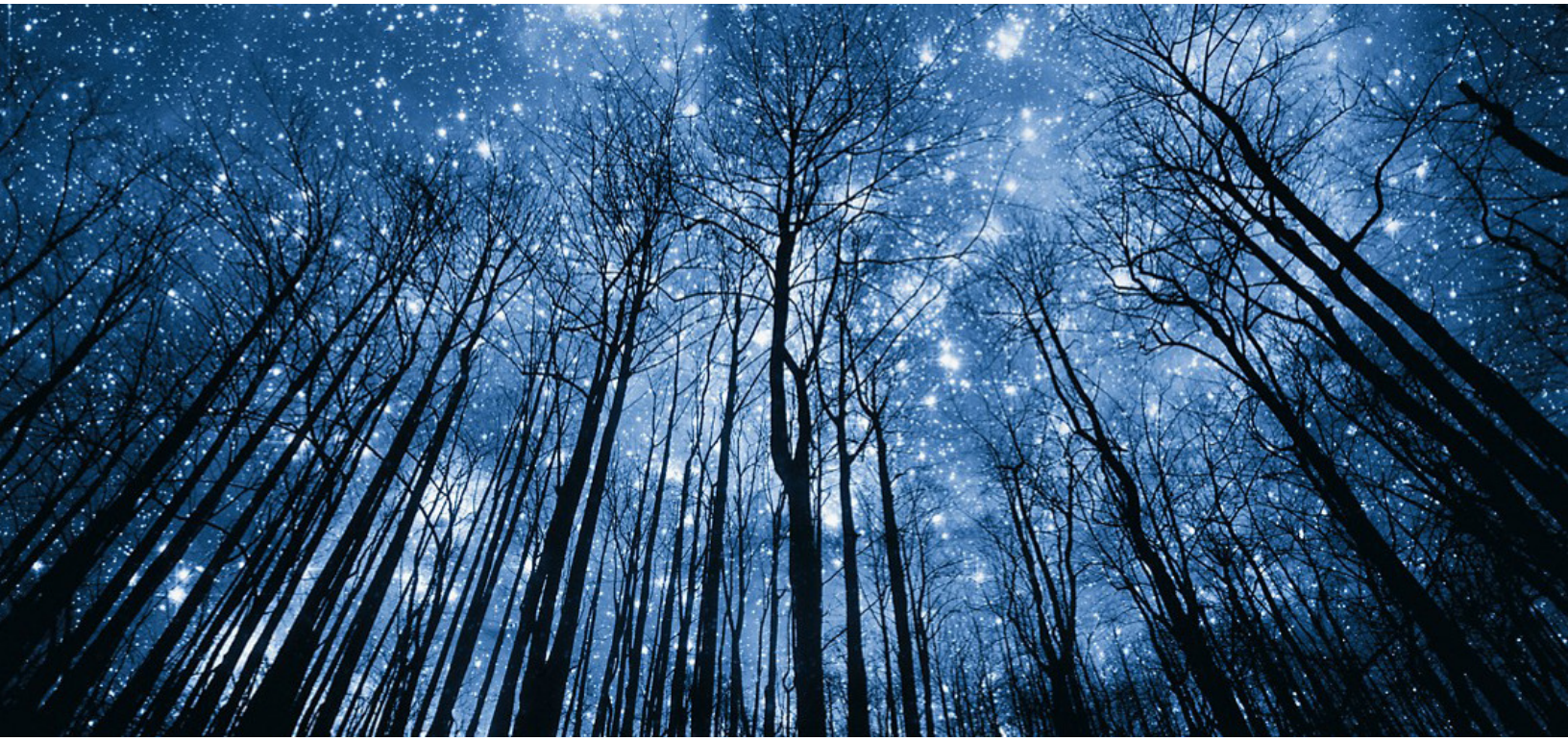
DELL Technologies

ZERO TRUST FRAMEWORK "DON'T TRUST, VERIFY FIRST"



Vishnu Ranya
Specialist 2, Inside Product
Dell Technologies

Rajesh Goda
Principal Systems Engineer

Proven Professional

Knowledge Sharing Article
© 2023 Dell Inc. or its subsidiaries.

Contents

Introduction:

In today's inter-linked world, the conventional paradigm of a business with a perimeter control firewall separating trusted insiders from untrusted outsiders no longer makes sense. An enormous security challenge demands a new approach to extend protection to not only all users and their devices but application and data level in this connected world regardless of their location. Employees, whether permanent or contract, working in hybrid mode as in office or remotely become insider threats, and attackers taking advantage of trust between internal systems or applications again in multi-cloud environment.

