Blog · 3 Min Read

Zero Trust Architecture: Redefining network security for complex digital environments

As businesses face new challenges such as corporate mobile applications and cloud access, traditional security models may struggle to keep pace. Zero Trust Architecture offers a modern solution to these evolving network security challenges.

Mohan Krishnamurthy Madwachar • ETGovernment
Updated On Aug 12, 2024 at 03:45 PM IST

Zero Trust is a cybersecurity model based on "never trust, always verify."

In the world of network security, trust is not as straightforward as it seems. Traditionally, the security model revolved around a clear distinction: the internal network was deemed trustworthy, while external networks were considered potentially dangerous.

This dichotomy often involved a De-Militarized Zone (DMZ) that provided controlled access to resources.

However, as we navigate the complexities of today's hybrid work environments and cloud computing, this traditional approach has proven inadequate. Enter Zero Trust Architecture (ZTA)—a paradigm shift in network security designed to address the modern challenges of a dynamic digital landscape.

Zero Trust is a cybersecurity model based on "never trust, always verify." Unlike traditional models that automatically trust internal traffic, Zero Trust treats all access requests with suspicion, requiring strict verification regardless of location.

As hybrid work, cloud computing, and mobile access blur traditional security boundaries, internal networks face new threats. Zero Trust focuses on continuously assessing who needs access, why, and under what conditions, rather than relying on trust based on network location.

Imagine trust as concentric circles, with the innermost circle reserved for your most trusted relationships. In the realm of network security, this model translates into a framework where trust is not granted automatically based on network location but is continuously assessed based on user identity, device, and the context of the access request.

Core Principles of Zero Trust

Implementing Zero Trust involves several key principles:

- **Least Privilege Access Control**: Users are granted the minimum level of access required to perform their tasks. This principle limits the potential damage from compromised accounts or insider threats.
- **Continuous Monitoring**: Rather than periodic checks, Zero Trust requires ongoing monitoring of user activity, network traffic, and system health. This real-time approach helps detect and respond to threats more effectively.
- **Multi-Factor Authentication (MFA)**: MFA adds an additional layer of security by requiring multiple forms of verification before granting access. This could include a combination of passwords, biometrics, and authentication tokens.
- **Micro-Segmentation**: This involves dividing the network into smaller, isolated segments to limit the spread of potential breaches. Even if an attacker gains access to one segment, they cannot easily move to others.

Adopting a Zero Trust Architecture is not about purchasing a product with a plethora of features; it requires a thorough understanding of your existing infrastructure, user needs, and access patterns. Organizations must evaluate their network topology, user roles, and access requirements to effectively implement Zero Trust.

Successful implementation hinges on a deep knowledge of the business, its employees, and its customers. It involves scrutinizing who needs access to what resources, how they connect, and whether their access exceeds what is necessary for their role. This granular approach helps prevent data breaches and enhances overall security posture.

As businesses face new challenges such as corporate mobile applications and cloud access, traditional security models may struggle to keep pace. Zero Trust Architecture offers a modern solution to these evolving network security challenges. By moving away from the outdated notion of inherent trust, Zero Trust provides a robust framework that adapts to the realities of today's interconnected world.

By embracing a Zero Trust approach, organizations can enhance their security measures, improve user experience, and, most importantly, safeguard against data breaches in an increasingly complex digital environment. Trust, after all, is no longer given freely—it must be earned and continually verified.

(The author is Country Manager, Sattrix India; Views are personal)

Published On Aug 6, 2024 at 02:24 PM IST

Zero Trust Architecture · network security · digital environments · cybersecurity model · cloud computing · hybrid work · continuous monitoring · data breaches · zero trust · enter zero trust architecture

