Infosys®
Navigate your next

VIEWPOINT

# ‘ZERO TRUST’ REQUIRES SOPHISTICATION

Employees are almost as likely as hackers to be a threat to your business data. One way of tackling this is through a “Zero Trust” strategy. But this should not be about locking everything down. Instead, businesses need to better monitor and understand trusted behaviors.

Infosys® | Knowledge Institute

Total business loss from cybercrime will rise to $6 trillion in 2021, up from $3 trillion in 2015. [1] A significant proportion of this crime is caused by internal actors. It can often feel like a business that is trying to protect its data simply doesn't know who to trust anymore.

Zero Trust was defined as an approach to protect against cybercrime back in 2010, by John Kindervag at Forrester Research. But more recently, it has grown as a popular concept in cybersecurity circles. The often oversimplified and common narrative is that companies should not trust anyone, and that they should verify all the possible parameters before providing access to any information. But applying Zero Trust effectively requires a lot more sophistication.

## Who to trust?

Zero Trust is different from its predecessors. Earlier approaches to information security focused on protecting the external perimeter — ensuring that no "outsider" could enter (e.g., through the use of firewalls or virtual private networks) and gain access to important information. The assumption was that anyone on the inside wasn't a threat. But today, insider threats are becoming more frequent. According to Verizon's 2019 Data Breach Investigations Report, 34% of breaches that occurred in 2018 involved internal actors. [2]

This does not necessarily mean that a third of employees are criminals. Often, these actors are unaware that they have enabled a breach. Today's users and devices often interact outside the corporate perimeter (Figure 1) and can bring in unwanted threats. So does that mean companies literally cannot trust absolutely anyone and anything?

Security architecture has always relied on trust models. Yet the common narrative about Zero Trust has a few misconceptions. First, the model is often perceived as an alternative to earlier approaches to information security and as a replacement, rather than as something that can coexist with the other models. Second, it is perceived as an absolutely binary approach. A company can either have it or not. There is no middle ground.

But this is not the case. To be effective, Zero Trust relies on a much more sophisticated understanding of how to balance the needs of a business, its employees and its partners with the need for security. To understand this better, we must first consider the meaning of the word "trust."

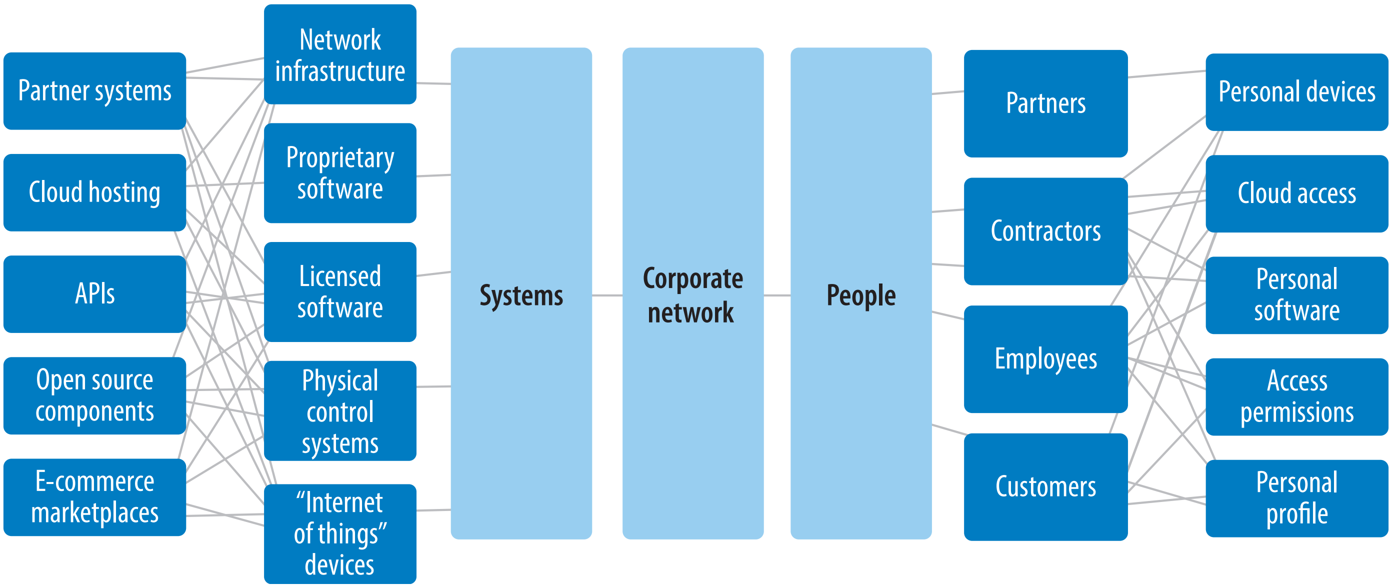
## What is trust?