The size and severity of cyberattacks have increased. There have been concerns raised regarding the security of our data following the most recent security breach at Samsung, AirAsia, and many other companies where name, contact and demographic information, date of birth, and product registration information were stolen.

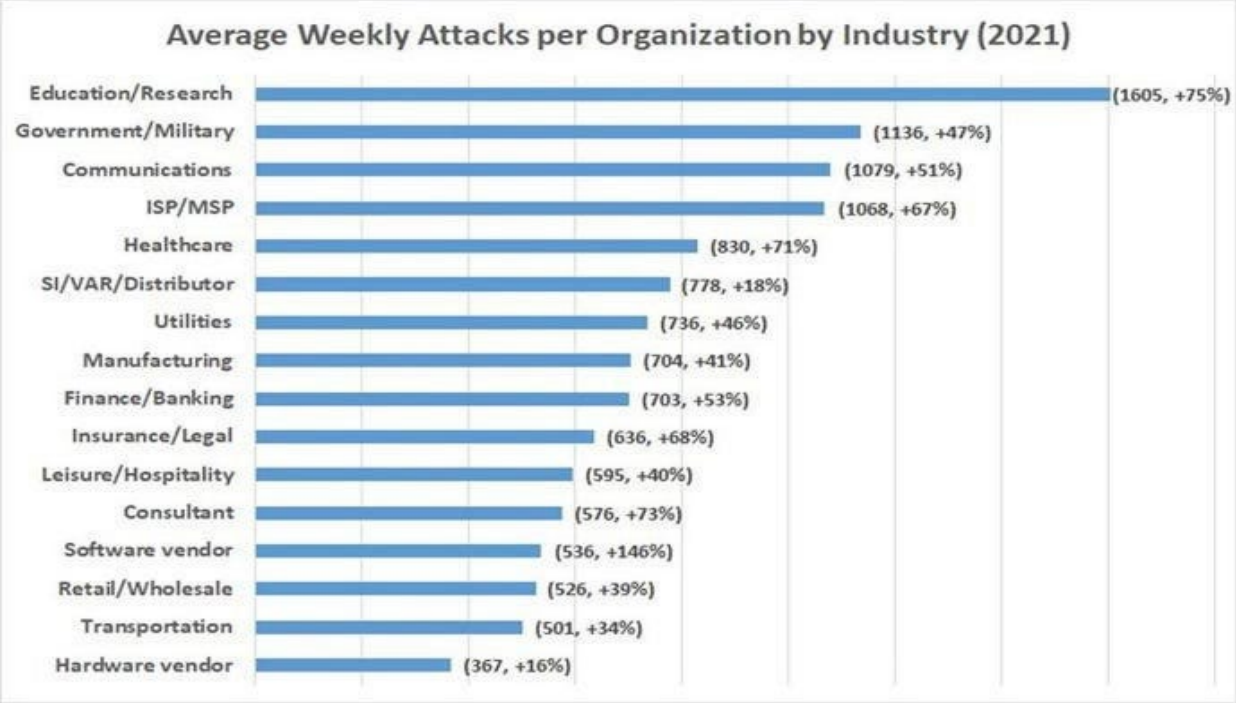


Image-1 (Image source: Forbes: Cyber Statistics for 2022)

There are almost never any days without new, severe cyberattacks making the news. The implementation of a Zero Trust model experienced tremendous rise in acceptance to better defend against data breaches.
The Zero Trust paradigm adopts "never trust, always verify" as its guiding concept as opposed to the conventional method of "trust but verify". [2] We believe this topic assumes significance in the light of all such cyber threats and prepare organizations to adopt “Don’t trust, Verify first”.

[3] The World Economic Forum defines “Zero trust is a principle-based model designed within a cybersecurity strategy that enforces a data-centric approach to continuously treat everything as an unknown – whether a human or a machine, to ensure trustworthy behavior”.

Traditional Digital Security Design Challenges

The traditional model of the Zero Trust Framework posits that organizations should not blindly trust any user, device, or service inside or outside of their network. Instead, they should verify the identity and legitimacy of every user, device, and service before allowing them access to sensitive data or systems. This model relies heavily on perimeter security such as firewalls, virtual private networks (VPNs), and web gateways to keep bad actors out of the network.

Businesses must understand that perimeter-based security, which focuses on securing networks, firewalls, and systems, provides no protection against attacks stemming from insiders or from threats based on identities and credentials. Up until you begin implementing identity-centric security measures, account compromise assaults will continue to make for the perfect cover for data breaches. The conventional Zero Trust Framework concept is no longer sufficient as more businesses implement BYOD policies and migrate their infrastructure to the cloud.

