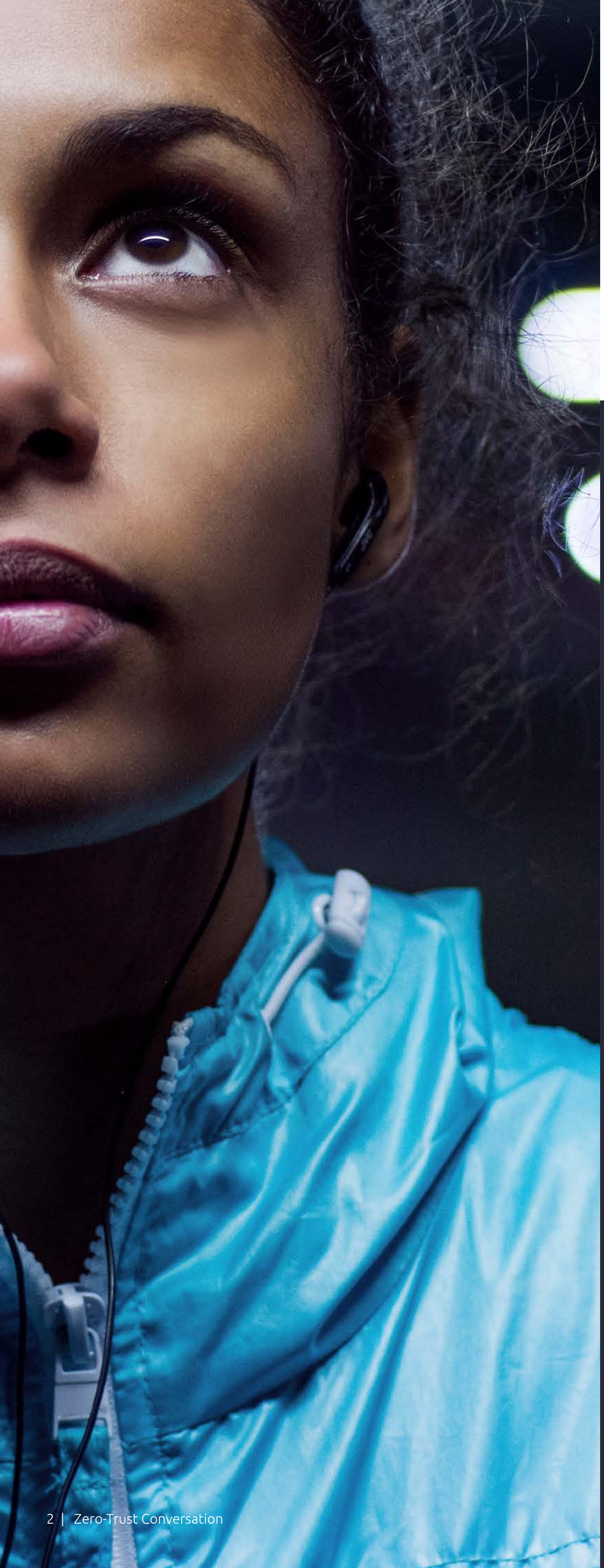
WHY IT'S TIME FOR A ZERO-TRUST CONVERSATION



WHY IT'S TIME FOR A ZERO-TRUST CONVERSATION

20 years ago, cybersecurity was little more than an idea. In the time since it has climbed up every business's agenda to the point that most organizations have built an effective fortress to protect their network.

But the last few years have reduced secure castles to rubble. A global pandemic has taken us into a new era of hybrid working, while at the same time, an avalanche of new technologies arrived at industries, changing the goalposts forever.
These seismic changes directly impact cybersecurity and no player, however large or small, can afford to sit still.

Before the pandemic, a successful attack could be damaging and, in some cases, existential, but the sophistication of attacks has escalated leaving a far wider scope of businesses more vulnerable. It is not enough for cybersecurity to merely adapt; it's time to rethink our approach entirely – this is why we're calling for **zero-trust.**

WHAT IS ZERO-TRUST?