Trust is defined in the dictionary as a firm belief in the reliability, truth or ability or someone's strength. In the digital world of cybersecurity, the use of the word trust is very intriguing. It is not only a feeling of confidence and security in someone or something, it is also a set of expected behaviors or an abstract mental attitude.

Trust creates conditions that lead to the emergence of new capabilities between parties that otherwise wouldn't exist. Without digital trust, companies could not innovate quickly, as they would always be on the defensive — unsure whether to rely on their colleagues to deliver their needs.

According to Gartner, "Trust is the bidirectional belief established

Figure 1. As businesses become more connected and flexible, securing trusted touchpoints becomes increasingly complex.



Source: Infosys Knowledge Institute

between two entities that the other entity is what it claims to be and that it will behave in expected ways during the duration of the interaction. Trust leads to access to capabilities between the entities that otherwise should not be possible."[3]

Furthermore, there are several implications to this, say Gartner. First, "Trust is not inherently a good thing. Trust is what we use in lieu of absolute certainty. However, we need trust to extend or access capabilities that otherwise should not be possible."[3] Take, for example, customer trust. When a person buys something online from Amazon, he or she doesn't know for sure whether the product's described qualities are true. By making a purchase, customers believe that their expectations will be met. Before they believe, they need to be able to trust the provider. Customers' trust can disappear at any time. Nevertheless, it is a mandatory and necessary stage in the formation of belief.

Second, "Trust is not absolute, binary or static. It is an indication of the relative level of strength of the assurance of the belief. Further, the level of trust is dynamic and changes over time. Thus, access to the capabilities should be adapted."[3]

> Lack of digital trust would slow down the ability of companies to innovate while making them defensive

Most "data leakage" incidents occur due to human mistakes. Insiders are particularly dangerous. They are just ordinary users of corporate IT systems such as employees, contractors and customers. All it takes is one careless mistake. Many insider users become victims of social engineering attacks such as phishing via email or social networks. And some leak confidential information on purpose.

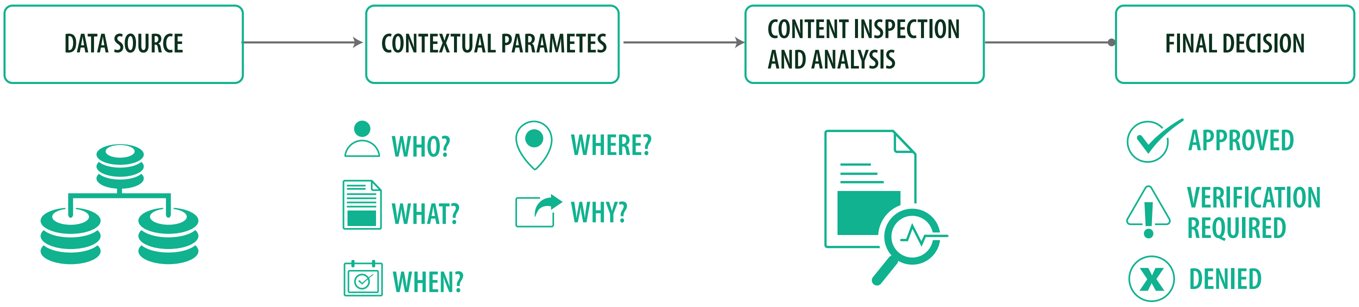
Third, "To compensate for the risk of extending capabilities based on a belief, we should monitor for expected behaviors during the interaction. If behaviors deviate from expectations in a risky way, access to the capabilities should be adapted or removed entirely."[3]

