cpl.thalesgroup.com

THALES
Building a future we can all trust

How Can You Trust an Untrusted Environment?

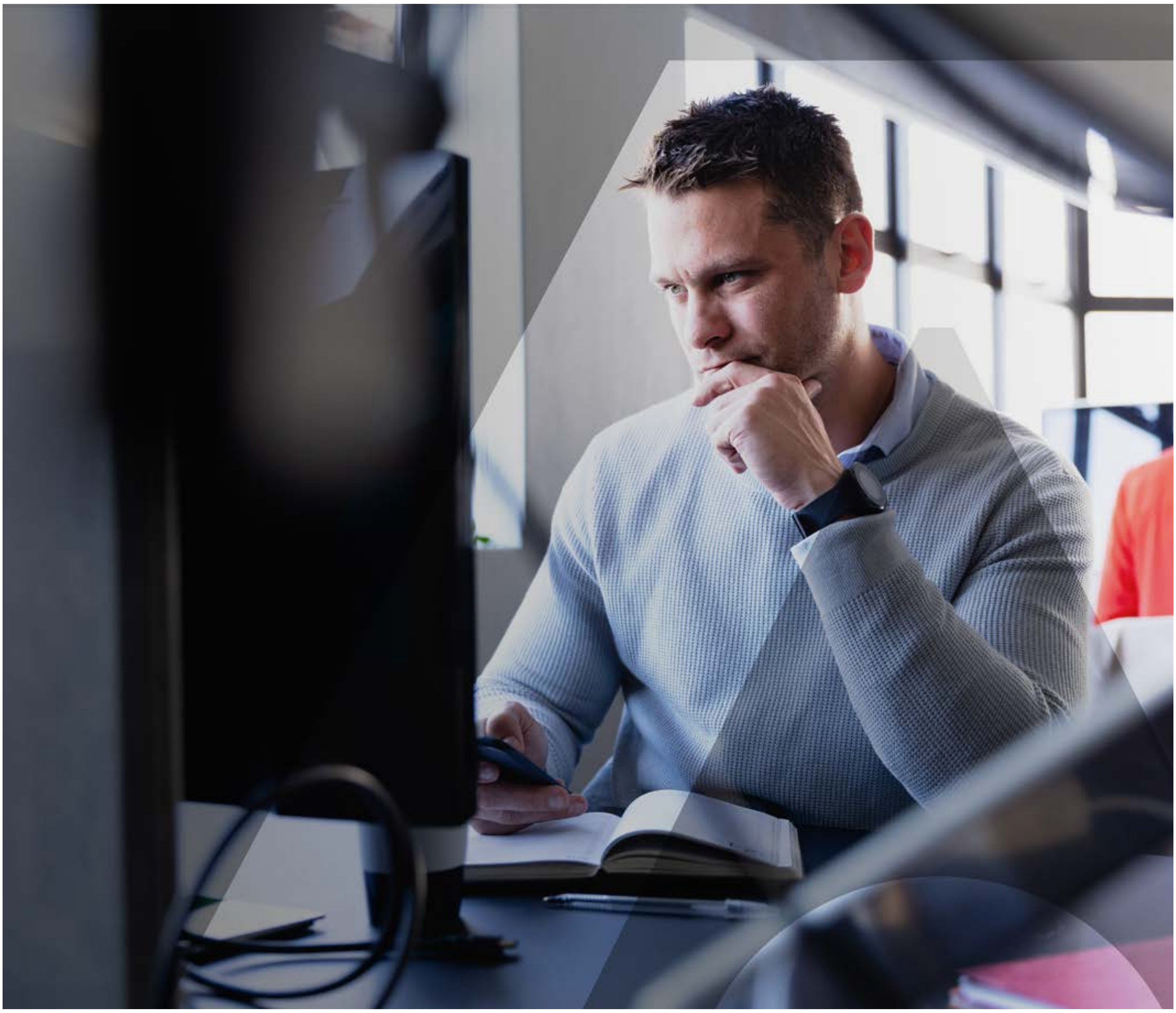
Navigate Safely to a Zero Trust Harbour with Our Experts' Advice

How Can You Trust an Untrusted Environment?

