SECURANCE CONSULTING

the advantage of insight

NEVER TRUST, ALWAYS VERIFY:

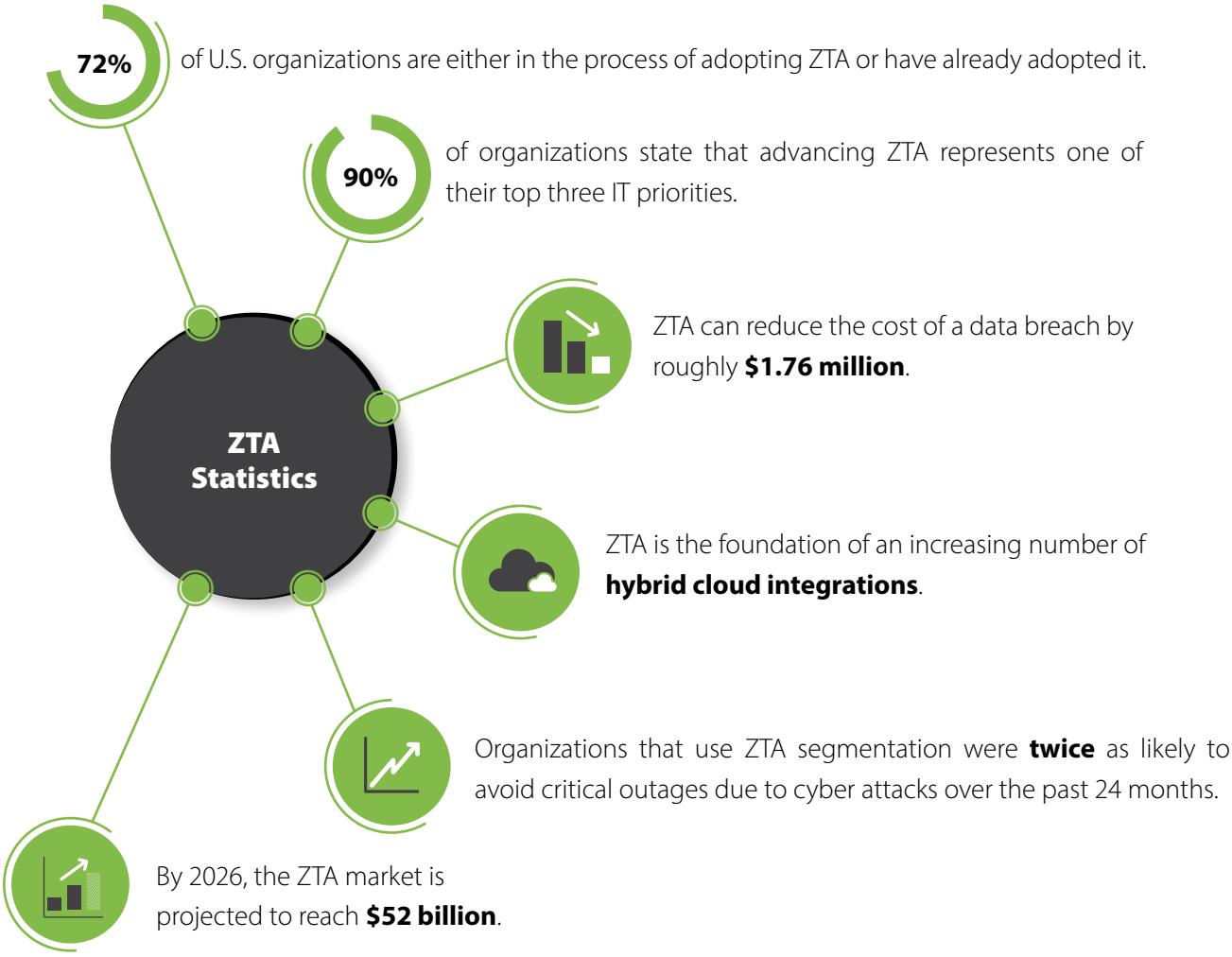
THE FUTURE OF ZERO TRUST ARCHITECTURE

www.securanceconsulting.com

INTRODUCTION

In our digital world, physical perimeters have become obsolete. Similarly, the idea that there is a network edge, or that trusted networks exist, is an outdated mindset. In the past, users and assets resided within the physical walls of the organization, and trust was defined by the perimeter. As cyber threats continue to evolve, and remote and hybrid work environments expand, implicitly trusting users, devices, and applications that are on a company's network is no longer a viable approach.