For us humans, trust is a feeling. This feeling is contextual and built on endorsements or past experiences. But what about trust in the cybersecurity world? Is digital trust absolute or contextual?

## Explaining the Zero Trust model

Companies have to think of Zero Trust as an additional layer to existing security. This approach is not binary. It is actually more about understanding behaviors and expectations. And that means understanding the context is key.

Figure 2. Contextual control prevents leaks by blocking unauthorized attempts to transmit data.



Source: Infosys Knowledge Institute

Sometimes people will work on specific projects or initiatives that may require additional access to resources. Someone from a finance department may need access to an employee database. Granting or denying access in this case depends on that person meeting certain requirements.

In the security world, these decisions are based on the foundation that prior to approving, denying or verifying a data transaction one would have to validate the Five W's: Who, What, When, Where and Why (Figure 2). This makes digital trust contextual.

The field of information security is and will always be a risk management function. The most common characteristics of the risk management function are trade-offs. They are risk acceptance decisions. During the implementation of security controls, trade-offs occur across different stages. And before making a final decision, one will have to make final adjustments and implement appropriate security controls based on a risk assessment.

The main assumption of Zero Trust is not about trusting nobody. It is that your company is constantly being compromised. It also means that the traditional model of perimeter-based security is outdated. Therefore, businesses need to implement continuous security controls within and outside the perimeter, i.e., across people, devices, data, networks and workloads. This can be done through a combination of strategies that includes strong identification, authentication, authorization, isolation, segregation, encryption, obfuscation and automation tools.

> Zero trust is about operating under the assumption that your business is constantly compromised

## More than Zero Trust

The pure English meaning of the word combination "Zero Trust" challenges the risk management principles, adaptive nature of security controls, defense in-depth principles and trust relations across entities in security management.

Businesses can't have zero trust — it will kill them. What they need to do is to continuously monitor against behaviors and expectations. This will enable them to proactively discover, assess and prioritize risks. They need to understand what the expectations are to use a certain application or data. They need to analyze the behaviors within the system that people, devices and applications are displaying. Based on that, they need to design contextualized security controls that determine final decisions. Flexibility is important.

To leverage Zero Trust into any security program, businesses can take the following three steps: First, operate under the assumption that the business is constantly under attack. Build security controls and responses based on this assumption. Second, replace the traditional model of perimeter-based security with context-aware, flexible and programmable security platforms. Discover, assess and monitor threats continuously. Third, design integrated, flexible and programmable security into systems, processes and people from the start. This approach will create an adaptive system that is not binary and understands context and expected behaviors. It will allow businesses to maintain defense in-depth principles and build trust across entities. Moving away from the security posture of default denial, this approach will help design and build strong multidimensional and comprehensive security parameters.

## References

[1] Global cybercrime damages predicted to reach $6 trillion annually by 2021, December 7, 2018, Cybersecurity Ventures, Cybercrime Magazine

[2] 2019 Data breaches investigation report, 2019, Verizon

[3] Zero trust is an initial step on the roadmap to CARTA, Neil MacDonald, December 2018, Gartner, (Gartner subscription required)

## Authors

**Vishal Salvi**

*SVP and Chief Information Security Officer, Infosys*
Vishal.Salvi@infosys.com

**Yulia De Bari**

*Consultant, Infosys Knowledge Institute*
Yulia.Debari@infosys.com

## About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next