Digital transformation, the proliferation of disruptive technologies and emerging trends such as 'work from home', coupled with the alarming increase in data breaches and security incidents have rendered the concept of trust extinct. Zero Trust security is based on the tenet "Never Trust, Always Verify", views trust as a vulnerability, and requires strict and continuous identity verification to minimize implicit trust zones.

Zero Trust is not a specific technology, rather a strategic initiative and principle that helps organizations prevent data breaches and protect their assets. Accomplishing the Zero Trust principles is not without challenges, as organizations will have to evolve their legacy "castle-and-moat" security policies into location agnostic ones. Seeking advice from experts is a great step towards selecting and developing the correct Zero Trust approach for your organization.

To help you navigate safely towards a Zero Trust harbour, we asked a group of leading information security professionals for their views on the challenges and for some advice for succeeding in building Zero Trust security. Here are their responses.



What are an organization's biggest challenges when it comes to achieving Zero Trust?

Fareedah Shaheed

CEO and Founder, Sekuva

follow profile

One of the biggest challenges is maintaining awareness and vigilance while people are working remotely. When people are at home, there is a different level of awareness than when they're at work. Many are distracted by the change in the environment, and they may not maintain the same security habits they practiced in their corporate workspace. This higher likelihood of mistakes presents a unique challenge to achieving the Zero Trust Model.

Ambler T. Jackson

Senior Privacy Subject Matter Expert

profile

Choosing the appropriate strategy and the best technology to meet the particular needs of the organization requires the right leadership, meticulous planning, time, and resources. It's about much more than just a change in mindset or a cultural shift.

Angus Macrae

Head of Cyber Security

profile

For most organizations, the move to Zero Trust is more likely to be an evolution than a revolution or a single-point- in-time achievement. It requires a fundamental change in mindset. However, from a non-technological perspective, it becomes more vital than ever that an organization and its IT department genuinely understand the assets it's trying to protect.

Jenny Radcliffe

People Hacker & Social Engineer

follow profile

One of the challenges of a Zero Trust program is that people will resist change when you make anything they are used to previously having, suddenly unavailable to them, even if they never actively used it. People resist "losing" anything, both psychologically and technically, so don't underestimate how quickly users will learn to "hack" the new system or find ways to get around the limits of the program. Key to mitigating this is explaining why moving to a Zero Trust model has been adopted, so that the changes don't seem to be imposed for no reason. Success includes having staff on board, and key to that is making them a proactive part of the process.

Michael Ball

Virtual Chief Information Security Officer, TeamCISO

follow profile

The biggest challenges to achieving Zero Trust is visibility of access and understanding the value, criticality, and location of corporate data. A significant challenge is knowing who is on the network at any point in time, the context of their access, and whether their connectivity to corporate assets is appropriate to their role.

Sarah Clarke

Data Protection and Security GRC, Infospectives Ltd.

follow profile

When I became aware of Zero Trust as a term, then as a concept, I struggled to work out the value-add. I've always flagged surrounding context as the essential ingredient when assessing risk, but I've also had the luxury of working in bigger firms with budget to look up from firefighting to do that. The lion's share of risk is inside your perimeter, and out in the unguarded wild. Primarily, you need a useful way to rate relative risk across resources, assets, and locations. Then you can prioritize deeper assessment, monitoring, and control.

Ross Moore

Cyber Security Support Analyst

follow profile

Perhaps the biggest challenge is getting authorization from corporate leadership. Like any other large project, it gets approved based on business numbers and confidence. Prior to full approval, it can be done piecemeal. Take it a step at a time by looking at your Zero Trust roadmap and picking the items that have an easily demonstrated Return on Investment (ROI), and those that have the largest leverage.

Chris Hudson

Security Architect, Tripwire

follow profile

I have seen two key challenges that organizations struggle with when getting started with Zero Trust - getting application tooling to support Zero Trust initiatives and pitching the new controls to the rest of the business. For the first challenge, it's important to consider what aspects of your existing implementation can be used to power Zero Trust processes, and that may require thinking not just about classic security apparatuses (such as antivirus, firewall logs, and similar tools.) The other consideration is how line-of-business applications handle authentication and access controls to effectively validate "trust per transaction" rather than just "security at the threshold".

Some organizations may find it difficult to frame Zero Trust as a practical option, with many companies believing that it's on the wrong side of the "security versus ease of use" scale. Fortunately, this concern can be easily addressed with a CISO who is prepared to talk about the mechanisms behind a Zero Trust approach in an understandable way.