A modern approach to cybersecurity validates identities seeking access to data and systems. This approach to security is referred to as Zero Trust Architecture (ZTA), a security framework that helps mitigate the risk of cyber attacks by treating all users and devices as potential threats. Organizations with mature cybersecurity programs have implemented ZTA to keep pace with the evolving threat landscape and regulatory compliance requirements.[1]



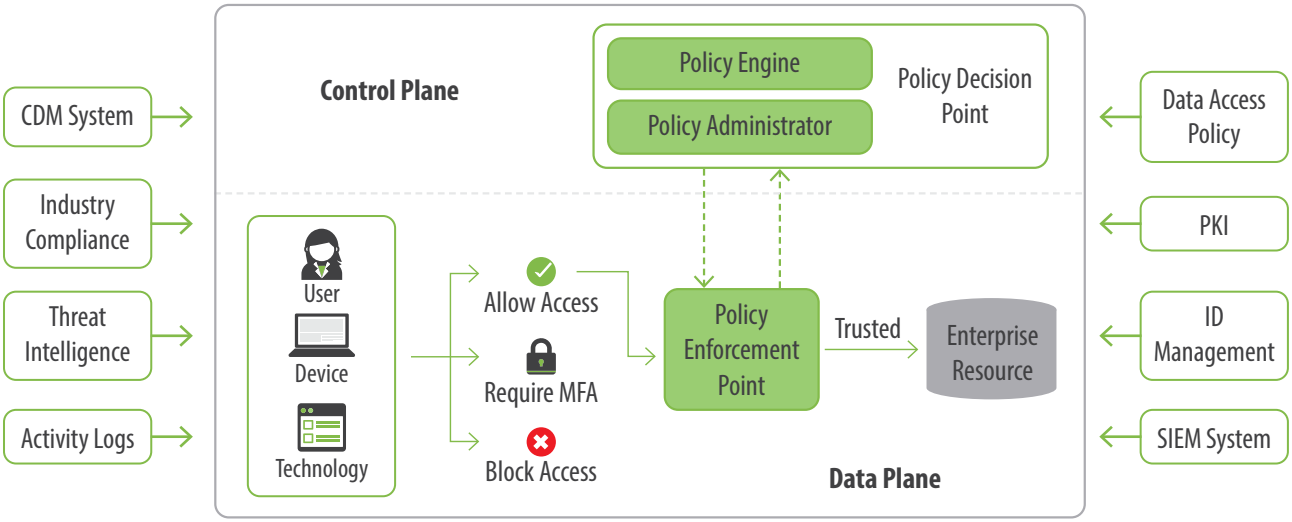
Cyber Talk, 2022[2]

ZTA is no longer just a concept or a buzzword, but an official framework that can be implemented and scaled to secure complex enterprise networks. By understanding the components of ZTA and deploying security solutions that follow the principle of least privilege, businesses can successfully implement ZTA across their environments.

WHAT IS ZTA?