Zero-Trust Model:

The zero-trust model is a security framework that assumes that any device or user attempting to access a network or system is potentially untrustworthy and therefore must be thoroughly authenticated and authorized before being granted access. The goal of a zero-trust model is to reduce the attack surface of a network or system by limiting access to only those resources that are strictly required for a user or device to perform its intended function.

Background:

John Kindervag of Forrester Research originally put up the Zero Trust Framework in 2010 to address the rising number of security threats and data breaches that were evading perimeter-based security solutions. The paradigm attempts to give a more safe and adaptable approach to network security and is founded on the maxim "never trust, always verify."

Components of Zero Trust Framework:

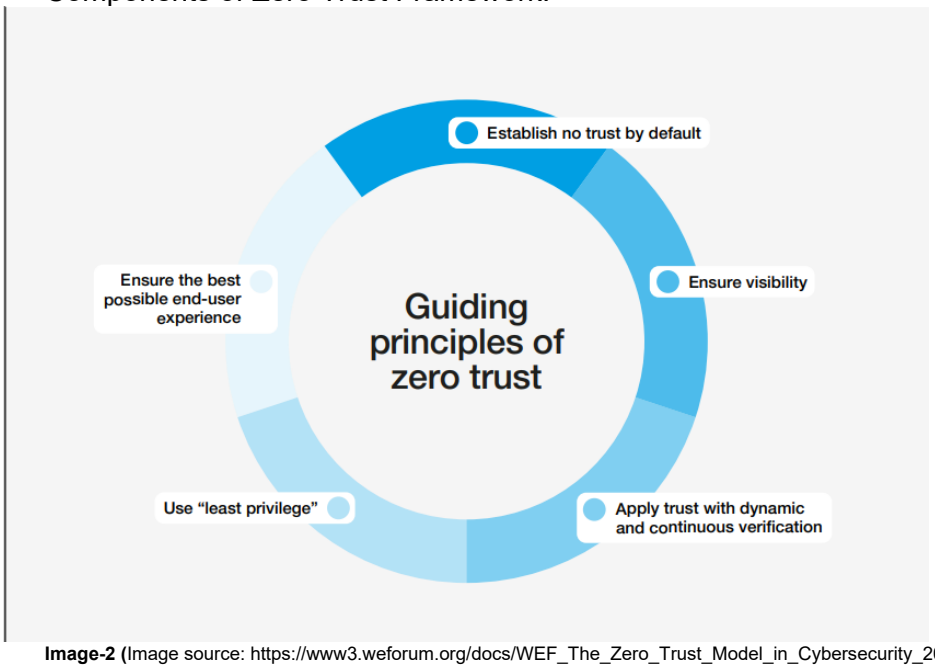


Image-2 (Image source: https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf)

To deploy a zero-trust framework, you will need to follow these steps.

- **Identify your assets:** The first step in deploying a zero-trust framework is to identify all the assets that you want to protect, including devices, data, and systems.
- **Micro segmentation:** To divide the network into smaller, more secure zones, this ZTF component uses network segmentation. This makes it possible to isolate sensitive data and implement granular access controls.
  One key aspect of zero trust architecture is the use of multi-factor authentication (MFA) to verify the identity of users attempting to access the network. MFA requires users to provide multiple forms of evidence to prove their identity, such as a password, a security token, or a biometric factor like a fingerprint.
- **Least Privilege:** This component of ZTF involves granting users and devices the minimum access necessary to perform their duties. This helps to reduce the attack surface and limit the damage that can be caused by a security breach.
- **Continuous Monitoring:** This component of ZTF involves the continuous monitoring of network traffic and user activity to detect and respond to security threats in real-time. This may include using tools such as intrusion detection systems (IDS) and security information and event management (SIEM) systems[2]. These tools can alert security personnel to potential threats and help them to respond and recover in the event of a security incident.
- **Respond and recover:** If you do detect a security incident, it is important to have a plan in place to respond and recover. This may include isolating affected systems, restoring from backups, and implementing any necessary patches or updates to prevent future incidents.