Gabriel Whalen

Manager, Information Security Solutions, CDW

follow profile

I would caution that the principal of Zero Trust needs to be applied beyond technical means. Human resources, training, and building a culture of security adherence is the first line of defense, yet perhaps the most important.

Randy Skopecek

Solutions Architect, PLM Insurance Co.

follow profile

Three things come to mind to achieving Zero Trust: Corporate Support, Risk Awareness, and Ability to Execute. Absent these, you will end up fighting your own employees, let alone customers, which will waste almost all your time.

BJ Gardner

Security Architect, PLM Insurance Co.

follow profile

Zero Trust will create enhanced security for all devices, mainly limiting connectivity to an enterprise application by device. Utilizing an enterprise multi-factor authentication (MFA) solution, married with an enterprise endpoint management platform, creates a multi-faceted approach to authentication into the systems. Another advantage will be the ability to bring mobile devices into the security model, as well as true device management capabilities.

Haroon Malik

Cyber Security Director (EMEA), 6Clicks

follow profile

In theory, "trusting nothing and verifying everything" should provide a simple solution for cybersecurity. In practice, however, Zero Trust brings a host of complications and new challenges, especially as there is now an increasingly distributed and remote workforce using devices ranging from IoT, mobile, and robotics. Some of the main challenges include legacy systems and applications that are generally hard to reconfigure or redesign to fulfil the micro-segmentation requirements of Zero Trust. The key challenge is mapping the flows of sensitive and critical data, identifying who needs to have access to it, and what approach can be used to secure it.

Justin Sherman

Tech Policy and Geopolitics Expert

follow profile

As the language of nationalism pervades our public discourse around technologies and their vulnerabilities, framing business security and supply chain security decisions in the language of trust is more important than ever. In an age of ever-evolving threats to digital technologies, as well as their globally complex and interconnected supply chains, Zero Trust can help business operators and decision-makers alike work to protect security.

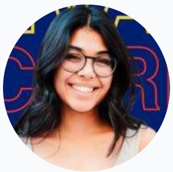
Didier Hugot

VP Technology and Innovation, Thales

profile

Zero Trust security is strongly related to the cloud and digital transformation trend which has been happening in the industry over recent years. This is seen in electronic messages, employee and customer data, and documents, all of which are no longer stored and processed only within the trusted perimeter of the enterprise, but outsourced to a wide range of third-party providers.

This new paradigm creates a large fragmentation in the enterprise's ecosystem, which makes it very difficult to have a global visibility on where sensitive assets reside. It makes it even harder knowing that these data are transiting through different types of personal devices which are not necessarily under the control of the enterprise. Regaining this global visibility is a must in order to enable consistent security policies across the enterprise.



Tazin Khan Norelius

Founder, Cyber Collective

follow profile

Zero Trust has always been relevant, but given our current circumstances, it has now forced organizations to look at security outside of the traditional network perimeter. The biggest challenge is that full workforces are now operating from uncontrolled environments, and most organizations were not prepared for this shift. Unfortunately, there isn't a magic tool that will be able to "fix" the issue because you're operating on unpredictability: human behavior.

Anders Lemke

Platform Architect and Lead Engineer, Zetland

follow profile

The biggest challenges when it comes to achieving Zero Trust are exactly the same as the challenges of all other IT development projects. Always remember that unnecessary complexity kills. Similarly, if the domain experts are not available to collaborate on the effort, you will have a more difficult path to success. Above all, the human element is most important. Respect the people using the system, or the change will create an environment of frustration.

Stephane Nappo

Vice President Global Chief Information Security Officer

follow profile

Driven by de-escalation of often unmanageable security, we ought to rethink the model from one of "cross border filtering security", to the "transversal mastering of security in an open world" with Zero Trust Security. A Zero Trust security model is much more than an IT concept or architecture. The Zero Trust approach is a new paradigm, an attitude, a philosophy. It is the way to rethink a prudent and convenient security of an open digital world, relying on fast evolving business models.

