)	Subject and Resources	$45 per endpoint for 1–250 endpoints. $41.75 per endpoint for 501 - 1000 endpoints	$4,500.00	$16,700.00	$29,225.00	$41,708.25
Kaspersky Security for Business with encryption services AO Kaspersky Lab, 2022	Data Encryption - Subject, Resources, and PEP Endpoint Protection - Subject and Resources	$45 per node	$4,500.00	$18,000.00	$31,500.00	$44,955.00
Google Workspace for Cloud-based Storage and Access Control Prokopets (2022)	Access Control - PE in PDP Data Encryption - Subject, Resources, and PEP					
Cloud Storage - Resources	2TB pooled cloud storage for $96 per user	$9,600.00	$38,400.00	$67,200.00	$95,904.00	
Microsoft OneDrive Prokopets (2022)	Access Control - PE in PDP Data Encryption - Subject, Resources, and PEP Cloud Storage - Resources	1 TB for $60 per user	$6,000.00	$24,000.00	$42,000.00	$59,940.00
Virtru Encryption Virtru Team, 2021	Subject, Resources, and PEP	$948 per 5 user	$18,960.00	$75,840.00	$132,720.00	$189,410.40
Microsoft Azure Active Directory for Access Control Zelleke (2021)	PE in PDP	Comes free with Microsoft OneDrive or $72 per user separately	$7,200.00	$28,800.00	$50,400.00	$71,928.00
Security Engineer Salary.com, 2022	PA in PDP	$60 per hour	5h/week $14,400.00	10h/week $28,800.00	20h/week $57,600.00	30h/week $86,400

The above table displayed estimates of the costs necessary to implement ZTA, with larger companies (701-999 employee count) only needing to budget $45,000 for the architecture, a relatively small expense for them. Additionally, for smaller enterprises (1-100 employees), the research drops that budget to around $4,500, again a small expense.