Benefits of Zero Trust Framework:

- **Improved Security:** ZTF approach assumes that all traffic and incoming data is harmful/malicious and needs check at every point-of-time.
- **Increased Visibility:** ZTF offers enterprises more network visibility and aids in the timely detection and mitigation of security threats by continually monitoring network traffic and user activities.
- **Compliance:** For organizations, achieving, auditing, and maintaining compliance is a constant and resource-intensive process. Organizations are given the visibility they require by Zero Trust Privilege to guarantee ongoing compliance.
- **Reduced Risk:** With 80 percent of breaches involving compromised privileged credentials and as much as one-third of breaches committed by “trusted” insiders, a properly implemented Zero Trust Privilege strategy can help organizations reduce the risk of breach by 50 percent[2].
- **Scalability and Flexibility:** The use of cloud-based security solutions in ZTF provides organizations with more scalable and flexible security options.
- **Digital transformation:** According to a February 2019 Forbes article, “Zero Trust Privilege . . . is the force multiplier digital transformation initiatives need to reach their true potential.” Zero Trust Privilege enables organizations to accelerate their cloud, DevOps, IoT, and other digital transformation initiatives with confidence[2].

Evaluate the Maturity Level of an Organization's Use of Zero Trust Privilege:

Cybersecurity and Infrastructure Security Agency (CISA) defines a model that represents a gradient of implementation across five distinct pillars. The pillars, depicted in the below figure, include Identity, Device, Network, Application Workload, and Data. Each pillar also includes general details regarding Visibility and Analytics, Automation and Orchestration, and Governance[8].

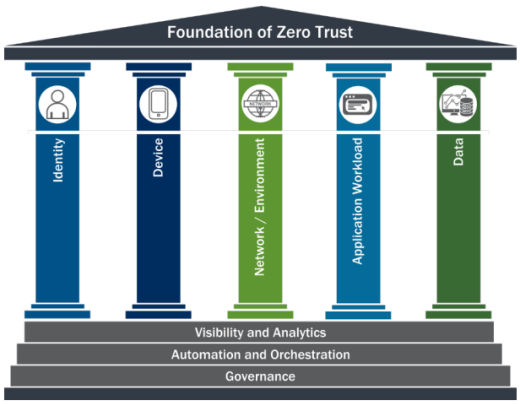


Image-3 (Image source: CISA Zero Trust Maturity Model)

1. **Identity**: An identity refers to attributes that describe an organization user or entity. Organizations should ensure the right users should have access to right resources at the right time.
2. **Device:** Organizations should ensure to inventory and manage all the DTLT's, Mobiles, BYOD's to prevent unauthorized devices from accessing company resources.
3. **Network/Environment:** This pillar refers to Internet, Wireless networks etc. Organizations should ensure to isolate these data flows from external access.
4. **Application Workload:** All programs, systems and services comprise of workloads. Organizations should manage the application layer workflow to ensure secure delivery.
5. **Data:** Organizations should categorize, label, protect data to prevent any spillage of data outside the organization.

Challenges to Adopting a Zero Trust Framework:

There are several challenges to adopting a Zero Trust Framework, including;

- **Complexity:** Implementing a Zero Trust Framework can be complex and requires a significant investment in infrastructure and resources.
- **Changing organizational culture:** Adopting a Zero Trust mindset requires a shift in thinking and can be difficult to implement across an entire organization.
- **Integration with existing systems:** Integrating a Zero Trust Framework with existing systems and networks can be challenging.
- **Lack of standardization:** There is currently no standard for implementing a Zero Trust Framework, which can make it difficult for organizations to know where to start.
- **Managing access:** Managing access to resources and applications in a Zero Trust environment can be difficult, as it requires a high level of granularity and the ability to quickly revoke access.
- **Cost:** Implementing a Zero Trust Framework can be costly, as it requires significant investments in new technology and infrastructure.
- **Continuous monitoring:** Maintaining a Zero Trust Framework requires continuous monitoring and updating of security controls and policies.

Dell Technologies Zero Trust Solution :

Dell Technologies Delivers Zero Trust, Cybersecurity Solutions to Protect Multicloud and Edge Environments[6].

Image-4 (Image source: Dell Technologies Info Hub)

To give corporations a safe data center to test Zero Trust use cases, Dell will power the Zero Trust Center of Excellence at DreamPort along with MISI, CyberPoint International, and a group of industry small, women-owned, and veteran-owned firms. The Department of Defense Zero Trust Reference Architecture will serve as the Center of Excellence's foundation as businesses test configurations before deploying them in their own environments.

Dell will give a reproducible blueprint of the architecture by orchestrating across a broad ecosystem, lowering the integration and orchestration complexity for clients, and enabling a shorter adoption path[6].

