SecureITWorld

ZERO TRUST SECURITY:

A HOLISTIC APPROACH TOWARDS ORGANIZATION'S SECURITY POSTURE

WHITEPAPER

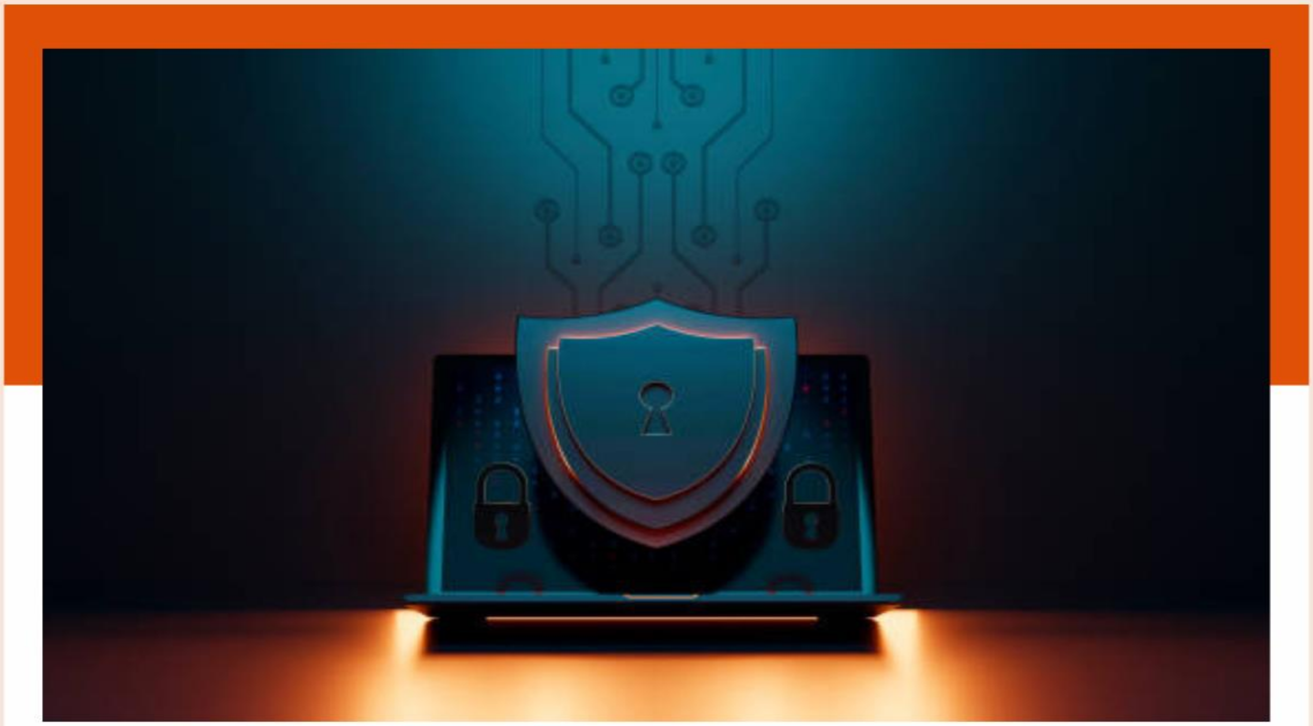


Table Of Contents

Executive Summary

The rise in cyberattacks leading to the loss of sensitive data, money, and business reputation has urged companies to have an intrinsic approach to strengthening their security posture. Previously, the IT sector heavily relied on perimeter security strategies to protect sensitive data. This involved strategies such as firewalls and additional network-based tools to examine and validate the users passing through the network. However, the digital transformation being in the shed light and growing at warp speed has prompted the move towards adopting cloud infrastructure to embrace the hybrid work environment. Plus, the complex modern environment has revolutionized the scenario of SMBs to big-dollar businesses; however, the perimeter security approach has struggled to keep pace.