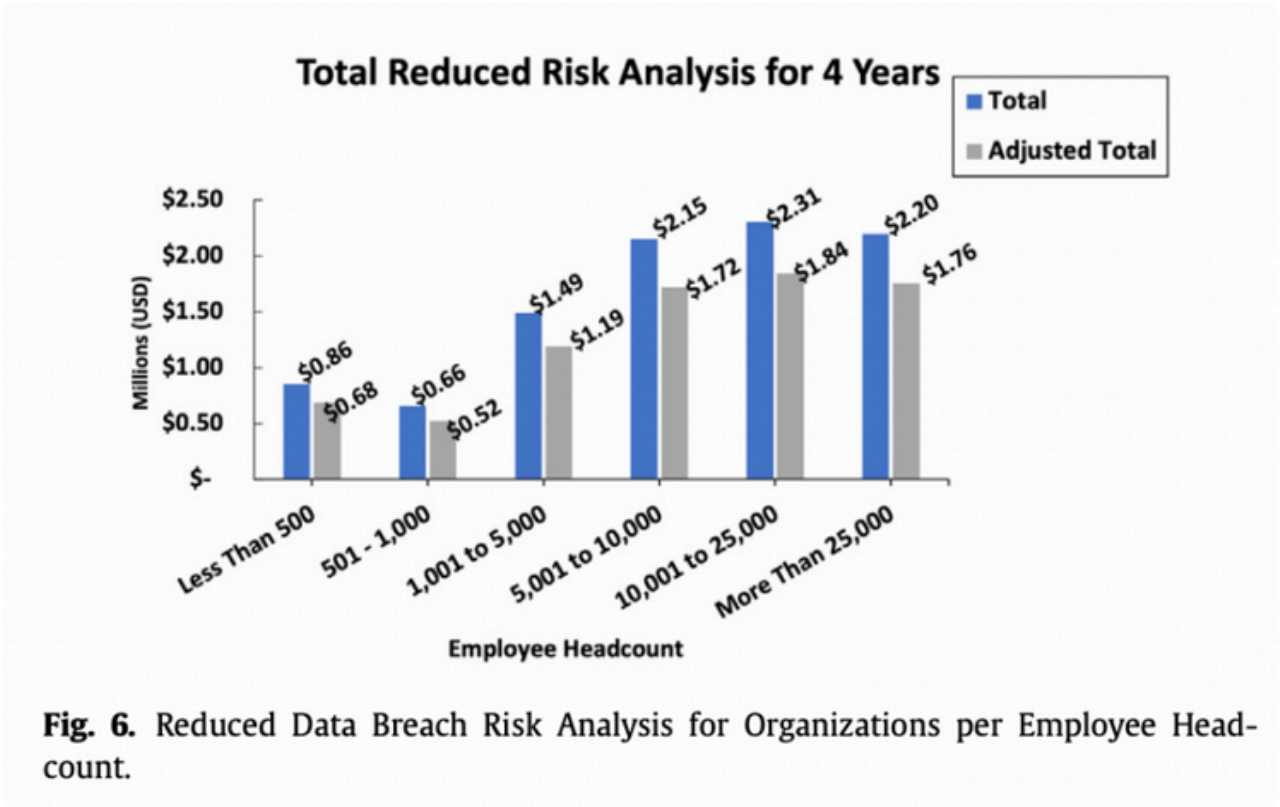

Fig. 6. Reduced Data Breach Risk Analysis for Organizations per Employee Headcount.

In addition to the small expense of budgeting for ZTA implementation, a study found that reduced risk from implementing the architecture can have positive impacts on expected costs up to $1.84 million, for companies with 10,000–25,000 employees worldwide, which more than outweighs the implementation costs for any size business, thus again showcasing why ZTA implementation decreases overall security costs for businesses in the long run.

Reduction in Expected Breach Costs

ZTA also comes packaged with the added benefit of reducing the expected costs of security breaches for an organization. If a company continues to operate with a dated legacy system that increases the overall risk of a serious breach as hackers and other malicious attacks become more powerful and ingenious, implementing ZTA to decrease that risk has the added benefit of decreasing potential costs from data breaches or other successful cyberattacks.

Organizations like Microsoft, Palo Alto Corporation, and IBM, with fully implemented ZTA approach, experienced a 42.3% savings on data breach costs IBM. Specifically, the average cost of data breaches for organizations with fully implemented ZTA is $1.76 million lower than organizations with no ZTA.

More specifically, the average cost of a data breach in the U.S. today is $4.88M. According to a report from IBM, 40% of data breaches involve data stored across multiple environments, which ZTA almost completely eradicates, thus drastically reducing the risk and associated costs of cybersecurity breaches.

Given all of the above research clearly illustrates the massive cost benefits of switching to ZTA, it's logical to assume that the rate of adoption will only increase in coming years as these benefits are made more widely known. Therefore, as more companies adopt ZTA, those who lag behind will unfortunately become the target of a higher proportion of cyberattacks due to more penetrable security systems. Thus, those companies will either adapt extremely quickly, thus increasing the rate of adoption on the tail end of the entire market adoption timeline, or they will fall.

Addressing the Lack of Cybersecurity Professionals

The CAGR of students graduating with degrees/focuses in cybersecurity has been around 19% for the past 4 years, signifying a future in which there are more cybersecurity professionals available to assist companies with less available capital to also implement Zero Trust Architecture, thus further decreasing costs of implementation.

Some notable companies who have already transitioned to ZTA, in addition to Google as mentioned, are Microsoft, Cisco Systems, Palo Alto Networks, Okta, IBM, Symantec (now part of Broadcom), Check Point Software Technologies, Akamai Technologies, and Fortinet. Essentially, most major tech companies are already on board with ZTA's innovative approach to authentication and security measures. It's only a matter of time until other sectors realize the value in ZTA.

Increasing Regulatory Compliance

The final added benefit of implementing ZTA is its ability to increase an organization's regulatory compliance. In an era of increased cybersecurity regulation, compliance is extremely important for any size organization. Biden's 2021 Executive Order on Increasing Cybersecurity is a recent example. Another important cybersecurity regulation is CMMC, or the Cybersecurity Maturity Model Certification, a certification program for Department of Defense Contractors. There are also other regulations in place for other industries – HIPAA for healthcare and life sciences, and the GLBA for the financial services sector, for instance.