ZTA is a security model based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, which requires that all users, inside or outside the network, be authenticated, authorized, and verified before accessing applications and data. ZTA requires organizations to track service and privileged accounts and control where they connect— and to what. One-time validation will not suffice, because threats and user attributes continually change.[3]

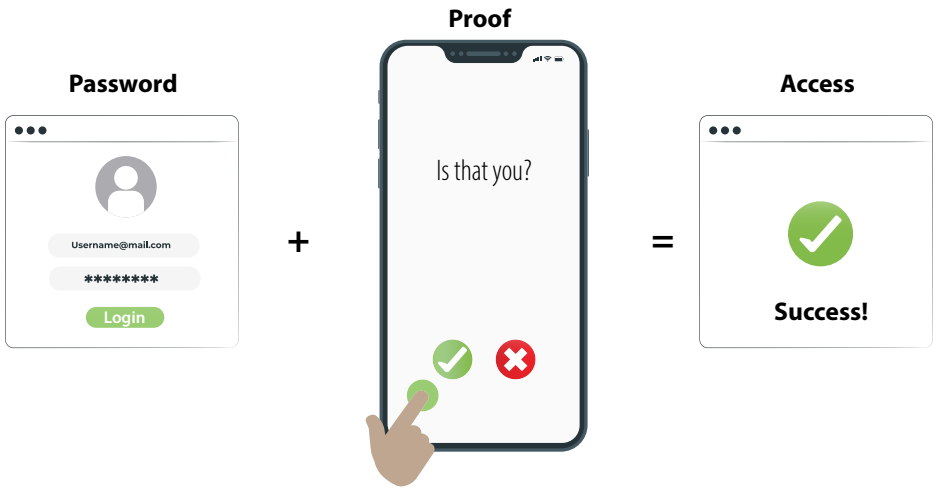
Components of Zero Trust Architecture



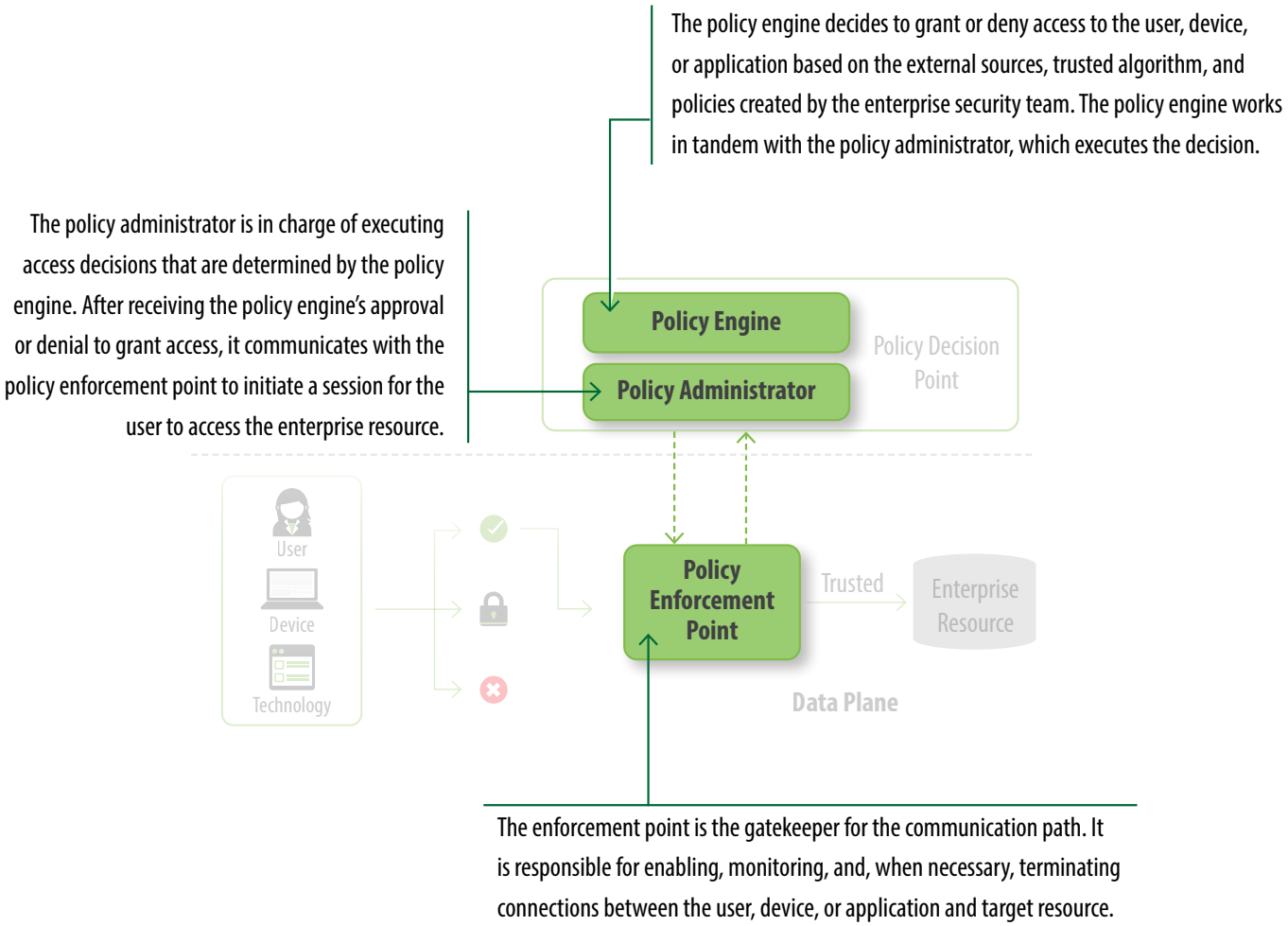
NIST SP 800-207, 2020[4]