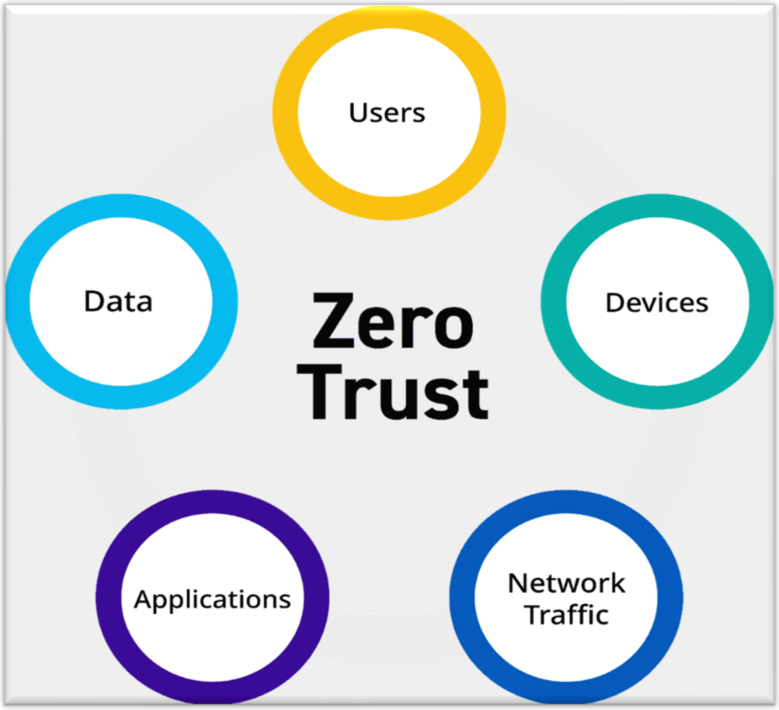
In the face of staying ahead and escalating these challenges, there is a need for the most viable and trusted approach. In a nutshell, it is a new paradigm: Zero Trust. Applying a zero-trust framework is beneficial as it teaches us to “never trust, always verify!”

By reading these white papers, businesses can unleash their true potential by shifting from the traditional security approach, putting the company at risk, to zero trust. This new holistic way responds to threats in a precise and faster manner.

Zero Trust Security (ZTA): Aiming Towards High-End Security

Zero trust is a cybersecurity model based on the phenomenon that every person or device inside or outside an organization's network perimeter undergoes strict verification and is granted access to the IT systems only if deemed necessary. It was first termed by an analyst at Forrester Research, John Kindervag, in 2010. After a few years, Google announced the implementation of ZTA to boost its network security.

A significant factor of the ZTA model is that it offers access to users based on their roles and responsibilities, whether at home, in the office, or anywhere else. Besides, for every single request, authentication, authorization, and encryption happen continuously throughout the network instead of just once at the perimeter.



Source:

The above diagram depicts the zero-trust model that works in and around data, users, devices, applications and network traffic. All of this form an efficient zero-trust model.

ZTA bridges the gap for perimeter security and further limits the unnecessary movement between the apps, systems, and services, accounting for insider threats and the prospect that an attacker might trade off on a legitimate account. In today's digital world, where interconnectivity is the need of the hour, security plays a silent yet crucial role. The ZTA security model can enable businesses to focus on their digital transformation goals without fearing data breaches, threats, and more.