In the past 20 years, as more and more sensitive information has been stored digitally, ensuring people's safety of information is critical. Thus, if we take the above research to be true that ZTA increases cybersecurity strength and reduces risk of breaches, it follows that ZTA will thus allow organizations to more easily and more cost effectively comply with current and future cybersecurity regulations, thus lowering their overall cost of security.

Insurance Benefits

The global cybersecurity market is rapidly expanding, with a $16.4 billion valuation in 2023, and a projected CAGR of 20.5% in the next decade. As the market expands and the risk of breaches increases, more and more companies are seeking insurance, commonly referred to as "cyber liability insurance". Moreover, in recent years, most cyber insurance providers are actually requiring ZTA to be in place before they sell a company an insurance plan.

Aside from that, it's also worth noting that implementing ZTA has a tangible impact on those insurance premiums – it lowers them. Moreover, implementing ZTA will decrease overall security costs for businesses, especially in part by means of their insurance premiums.

Potential for Remote Work

The final benefit of implementing ZTA is that users can securely access resources from anywhere, supporting remote and hybrid work environments. Thus, implementing ZTA has the potential upside not only of increased risk management, but also allowing firms to increase hiring and productivity with more people connected to the network away from a centralized office.

Potential Drawbacks

Implementing ZTA isn't a weekend-long ordeal. From various estimates, it can take anywhere from 3 months to a full year, depending on a host of factors. However, a rule of thumb is that the larger the network, the longer it will take to create a ZTA network. Additionally, there is often cultural pushback against ZTA implementation, along the lines of employees viewing the increased security not as a positive for the organization but a hindrance to their access to information, and thus, productivity. Making sure employees and executives alike are trained and understand the benefits of ZTA is crucial for decreasing the human capital necessary to make a ZTA network run smoothly.

Additionally, as mentioned above, old security models use a walled garden approach to security. Changing mindsets and work patterns can be difficult if the ZTA solution is not easy. However, in the past, ZTA solutions have marketed themselves this way – "our service is easy, no VPN's, or messy connections, just preinstall a client on a customer's machine and we will take care of the rest!" Thus, from the user side, ZTA is super easy to use, despite the few added inefficiencies of more necessary logins.

From an admin point of view, however, it adds complexity. Instead of a system where you can generally connect, connect remotely, and access resources across the network, by design you are logging in more and there are blocks connecting to resources.

THE SOLUTION

After reading this article, as a business owner, there's no doubt that you're sold and are already looking for ways to implement ZTA. If that's you, consider the following course of action. First, speak to your internal IT team, who will be at the forefront of the implementation process.

They will be the ones to draw, configure, connect, and monitor the new ZTA network for the organization. Consult them on if they have the bandwidth to do so, etc. Second, reach out to IT vendors who can partner with your team for services or hardware that may expedite the process. Third, configure the new network.

Fourth, train employees on how to access all of the decentralized resources within the network given their credentials, and update their cybersecurity awareness training. Fifth, train IT administrators on monitoring the network and allowing all verified access to employees.

Finally, enjoy your new network, with increased security and decreased risk of breaches.

CONCLUSION

In conclusion, Zero Trust Architecture represents a transformative approach to cybersecurity, addressing the limitations of traditional perimeter-based models and aligning with the evolving needs of modern organizations.

Despite initial concerns about implementation costs, complexity, and cultural resistance, research overwhelmingly supports ZTA's ability to reduce security risks, improve regulatory compliance, and lower long-term security expenses. As more companies adopt ZTA and the availability of skilled cybersecurity professionals increases, its implementation is becoming increasingly accessible and cost-effective. Organizations that delay this transition not only risk higher breach costs but also face growing challenges in maintaining competitive insurance premiums and regulatory compliance.

Ultimately, investing in ZTA is not just a cost-saving measure but a strategic necessity in an era of sophisticated and ever-evolving cyber threats.