How does it work?

The ZTA model removes implicit trust and, instead, requires that users, assets, and devices be verified during each login session or activity before access is granted. Think of ZTA as an advanced form of multi-factor authentication (MFA) that goes beyond the use of just a username and password for authorization.



At the core of the ZTA framework are three components:



ZTA incorporates the following key principles:

- **MFA**— MFA is a layered approach to security that requires a user to provide two or more identity credentials before they can access a system. MFA increases security because, even if one credential is compromised, an unauthorized user will not be able to meet the second authentication requirement to access the targeted physical space, computing device, network, or database.[5] ZTA uses MFA to reduce the risk of identity theft.
- **Principle of least privilege**— ZTA only gives users the access and permissions that they need to perform their job functions, limiting exposure to sensitive data and network assets.
- **Device access control**— ZTA minimizes the attack surface by monitoring the number of devices trying to access the network and ensuring that every device is authorized.
- **Micro-segmentation**— Micro-segmentation creates safe zones across data center environments to isolate application workloads from one another and secure them individually. In a ZTA, a person or program with access to one segment will not have access to any other segments without separate authorization.
- **Continuous monitoring and verification**— ZTA verifies devices, user identity, and privileges and ensures that established sessions time out periodically, forcing devices and users to reauthenticate. Risk-based conditional access ensures workflow is only interrupted when risk levels change and provides continual verification, without sacrificing user experience.[6]

IS ZTA RIGHT FOR YOUR BUSINESS?

ZTA is often recommended for organizations with mature security programs that want to further improve their cyber risk postures. ZTA solutions vary, from commercial tools to complex and large-scale approaches. When considering any new security initiative, it is important to consider the benefits and challenges, as well as your organization's unique objectives and requirements.

Benefits

The benefits of implementing ZTA include:

- **Improved security—** The ZTA model introduces the concept of treating all users and devices as potential threats, regardless of title or privilege level. ZTA requires strong authentication, authorization, and encryption methods for all users and technologies to detect and prevent malicious cyber attacks.
- **Reduced costs—** Implementing ZTA can cut costs because the model removes the need to continuously update and maintain outdated security practices, eliminates costly perimeter-based security solutions, such as firewalls and intrusion detection systems, and reduces the number of unique user accounts and permissions needed to access the network.
- **Increased productivity—** ZTA complements the transition to hybrid and remote work environments by allowing users to access critical data and systems from anywhere, eliminating the need for users to be physically present in the office.