Zero Trust Security Standards

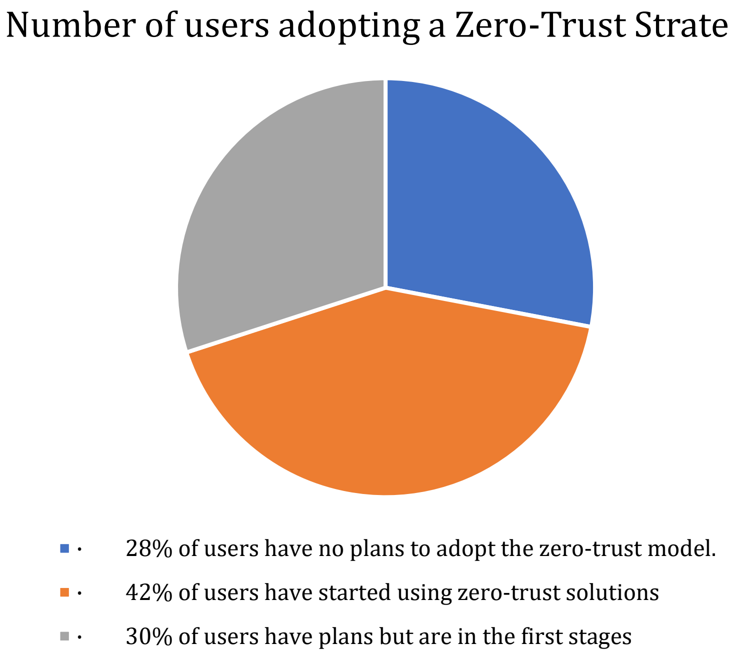
Cyberattacks should continue to rise if the last few years are any indication. As a result, an advanced strategy for cybersecurity is required, and implementing a zero-trust mentality across all of your systems is essential.

Businesses that use information security management system (ISMS) techniques, like ISO 27001 and 27002, will implement zero-trust architecture and alternative security controls. Specific controls, like authorization and authentication, call for more resources (and administration), but controls related to perimeter security might receive less attention.

The Importance of the Zero Trust Security Model

In the ever-evolving digital landscape, hackers and bad actors are going nowhere. Cybersecurity is a need of the hour, with zero-trust security standing as the top security model. The point is that everything inside is secure by default; the only thing that needs ample protection is the network that's present outside.

That being said, the traditional security approach needs to be more competent. Many businesses have an extensive network of connections, perhaps targeted by cyber attackers. They constantly monitor enterprise networks with the least possible security layers. Further, as the network is accessible and open to everyone inside the organization, anyone can share everything, which becomes a point of discussion.



The above pie chart shows the number of users adopting a zero-trust strategy for their organization.

- 28% of users have no plans to adopt the zero-trust model.
- 42% of users have started using zero-trust solutions
- 30% of users have plans but are in the first stages

Thus, organizations today need a whole new security approach and access management that minimizes the data breaches or threats caused by malicious attackers.

What is Zero Trust Security, and What is Not?

Zero Trust Security Approach:

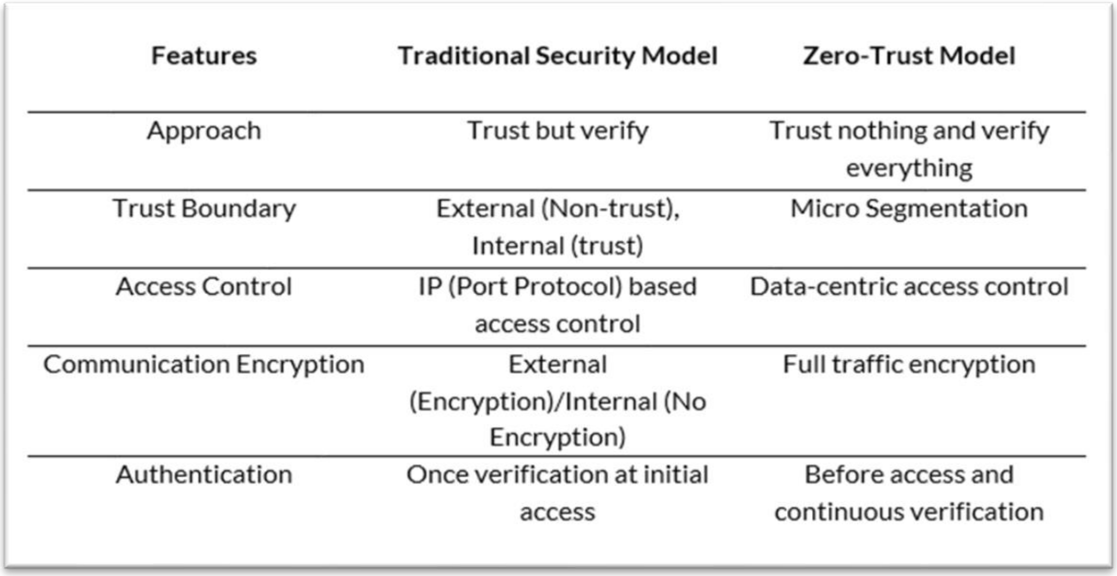
- It is a highly robust and defensible security strategy comprising different security measures, best practices, and technologies.
- Safeguard the organization's data wherever it may live and allow only authorized users or entities to access the resources.
- It is a data-centric approach that focuses on continuous authentication and authorization.