Chrispoher Budd

Consultant, Writer

follow profile

Zero Trust has always been relevant, but we're now reaching the point where its necessity is meeting or exceeding its relevance. The reason for that, is that changes in the composition of networks have unveiled the illusion that "networks" can be trusted. Starting with moves towards BYOD, which introduced uncontrolled devices into perimeter networks, and now culminating in the sudden, widespread adoption of work-at-home because of COVID, we're seeing that network composition can't be trusted, so Zero Trust is necessary. The thing is, we should always have been viewing our networks through a Zero Trust prism because that's the only way to be sure.

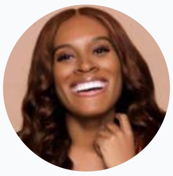
Haider Iqbal

Business Development Director, Thales

profile

The big challenge is not understanding that achieving Zero Trust is an ongoing journey that has multiple steps. Though there are some foundational technology capabilities that are a must, organizations tend to equate Zero Trust to implementing a single capability.

There is no "silver bullet" that will make an organization achieve Zero Trust. This leads the CISO/CIO either into rush decisions, or conversely, into an analysis-paralysis phase, leading to unfavorable outcomes or no outcomes at all!



Jihana Barrett

CEO & Founder, CybrSuite

follow profile

As it stands, too many networks and applications run on an "assumed trust" system. Assumed trust leads to hackers moving laterally within a network with ease once they have access. With the Zero Trust model, all of that assumed trust is no longer an issue.

One of the challenges with implementing the Zero Trust model comes from the employees. The ease of accessing applications and services on the network won't be as simple as it once was. In this new model, employees will also have to contend with the restrictions that come with a "need to know" access policy, training, and implementation.

In addition to the challenges created with employees, there are also challenges associated with integrating newer technology into legacy systems, and poor configurations, potentially creating new access vectors for malicious hackers.