Zero-trust security is exactly what it sounds like: don't trust anyone when it comes to cybersecurity. Whether CEO or intern, every user is guilty until verified. This means access must be granted every time a user picks up their tools - eliminating any room for doubt and allowing for better monitoring of unusual behavior.

By focusing on protecting data, adopting zero-trust enables organizations to secure information on any platform, legacy system, hybrid cloud, API, or SaaS application. As much as marketing might say otherwise, there is no one-size-fits-all for zero-trust coverage; in other words, it cannot be bought. Instead, zero-trust is really an umbrella concept with a range of implications that frames an approach to cybersecurity, rather than pertaining to a particular technology.

Achieved by setting a comprehensive strategy that leverages existing investments with new capabilities, zero-trust provides a security framework based on asset or data-centric security, policy-driven controls, modern identity management, and security zones.

So, before we dive into the details of how we achieve with zero-trust, let's consider: why now?

WHY ARE WE HAVING A ZERO-TRUST CONVERSATION?

IT security is becoming increasingly complex. New technologies such as nanotech, quantum computing, and robotics, are soon to arrive in industries already grappling with the likes of IoT, 5G and the edge.

While such digitization brings extraordinary capabilities, it also carries a mountain of new threats as the endpoints – and so ways of entry – are multiplying many times over. Stretched further by the remote working revolution, more and more assets are leaving a central network to multiple devices which might span varying geographies and time zones.

This is changing the type of attack as well as the level of threat. Once upon a time, a "Trusted Network" security strategy was sufficient to counter a network-based attack - picture a castle wall keeping attackers outside, with those inside roaming free in relative safety. But it is now those inside who represent just as much risk. Phishing and credential theft is abundant as hackers try to go through the back door, leaving security teams overwhelmed.

It might be against human nature, but an approach that trusts nobody - wherever and whoever they are - is the most effective way to counter evolving threats.

WHY ZERO-TRUST MAKES BUSINESS SENSE?

In the past, cybersecurity was perceived to be done for the sake of doing cybersecurity. Today, it is integral to a business's success and the ease with which it can pivot to environmental changes. We see three key reasons why adopting the zero-trust approach specifically makes business sense.

Firstly, implementing a zero-trust approach will better prepare an organization for changes to technology, regulation, geopolitics, culture, and even new partnerships. It not only enables businesses to get ahead of changes before they happen but allows them to accelerate digital transformation initiatives with lower risk at the same time.

Secondly, zero-trust bolsters business support. By building effective trust policies, such as those when people change roles, the approach mitigates risks associated with the wrong people having access to information they shouldn't. By implementing better asset identification, businesses will gain better overall visibility of trusted networks which applies as much to new ventures and acquisitions, as it does to people.