Not a Zero Trust Security Approach:

- There are better solutions to all the security issues within the organization.
- Only some technologies will enable organizations to transform their security approach completely.
- Focus on something other than the identification and authorization of users and devices.
- It is not a one-time task nor a solution that can be purchased and installed.

The Difference Between Zero Trust Security and Traditional Security Model

Both of these differ in aspects, as shown below:



Features	Traditional Security Model	Zero-Trust Model
Approach	Trust but verify	Trust nothing and verify everything
Trust Boundary	External (Non-trust), Internal (trust)	Micro Segmentation
Access Control	IP (Port Protocol) based access control	Data-centric access control
Communication Encryption	External (Encryption)/Internal (No Encryption)	Full traffic encryption
Authentication	Once verification at initial access	Before access and continuous verification

Approach:
The traditional security model follows a “Trust but verify” approach, while the Zero Trust model follows a “trust nothing and verify everything. This is one of the key differentiating factors amongst both of the systems.

Trust Boundary:
In the traditional security model, external parties have no trust boundaries, and internal parties have trust boundaries. At the same time, the Zero Trust security model has micro-segmented trust boundaries.

Access control:
Traditional security model encourages internet protocol (IP) address-based access control. On the other hand, the Zero Trust security model is all about data-based access control.

Encryption:
The traditional security model supports external (encryption), whereas there is no internal encryption. The case of Zero Trust security supports full traffic encryption, meaning all ongoing traffic is encrypted to avoid unnecessary threats and attacks.

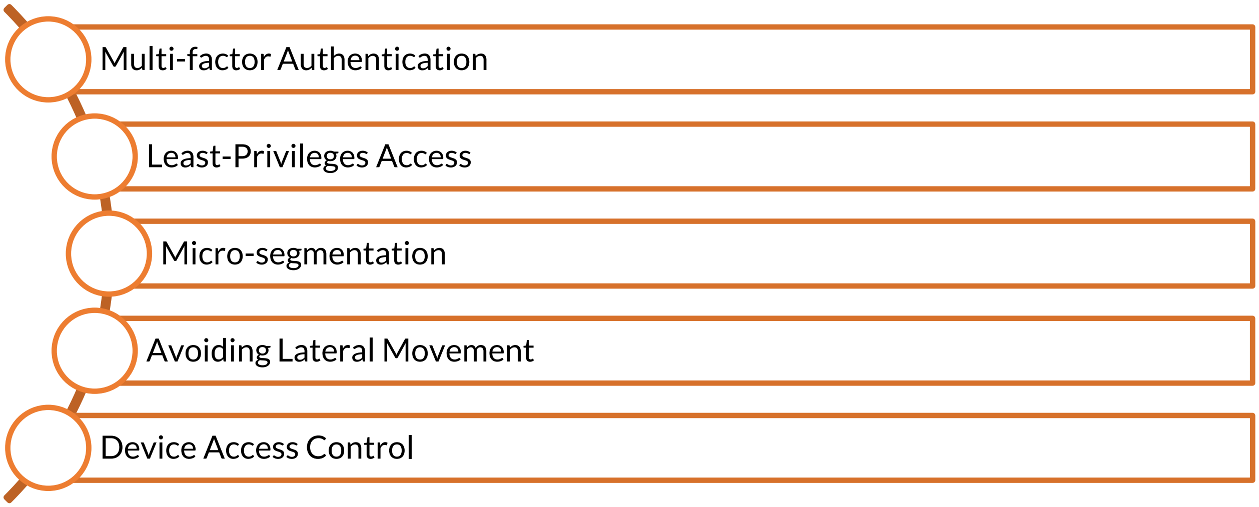
Authentication:
In the traditional security approach, verification is done only once and at initial access. However, the zero-trust model offers access and continuous guarantees before access.