Dell Cybersecurity Advisory Services offer enterprises a roadmap to Zero Trust that builds on their current cybersecurity assets to assist organizations in aligning to Zero Trust principles and achieving cyber resiliency. These services assist customers identify and close security holes, decide which cutting-edge technology to deploy, and learn how to maintain ongoing vigilance and governance for long-term cyber resilience. Organizations who partner with Dell have access to the tools and practical knowledge they need to secure their data and IT environments more effectively[6].

To reduce attack surfaces and better safeguard organizations, Dell now provides a new Vulnerability Management service with Dell specialists that frequently scan customer environments for vulnerabilities, present a complete picture of exposures, and help prioritize patching operations.

Other Industry available models of Zero Trust:

- **Cloudflare manages zero-trust access controls[3]**
  Security product developer Cloudflare was in a unique position to address this issue for both it and its clients. With a zero-trust philosophy, it created Cloudflare Access to protect its software-as-a-service (SaaS) and internal applications. Onboarding and offboarding of employees and contractors became significantly easier after securing its internal applications. Now, access to the necessary applications is rapidly offered to each new employee and contractor. Access allows for the granular assignment of permissions to staff members and independent contractors as well as the security team's ability to spot suspicious activity on any applications by validating every packet. More thorough management of attack surfaces is made possible by improved visibility and more granular control taken together.

- **Zero trust as a fundamental security pillar for Eni**[3]
  Eni will concentrate on user and device identities to create security around this new organizational boundary. Eni is advancing its access procedures with cutting-edge, adaptable technologies that enable ongoing risk analysis.
- **Identity & Endpoint Protection with Microsoft Zero Trust**
  Enables enterprise customers to innovate and secure their existing Microsoft Cloud and On Premises Infrastructures while partnering with Dell Technologies, creating a trusted advisor relationship.
- **Protect your data and your business with Unisys Cybersecurity solutions**[7]
  The scalable Zero Trust architecture made possible by Unisys' cybersecurity solutions allows remote users to access only the resources they need, not the entire network.

Conclusion

The powerful idea of zero trust might help to strengthen a company's cybersecurity position. To realize its full potential, it must be analyzed in the context of the present security practices. A thorough understanding of industry best practices, a clear deployment plan based on a set of guidelines that apply to the organization's current circumstances, and a futuristic outlook in which technology plays a prominent role are necessary for the successful implementation of zero trust.

Through the publication of this Whitepaper, we hope to shift the perception of Zero Trust from one of a final goal to one of a journey with each employee having a part to play in accepting, implementing, and consistently testing the model for a stronger security posture.

Bibliography

1. *Cost of a data breach 2022* (no date) *IBM*. Available at: https://www.ibm.com/reports/data-breach (Accessed: January 17, 2023).

2. *Zero trust privilege for dummies* (no date) *PDF eBook*. Available at: https://delinea.com/resources/zero-trust-privilege-for-dummies-pdf (Accessed: January 17, 2023).

3. *The 'Zero Trust' model in cybersecurity: Towards understanding and ...* (no date). Available at: https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf (Accessed: January 17, 2023).

4. *Cybersecurity White Paper* (no date) *LeadingAge*. Available at: https://leadingage.org/cybersecurity-white-paper/ (Accessed: January 17, 2023).

5. *National Institute of Standards and Technology* (2023) *NIST*. Available at: https://www.nist.gov/ (Accessed: January 17, 2023).

6. *2022.10.04: Dell Technologies Delivers zero trust, cybersecurity solutions to protect Multicloud and Edge Environments* (no date) *Computers, Monitors & Technology Solutions*. Available at: https://www.dell.com/en-us/dt/corporate/newsroom/announcements/detailpage.press-releases~usa~2022~10~10042022-dell-technologies-delivers-zero-trust-cybersecurity-solutions-to-protect-multicloud-and-edge-environments.htm#/filter-on/Country:en-us (Accessed: January 17, 2023).

7. *Cybersecurity Solutions* (2022) *Unisys*. Available at: https://stealthsecurity.unisys.com/products-services/?_ga=2.109608581.1211913317.1669181089-1762570207.1668608552 (Accessed: January 17, 2023).

8. *Cisa Zero Trust Maturity Model* (no date) *CISA Zero Trust Security Model*. Available at: https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf?trk=public_post_comment-text (Accessed: January 17, 2023).

Dell Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Disclaimer: The views, processes or methodologies published in this article are those of the authors. They do not necessarily reflect Dell Technologies' views, processes, or methodologies.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL TECHNOLOGIES MAKES NO RESPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell Technologies software described in this publication requires an applicable software license.

Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.