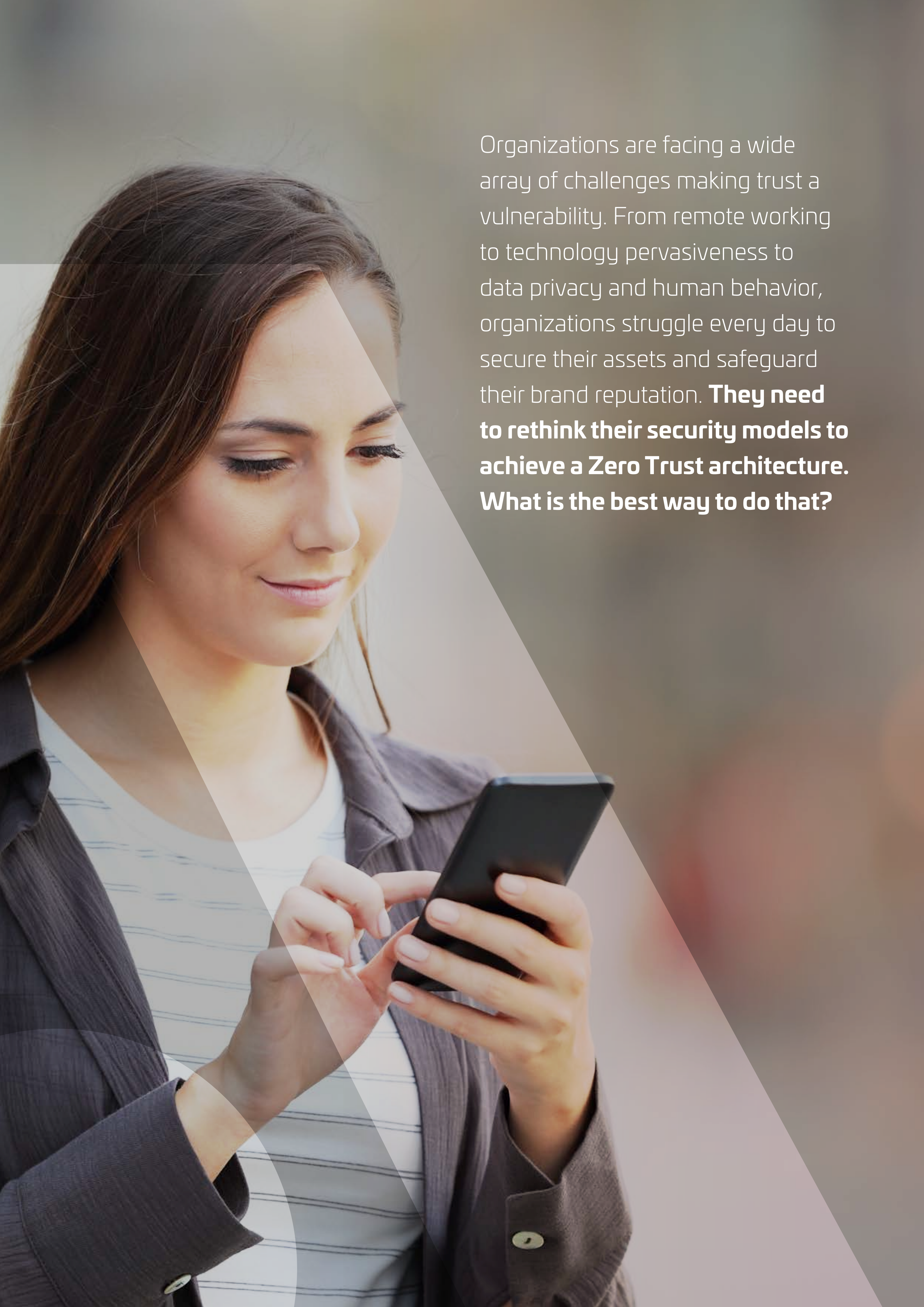
Christine Izuakor

CEO of Cyber Pop-up

follow profile

The obvious concern today in this remote era is that people and data are all over the place, with porous geographical boundaries. It's in your employee's living room. It's in their basement. It's in the coffee shop. It's in the personal iPad that is shared with their child for school assignments. It's all dramatically opening up the risk landscape.

This was already a challenge before, but it's been bolstered by the current remote work uptick. Remote work is a good thing for the future of business and the way that we work, but it requires meticulous management of access to organizational resources in order to control the cybersecurity risk that comes along with it. The question really becomes: with all of this data and movement, and this change in environment, who can you trust? That's where the concept of "never trust, always verify" or "Zero Trust" becomes critical.



Organizations are facing a wide array of challenges making trust a vulnerability. From remote working to technology pervasiveness to data privacy and human behavior, organizations struggle every day to secure their assets and safeguard their brand reputation. **They need to rethink their security models to achieve a Zero Trust architecture. What is the best way to do that?**

When it comes to Zero Trust, what advice would you provide organizations, and the people working within them, to achieve a Zero Trust model?

Angus Macrae

Head of Cyber Security

profile

I would strongly advise anyone who is contemplating a move to Zero Trust models or architecture to read and consider the many valuable points made in the current documents, such as NIST Special Publication 800-207. Subsequently, if you do not have the time to read the full 59-page treatise, I have written a short introductory blog about the publication: "Zero Trust Architecture: What is NIST SP 800-207 all about?"

Jenny Radcliffe

People Hacker & Social Engineer

follow profile

From a social engineering perspective, Zero Trust is a good mindset to have, mostly because it avoids the guard the perimeter "castle and moat" idea of security, taking account of the fact that our threats can already be on the inside or find some way inside. A malicious social engineer might gain access to a system through compromising an insider, so limiting and monitoring what any one individual can do, and continually verifying users helps limit lateral movement once inside, and ultimately slows down a people-based attack.

To be successful, Zero Trust efforts need to be consistent, including an on-going process that is updated to reflect what's necessary in terms of IAM. The system needs to also consider user trends and shifting requirements, rather than looking soley at least privilege access. Attacks can be patient and happen over time, so we need to monitor shifting patterns of use and "scope creep" in terms of what people have been requesting access to, and actually using.

Michael Ball

Virtual Chief Information Security Officer, TeamCISO

follow profile

Next, understand that User Identity is the new perimeter. Manage user access contextually. Not only with multi-factor authentication, but the entire context can be used to protect resources. Questions, such as: Do I know and trust the device they are authenticating from, as well as the network from which they are authenticating? Do I know and trust the geographic region they are authenticating from? Do they require privileged access for this task? Is the login occurring during typical working hours for this user? Any of these can change how I treat connectivity and access to corporate information.