How is a Zero Trust Network Better than VPNs?

Trust assumptions have made VPNs the most significant security risk. VPN gateways often publish their IP address and device identifiers, which are open online so anyone can access them. Cyberattacks can quickly gain access and traverse within the trusted user whenever a VPN gateway gets compromised. However, zero trust security hides all networks and resources behind software behind parameters. Thus, the network remains protected and no unauthorized entity or user can access it.

Critical Principles of Zero-Trust Security

The zero-trust security model defines a set of principles focused on network security. It is more than terminology and technology.



- Multi-factor Authentication
- Least-Privileges Access
- Micro-segmentation
- Avoiding Lateral Movement
- Device Access Control

Multi-factor Authentication
MFA is an important core principle of multi-factor authentication. It adds an extra layer of security to your device. This means it necessitates providing two or more verification factors to access the resource or device. Entering the password is not enough; you must enter a code sent on another device, such as a mobile phone, thus providing two pieces of evidence that they are who they claim to be.

Least-Privileges Access
One of the crucial principles of Zero Trust Security is the least privileged access. This limits users' access, minimizing the risk of exposing sensitive network data. Implementing the least privileged access can help to manage user permissions carefully. The main aim is to be assured of keeping your data at bay from unauthorized users.

Micro-segmentation

It breaks up a network's security perimeter into smaller zones, ensuring different access for different areas. To give a practical example, a network that stores all the files in a single data can efficiently microsegment them into dozens of secure zones. Thus, a user program needs separate authorization for different zones.

Avoiding Lateral Movement

Lateral Movement refers to the capacity of an attacker to move within the network after acquiring access to the device. An attacker can negotiate on the other network parts as they pass through them, making it challenging to detect them. The proximity of network segmentation allows the IT team to see and confine the device or account.

Device Access Control

While implementing the zero-trust security model, organizations see every connected device as a threat and untrust them. Therefore, continuously monitor each device that tries to access system data. This allows tracking and isolating devices that may create a threat and restrict probable data breaches.

Popular Use Cases of Zero Trust

Most organizations deal with networks and storing large amounts of data. Considering a zero-trust architecture in this scenario is beneficial. Here are some of the widespread use cases of zero-trust architecture.

Replacing VPN
To maintain high security and protect data, organizations rely on VPNs; however, that's not enough in today's burgeoning cyberattacks and defending against threats. Thus, implementing the Zero Trust approach is necessary as it provides enhanced security in the most complex scenarios.

Supports Remote Work
The zero-trust architecture stands out with its noteworthy features, unlike VPN, which can hamper productivity and has less secure grounds. At the same time, the zero-trust approach offers fast access control to connections from anywhere.

Assist in Rapid Employee Onboarding
Zero trust network promotes quick onboarding of new internal users, making it an ideal fit for rapidly growing organizations. On the other hand, a VPN might need to add capacity to accommodate more numbers of users.