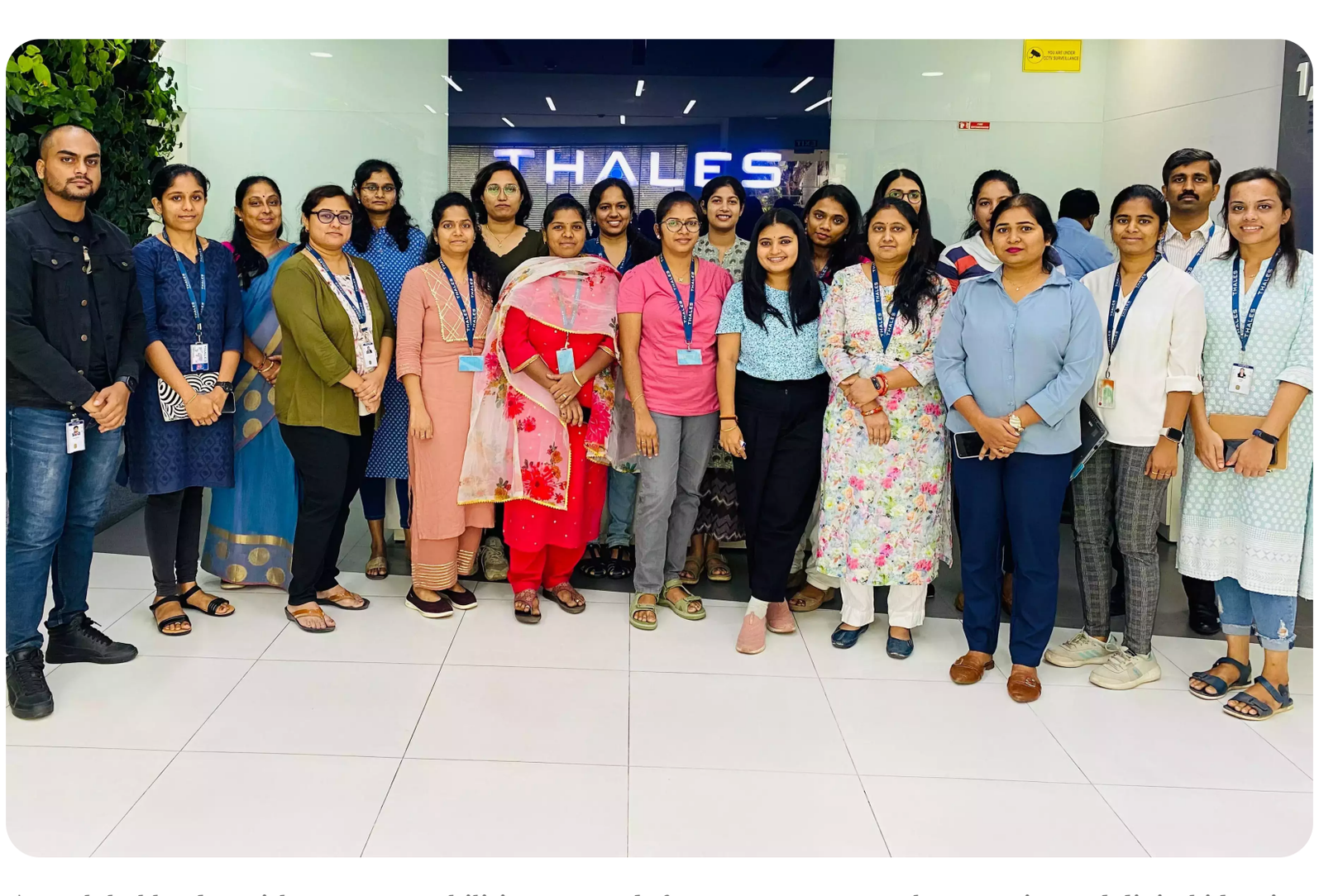
Next Story

Blog · 3 Min Read

Bridging the gender gap and empowering women in engineering

According to the World Economic Forum's Global Gender Gap Report of 2024, while women's representation in both STEM and non-STEM workforces has increased since 2016, they remain underrepresented in STEM roles, comprising only 28.2% of the STEM workforce compared to 47.3% in non-STEM sectors worldwide.

Ashish Saraf • ETGovernment
Updated On Aug 6, 2024 at 11:12 AM IST



As a global leader with strong capabilities across defence, aerospace, cybersecurity and digital identity, Thales is dedicated to empowering women across all levels.

It is heartening to see the growing participation of women engineers in India and abroad. With India emerging as a global powerhouse in the field of technology, the role of women in this sector is more crucial than ever before.

While women are making significant strides and breaking barriers by taking up STEM (science, technology, engineering, and mathematics) to build their careers, organisations continue to prioritise efforts to increase representation of women in the technology and engineering sectors.

According to the World Economic Forum's Global Gender Gap Report of 2024, while women's representation in both STEM and non-STEM workforces has increased since 2016, they remain underrepresented in STEM roles, comprising only 28.2% of the STEM workforce compared to 47.3% in non-STEM sectors worldwide. Additionally, women comprise over half of the workforce base in non-STEM roles, as compared to only one third in STEM. This shows the need to increase women's participation at all levels.

Notably, social and cultural barriers, along with the perception that certain engineering streams are more suitable for men, act as a deterrent for young women from considering engineering as a career. Additionally, the lack of female mentors and role models in engineering further diminishes their interest.

Key Drivers for Encouraging Women to Pursue Engineering

Today, organisations strongly believe that gender diversity is not just a matter of providing equal opportunities, but it is also essential for driving innovation and optimising the overall performance of businesses. Women engineers have shown their capability to contribute to cutting-edge technologies that transcend disciplines and transform ideas into actual solutions.

Recognising the benefits of having diversity in the workforce, organisations across India are trying to address the gender gap in engineering roles, implement strategic initiatives to inspire and empower young girls to pursue careers in engineering. To empower women in this field, global technology firms like Thales, are taking proactive steps to create equal opportunities for women to progress in their careers. This involves implementing strategies at every level of the organisation, from recruitment and retention to mentorship and leadership development.

As a global leader with strong capabilities across defence, aerospace, cybersecurity and digital identity, Thales is dedicated to empowering women across all levels. The organisation has been promoting women employees to higher levels of responsibility along with increasing their representation on management committees. Our in-house women leadership development programmes such as Fly High, employee resource groups and forums, international mentoring exchanges, diverse and flexible employee friendly policies such as hybrid working, maternity leaves and insurance policies in addition to an unbiased approach helps in creating an inclusive and respectable workplace.

The Journey Towards an Inclusive and Trusted Future

We call on all organisations to reaffirm their commitment to creating an inclusive environment where women can excel in engineering and pursue their dreams without any barriers.

In the ever-evolving technological landscape, organisations are striving to build diverse teams with women leaders and engineers that can bring unique perspectives, problem solving approaches and innovative thinking to the workplace.

Encouraging young girls to take up engineering as a career, increasing the number of women engineers at various levels of the organisation, and promoting them to leadership positions can help in building a future of trust where everyone has equal opportunities to drive innovation and contribute towards the overall growth of society.

Published On Aug 6, 2024 at 11:12 AM IST

women engineers · gender gap · STEM · empowering women · Thales · fly high · world economic forums global gender gap report