> Implemented correctly, ZTA has the potential to revolutionize the way organizations approach security. In the future, more organizations will likely adopt ZTA to improve their security postures.

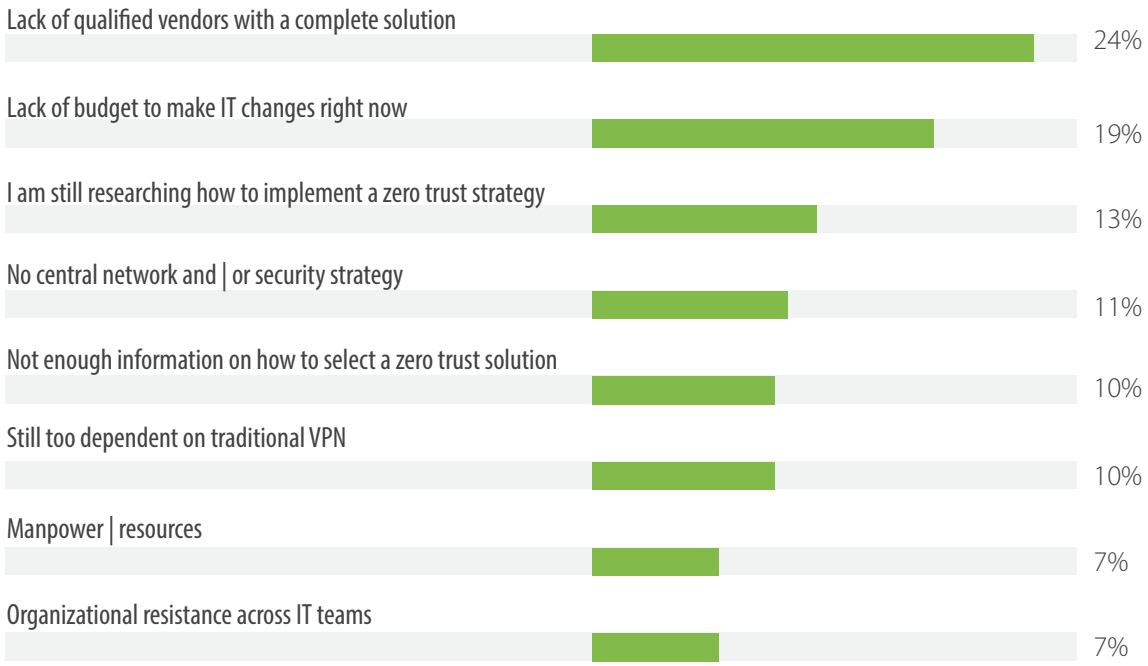
Challenges

Although there are many benefits to ZTA, there are some drawbacks to consider:

- **Harder to implement on legacy security systems—** ZTA can pose challenges for organizations with outdated equipment. The initial deployment requires replacing or updating existing security solutions to meet the requirements of the framework.
- **Requires extensive resources and planning—** Implementing the ZTA model requires extensive time, planning, resources, and collaboration between IT and security teams. Organizations must consider their unique security needs before committing themselves to implementing zero trust initiatives.
- **Reliance on strong authentication and authorization—** ZTA relies on the principle of least privilege. If authentication and authorization methods are not implemented correctly, and data is not encrypted properly, this can introduce additional security vulnerabilities.[7]

The largest barrier to the widespread use of ZTA is that it is not a singular system. Instead, organizations must adopt a number of approaches and consistently improve their methods over time to get the best outcome. For smaller businesses with little to no IT staff, the framework's strict guidelines make it very difficult to implement without the proper resources, knowledge, and budget in place.