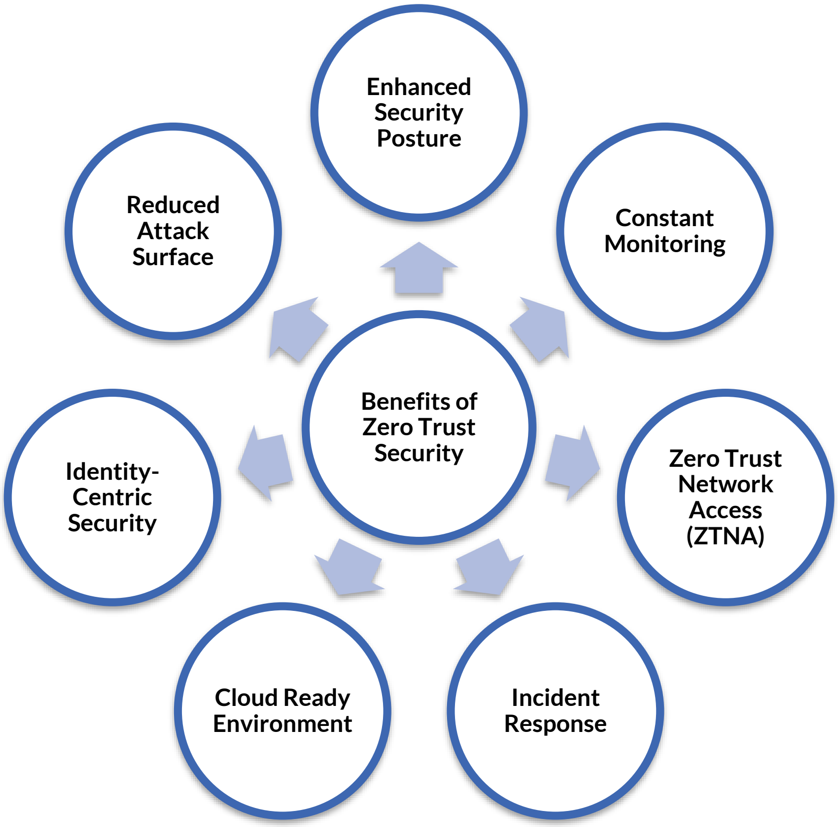
Third Parties and Contractors
Zero Trust can rapidly extend restricted, least privileged access to outside parties who use computers that aren't managed by the IT teams.

Support Teams Working Globally
In every organization, some employees work in different offices and some work remotely, all connected to a central head office. As the teams are working remotely, the cloud environment is generally adapted.

Also, companies force remote workers and locations to fetch resources using a VPN. However, these options cannot meet the demands and should be burdensome. Zero Trust does not need to require users to connect to the corporate network before accessing resources.

Benefits of Zero Trust Security

Zero Trust Security is a paradigm shift in cybersecurity that challenges the traditional notion of trust within a network. In this model, trust is never assumed, regardless of whether a user is inside or outside the corporate network. The key benefits of the Zero Trust Security approach can be summarized as follows:


Enhanced Security Posture
Constant Monitoring
Zero Trust Network Access (ZTNA)
Incident Response
Cloud Ready Environment
Identity-Centric Security
Reduced Attack Surface
Benefits of Zero Trust Security

Enhanced Security Posture
Zero Trust Security helps to significantly improve overall security by eliminating the aphonic trust associated with traditional network architecture. Organizations reduce the high risk of data breaches and unauthorized access by necessitating authorization and authentication for every device or user.

Constant Monitoring
Unlike the traditional security approach that is mainly dependent on perimeter defense. However, zero trust security works beyond this. It constantly monitors the users and their behaviors. This efficient and robust approach aids organizations in detecting potential threats and anomalies quickly and in real time, enabling faster response time and escalation.

Zero Trust Network Access (ZTNA)

ZTNA is the core component of Zero Trust Security that offers secure access to all the resources and applications based on their identity. This approach mainly supersedes the conventional VPN model, limiting access control and reducing the risk of unauthorized access.

Incident Response

Zero Trust Security increases incident response capabilities by offering thorough visibility into network activities. Access control and continuous monitoring assist organizations in quickly identifying and responding to security incidents, reducing the impact of threats.

Cloud Ready Environment

Zero Trust Security architecture is cloud-adaptive. It facilitates secure access to cloud-based resources and applications without relying solely on the traditional network perimeter.