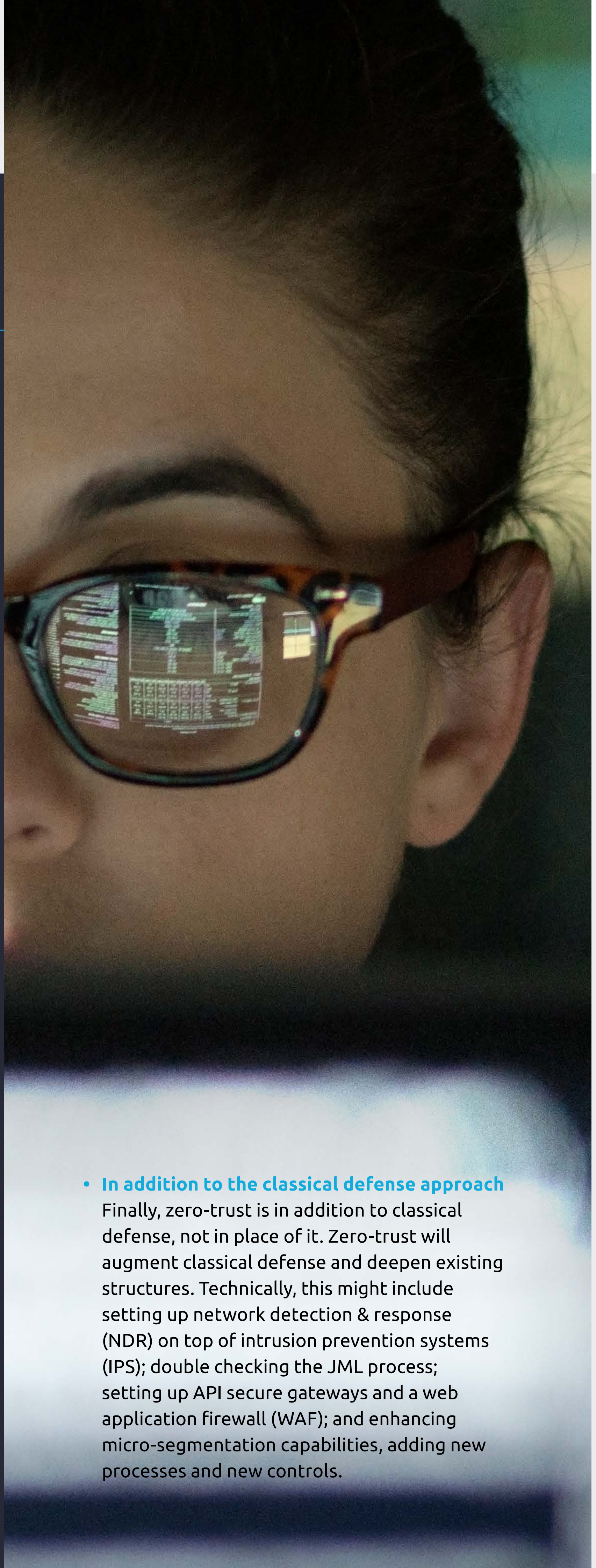
Finally, the result for IT and security will be a simplified, cost-effective architecture, with a clear view of technical risks and better prevention of common ones. It also opens the door for Passwordless security which will make securing the workplace easier in the future.

CONCEPTUALIZING ZERO-TRUST

To apply the framework, you must know the concept's objectives. We see these as fourfold: give access to data on a need-to-know basis, adapt policies to the needs of data use, always verify and never trust, reduce impact in case compromising, and finally, build on classical defenses.

In a nutshell, this means:

- **Access to data on a need-to-know basis**
  Every organization must know their data, what category it fits into, and where it's stored. Every access path must be controlled with watertight asset management and identity and access management (IAM) processes. Key to this is ensuring strong communication between HR, procurement, and IT so that Joiner-Mover-Leaver (JML) policy leaves no room for access when employees come and go. This is not a small task, but it is an essential one.
- **Adapt policies to data use needs**
  Industry-wide policies on data management are a work in progress. Policies will need automation to be technically implemented and should be enforced in a distributed manner. For organizations with large legacy systems and hard to reach data, this is easier said than done. In such instances, zero-trust should be thought of pragmatically – it is not necessarily appropriate to try to deploy in every example.
- **Reduce impact in case of compromising**
  Some points, like network zoning are easier to manage and many businesses will be well on their way with this journey. What this essentially means is locking groups of assets behind doors to ensure one pass can't access all areas. Network security is often the strongest pillar of cybersecurity for business, but zero-trust asks for a deeper understanding of networks and assets. Precise asset management is better than application-level management, so you must know your network components.



- **In addition to the classical defense approach**
  Finally, zero-trust is in addition to classical defense, not in place of it. Zero-trust will augment classical defense and deepen existing structures. Technically, this might include setting up network detection & response (NDR) on top of intrusion prevention systems (IPS); double checking the JML process; setting up API secure gateways and a web application firewall (WAF); and enhancing micro-segmentation capabilities, adding new processes and new controls.

HOW TO MAKE THE JOURNEY TO ZERO-TRUST

To embrace zero trust concepts, we say it is imperative you get the basics right before anything else. There is no easy shortcut to zero-trust, so you must be thorough in approach and pragmatic in outlook.