Most Significant Challenges Building Zero Trust Strategies



Fortinet, 2022[8]

IMPLEMENTATION

If your business has begun or is considering ZTA initiatives, consider adopting the following security measures for your IT environment:

Data Segmentation

Data segmentation is the process of grouping data into multiple subsets. When critical data and sensitive information are separated from the rest of the network, and different security measures are applied, even if an attacker gains access to one network segment, they will not be able to cause a widespread security breach. Organizations should define their most sensitive data as their "protect surfaces," separate the protect surfaces from the rest of the network, and apply additional security measures to protect them.[9]

Data Flow Mapping

Understanding and observing the interactions between different system segments will help you map data flows, which your security system can track and monitor. Any irregular data flow will be caught by the system and require verification to continue. If the user cannot be verified, the system will isolate the segment and deploy security protocols.[10]

Developing Network Security Architecture

Network security architecture refers to the practice of ensuring data security and is the foundation of an organization's security defenses. In order to implement effective ZTA strategies, your business must design an architecture for your system that addresses your unique objectives, requirements, and needs and incorporates the ZTA security principles. This can include implementing security measures, such as network segmentation, MFA, and regular data backups.

Formulate ZTA Policies

Once the network security architecture is in place, organizations must develop ZTA policies. This includes following the principle of least privilege by defining users, the systems they need access to (and why), and how they will connect to systems and applications.

> As the hybrid workforce, cloud migrations, and security advancements fast-track digital information, implementing ZTA has become essential.[11]

Continuous Monitoring

Effectively implementing ZTA requires manual and automated system monitoring to detect malicious activity. Automated monitoring solutions alert IT staff to suspicious activity; after investigating, staff can either allow or deny access. ZTA operates under the assumption that no one is trusted, so every single user, system, and device must be authenticated before being granted access. With this in mind, a large portion of the network must use continuous automated monitoring in order to constantly verify who and what has access.

Update and Maintain

Adopting ZTA is a gradual process that requires a phased approach. Performing regular updates and maintenance on systems that use ZTA is crucial to realizing the benefits. This will also help your organization identify exposures and vulnerabilities within networks, systems, and devices.

> The best starting point for this journey towards ZTA is to replace the traditional network perimeter-centric view of security with an identity-centric mindset that ensures secure access for various user types regardless of their location, device, or network. The digital nature of our modern economy means that security threats will only intensify, so no business can afford to stand still.[12]

CONCLUSION

The Future of ZTA

The perimeter-based model of network security ("trust, but verify") is a thing of the past. Organizations today should follow the governing principle of ZTA: "never trust, always verify." Advanced MFA and identify and access management controls will protect networks, systems, and assets from evolving security risks and vulnerabilities.

ZTA is not a single product or step to take, but a comprehensive security model. Organizations that want to implement ZTA initiatives must reengineer their security programs to align with the framework. This requires significant time and resources but can pay dividends in the long run. When implementing properly, ZTA can improve security and help organizations scale their defenses to combat the next wave of cyber threats.

ABOUT SECURANCE

Securance has more than two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://techspective.net/2022/07/29/the-past-present-and-future-of-zero-trust/
2. https://www.cybertalk.org/2022/08/05/12-zero-trust-statistics-and-trends-in-2022/
3. https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/
4. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
5. https://www.cisa.gov/publication/multi-factor-authentication-mfa
6. https://www.comparitech.com/net-admin/zero-trust-architecture/
7. https://www.wildmintstudios.com/zero-trust-architecture-the-future-of-security/
8. https://www.fortinet.com/blog/business-and-technology/fortinet-zero-trust-survey-indicates-gaps-in-implementation?utm_source=blog&utm_campaign=ztsurvey
9. https://www.datamation.com/security/data-segmentation
10. https://cloudcomputingtechnologies.com/how-to-implement-zero-trust-architecture-zta/
11. https://www.linkedin.com/pulse/importance-benefits-zero-trust-security-richard-peterson/
12. https://www.okta.com/resources/reports/state-of-zero-trust-security-in-global-organizations/

Never Trust, Always Verify: The Future of Zero Trust Architecture

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com