Identity-Centric Security

Zero-trust security draws more attention to identity as a new perimeter. By solely focusing on users and device identities, organizations can build a resilient security framework that authenticates and authorizes based on individual identities.

Reduced Attack Surface

Organizations can reduce the attack surface by implementing micro-segmentation principles and least privilege access. This reduction in prospective points of compromise makes it difficult for attackers to exploit vulnerabilities.

Top Practices for Zero Trust Adoption

While the principles mentioned above form the core foundation of zero trust security, implementing them at a significant level is challenging. However, we have noted some of the best practices for zero-trust security.

Have Clear Business Objectives
You need first to consider the business requirements that can be improved by adopting the cybersecurity best practices. Zero Trust benefits any small or enterprise-scale business looking for top-notch security.

Cyber Hygiene
Cyber hygiene must be maintained before considering the zero-trust security approach. The six controls defined by the Center for Internet Security (CIS) can be an apt starting point.

End-to-End Strategy
The current and maturity of security solutions should always be the basis before defining a Zero Trust Security strategy. Enterprises need to carefully asses, replace, reuse, and rebuild options.

Introduction of Centralized Monitoring
The number of monitoring solutions you currently use doesn't matter; all the data must be accessible from a single dashboard to give a complete overview of the enterprise's network. It prevents the scenarios wherein malicious activity is identified. However, the report needs to be included.

Challenges of Zero Trust Security

Zero Trust Security is not a one-and-done effort. While it has numerous benefits, Zero Trust Security has several challenges. Organizations considering or in the process of implementing the zero-trust approach need to be prepared to address the following challenges:

Insufficient Time and Resources
Evaluating and selecting the right combination of Zero Trust Model technologies that are apt to an organization's unique requirements can demand more time and resources—delving into diverse solutions, conducting proofs-of-concept, and gauging their efficiency of time intensive. Furthermore, organizations need to invest resources in essential aspects such as staff training and management of the adapted ZT approach.

Hinders Productivity
At times, implementing a zero-trust model can lead to complex outcomes. Even a single configuration adjustment can render specific systems or data for employees. People need access to sensitive data to work, communicate, and collaborate with their teams. Productivity can be hampered if individuals change their roles and get locked down for a week.

Cost Implications
Implementing zero trust involves investing in new technologies, staff training, and ongoing maintenance. For many organizations, the cost may hinder their overall business growth. Thus, they need to keep an eye on the cost-effective solutions and tools to manage the Implementation costs.

Legacy Systems
Modifying legacy systems and applications initially built with perimeters in mind, but this isn't possible with zero trust. These legacy pieces need to be in place, which may create security gaps, need different security deployments to protect them, or need to be replaced, which can be very time-consuming.

Scalability
Ensuring Zero Trust scales effectively as an organization grows can be challenging. The dynamic nature of the modern IT environment, with changes in user roles, devices, and applications, requires a scalable and flexible security solution.

Case Studies of the Zero Trust Approach

Several organizations have implemented the Zero Trust Security approach to boost their cybersecurity posture. The case studies below clearly depict how companies are embracing the power of the Zero Trust Approach.

Cimpress Zero Trust Security Journey:

Cimpress is a $2 billion company specializing in mass customization, customizing business-to-business (B2B) and (B2C) business-to-consumer digital print products. Cimpress was founded in 1994 to help small businesses with their impressive-looking print products that would allow them to compete in large-scale markets.

The Challenge:
Cimpress's zero trust journey began years ago; however, it faced several challenges implementing the zero-trust approach for all its businesses. Every company operates independently, and teams can select their technology to run their organizations. They used different systems, from cloud providers to marketing and CRM tools, allowing flexibility and introducing management complexity.

Solution:
A zero-trust approach is an apt solution for complex, multi-layered, and distributed organizations, as zero trust is a design principle rather than a stack or a technology. The business units mount the Cimpress Security decisions and need to abide by the regulations of zero trust. Cimpress Security has cut down the cybersecurity risk for individuals and organizations by implementing the zero-trust security approach. They have this approach presently deployed on the parent company.