For an effective strategy, here's what you need to do at a basic level:

- **Review the JML process and its implementation**
  An inefficient leavers process can cause headaches, but the risks are too great to ignore. To establish zero-trust, organizations need to ensure there is double control of employees or partners who leave the business. HR, IT, and when necessary, procurement must work together to ensure network access is blocked on time.
- **Assess the mover process**
  Toxic combinations are created when a user has inappropriate access to critical assets. For instance, a poorly monitored moving process might result in an employee being able to create a transaction and validate it at the same time. AI will be key to avoiding such instances of 'God mode' but the first line of defense is to simply ensure two people control the separate functions.
- **Automate asset management**
  This starts by defining your assets (hardware, software, applications, CIA values, risks related to applications hosted, hosted data classification), then tagging them to ensure they are easy to identify and strong enough to ensure zero-trust objectives. Finally, automation must be introduced to integrate the assets into the configuration management database (CMDB) and to remove any exceptions.
- **Implement network zoning**
  There's no need to throw away existing zoning policies or best practices. It is more a case of ensuring existing applications are well described and that you're using AI-driven tools to identify network flows. Again, asset location strategy is key, using IPs and tagging, as well as identification and the use of certificates. Not many companies have a common certificate management strategy and it's common for certificates to expire without anyone noticing, which can cause the temporary loss of a critical system.
- **Build-in encryption**
  Build a long-term encryption strategy, evaluate cloud impacts, and employ regional management systems. Encryption is strongest when it's identity-aware and new (and future) technology like homomorphic encryption is something to consider too.
- **A true Cyber Defense Center (CDC)**
  A final success factor to zero-trust is establishing a defense that proactively models threats and reviews processes. Involving cybersecurity teams with key business initiatives is one way to preempt threats. As opposed to a response team, an effective CDC will track asset exceptions and apply AI solutions in areas like security information and event management (SIEM).

ZERO-TRUST IS A CONTINUOUS PROCESS

Putting in place an effective framework for zero-trust does not mean it's time to sit back and relax. Implied by many of the above strategies, it is in reality a process that requires continuous monitoring to detect behavior and policy infringements.

Policy enforcers are key components of zero-trust, but despite some tools being developed, we're so far missing a set of clear rules to ensure everything communicates together. Non-profits will ultimately build these frameworks, but while we wait for industry-wide standards you can implement other monitoring strategies to keep on top.

By setting up sensors, for example, you can detect instances of unusual activity that monitor the who, what, where, and how. This means deploying user authentication, a device monitoring solution, device location monitoring, and application and data plane tracking.

Such capabilities will be driven by AI-detection software that will enable your monitoring system to manage new content and sets of use cases based on anomaly detection. With an overview of identities risk scoring, you'll ultimately entrench visibility into your network and gain a better understanding of priority areas.

A MULTI-YEAR TRANSFORMATION

If zero-trust sounds like a big shift, then you've heard correctly. It is not an overnight tale but is a multi-year journey with a length determined by its industry vertical. It will depend on the amount of legacy infrastructure involved as well as the wider security requirements of the industry.

This means that a transformation in approach is more urgent in some industries than others. The increasing connectivity of automotive and healthcare, for example, raises the threat level directed towards the manufacturers and so moving beyond network zoning in years ahead is imperative. In other industries, some may already be at or close to zero-trust.

For most businesses however, zero-trust will be a multi-year journey. And it is one worth taking - organizations should not wait for standardized policies to be published. At Capgemini, zero-trust does not necessarily have to start with a major investment, but by applying the basics and building on best practices. The industry will evolve in time, but the threats will not wait. Now is the time to embark on your zero-trust journey.

AUTHOR

Jerome Desbonnet

Global Cybersecurity CTIO, Capgemini

jerome.desbonnet@capgemini.com

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 325,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fuelled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

Get the Future You Want | www.capgemini.com

Copyright © 2022 Capgemini. All rights reserved.

For further information please contact:

cybersecurity.in@capgemini.com