Cisco's Zero Trust Journey

Cisco stands as the largest technology company in the world. It is popularly known for its networking products.

Approach:
Cisco's Zero Trust journey involved protecting all applications by validating users and devices and using security tools that promote productivity while securing critical data and information.

Results:
The results of the zero-trust security approach were astounding. Over 100,000 employees, vendors, and contractors, with only 1% support needed, got clear insights into who and what is on the network, allowing faster response time to the potential risks.

Google's Successful Implementation of Zero Trust Model

Google is well-known for paying keen attention to security measures and investing heavily in them. It has implemented a zero-trust model named Beyondcorp. This is built with years of experience at Google and ideas and practices from the community.

Approach:
An initiative that enables every employee to work hassle-free from an untrusted network without needing a VPN. In today's ever-evolving threat landscape, Beyondcorp is used to authenticate and authorize resources and Google's infrastructure.

Results:
Google experienced a reduction in the attack surface. Additionally, it allowed employees to work from anywhere without needing a traditional VPN. This resulted in enhancing the overall security and keeping away from devastating threats and attacks.

The Future Trends of Zero Trust Approach

The future of the zero-trust approach looks promising. Some top trends would take center stage and toil in combination.

AI-Powered Security
Artificial intelligence is a booming technology and is audacious in enhancing cybersecurity frameworks. AI security systems can monitor and analyze large amounts of data to identify patterns and anomalies and predict threats. By leveraging AI, organizations can improve their ability to detect and mitigate cyberattacks, reducing the risk of data breaches.

Biometric Authentication
Passwords, the traditional security approach, are more susceptible to hackers and exploiters. On the other hand, biometric authentication offers your device an additional layer of security. Technologies such as facial recognition, iris scanning, and more are gaining a good grip on the zero-trust security landscape. Integrating biometric authentication and Zero Trust security helps enhance identity verification and boosts security posture. Further, multi-factor authentication is also on the top security feature list.

Access Controls Systems
In recent years, the number of cyberattacks has risen sharply and will continue to grow in the next few years, increasing the computing environment's complexity. The access control system is the future trend in the Zero Trust approach as it incorporates different factors such as the trust degree of users and devices, i.e., location, time, and the current security threat level in the user's environment.

Conclusion

Zero trust security is a sophisticated approach to cybersecurity. It is a pro defender against potential threats and malicious attackers. Zero Trust has overcome the challenges faced by the traditional security method, primarily focused on the user's network location. Alternatively, ZTA relies on continuous authentication and authorization of devices and users.

Organizations looking to experience a risk-driven, adaptive, and pragmatic approach toward security should start implementing the zero-trust security approach. This will not only help to bolster the organization's safety but also help it thrive in the digital-first landscape.

References

Buckbee, M. (2023) What is zero trust? Architecture and security guide.
https://www.varonis.com/blog/what-is-zero-trust

DelBene K, Medin M, Murray R (2019) The Road to Zero Trust Security
https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF

Cloudflare (2023) Zero trust security.
https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

Kaspersky (2020) What is zero trust security? What is it and how does it work?
https://www.kaspersky.com/resource-center/definitions/zero-trust

IBM (2023) What is zero trust?
https://www.ibm.com/topics/zero-trust

RedHat (2022) What is zero trust?
https://www.redhat.com/en/topics/security/what-is-zero-trust

Contact Information

For General Inquiries and Information: david.martin@secureitworld.com

Advertising and Partnerships:

Drop an email to our marketing team at emily.johnson@secureitworld.com for advertising opportunities and potential partnerships.

Your feedback is important to us, and we will do our best to respond to your inquiries promptly.

Thank you for choosing SecureITWorld as your trusted and greatest source for cybersecurity and technology insights.

Feedback and Contributions:

If you have suggestions, would like to contribute to our publications, or have specific inquiries, please get in touch with our editorial team at david.martin@secureitworld.com