Sarah Clarke

Data Protection and Security GRC, Infospectives Ltd.

follow profile

You need to get everyone in the organisation to help you get the most Zero Trust bang for your buck. The answer is a triage step. Asking key stakeholders the simplest possible questions to flag inherently risky characteristics of connections, data, data processing, software and devices. Questions that can be answered as early as possible in development, change, procurement processes. For example, how much data, how sensitive, how available must it be, user access level, what kind of internet connection, access to and from where? If you do it right, in a simple and engaging way, with standardised responses that enable analysis, answers will breathe life into context-lite diagrams, help to refine trust boundaries, and clarify where policy-driven rules should apply.

Ross Moore

Cyber Security Support Analyst

follow profile

A possible path for starting out would include, researching Zero Trust and making a long-term roadmap, then, deconstructing your Zero Trust roadmap into strategic goals using a project management criterion. Once that is done, implementation of specific technologies can begin. Whenever possible, use technologies that have security built-in and are as easy as possible to deploy. While there's much more to Zero Trust, the advancements made in achieving these goals provides a metric for future projects.

Chris Hudson

Security Architect, Tripwire

follow profile

Zero Trust maturity requires a lot of moving parts to be aligned, so breaking out individual components (such as devices, applications, and networks), and identifying where you will start and how you will provide verifiable improvements will make it easier to get a foothold. A good starting approach to Zero Trust is to first ensure you have visibility across your estate and then build automations based around your real-world usage. No "one size fits all" approach will cover every trust transaction, so identifying where you are first is an important starting point.

Fareedah Shaheed

CEO and Founder, Sekuva

follow profile

Since many are working from home, it's important that the Zero Trust model is instilled in everyone as a mindset and not just as a framework. This means that everyone should integrate the Zero Trust model into their online habits, whether they're logged into work or not. The default mindset should be "let me double-check this" or "better safe than sorry".

Randy Skopecek

Solutions Architect, PLM Insurance Co.

follow profile

The intent is about being explicit and supportive of needs, knowing that bad actors exist, versus being open for effort savings while hoping bad actors don't exist.

Don't rush to lock everything down in a hurry. You will increase the chances of making mistakes (including locking yourself out of those resources, possibly permanently), or creating other undue loss of productivity for the organization. With that, ensure you have a good backup and recovery process.

Work off a prioritized risk profile list. There is plenty to be done and it doesn't all have to be tackled at the exact same time. Finally, ensure you are addressing the productivity tooling and education, such as password managers, and security awareness training that improves the end-user game while also achieving the security objectives.

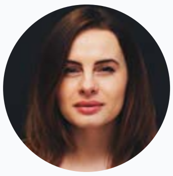
Chloé Messdaghi

Chief Strategist, Point3 Security

follow profile

Some guidelines to consider include: A universally shared commitment not to inherently trust anyone inside or outside. Doing this without business disruption requires visibility, analytics and automation. Analytics are crucial because every organization needs to work on the assumption that, sooner or later, a determined attacker will succeed. Without the foundational knowledge that analytics provide, timely mitigation is far harder. It's all about who has access to what, and making sure you have a secure administrative environment.

Adopting a Least Privilege Access model for data pools and resources, and constantly auditing who has access to what, are perhaps the most painstaking processes, yet absolutely crucial. Finally, embrace third party risk management. Zero Trust fails when your organization partners with other companies whose practices are laxer than yours.



Andra Zaharia

Content Marketer for Cybersecurity Companies

follow profile

After years — decades even — of building their security setup, and millions invested in hardware, software, processes, and training, the pandemic reset the "normal" mode of operations. Security baselines are gone, business hours lack consistency, and usage habits look nothing like they used to. As a consequence, security professionals have to remap their understanding of how the business works. That's where Zero Trust comes in as the only model that can reliably accommodate these changes, while still providing the level of predictability companies need to operate safely. Infosec professionals have to do a lot of additional work to implement controls that can effectively work in a world where the perimeter is obsolete.

Panagiotis Sotiriou

Cyber Security Technology Director

follow profile

Zero Trust increases visibility on an organizations' assets, while improving security, and empowering digital business transformation.

A well-designed and enforced Zero Trust model can effectively reduce expenditures on security while also assisting in solving the security skills shortage, as it reduces the scope and relative cost of compliance.

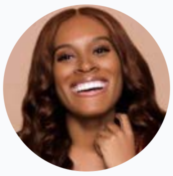
When it comes to deciding a Zero Trust model, organizations need to first return to their basic security principles, including verified trust of anyone and anything, secure and authenticated access to all resources, a least privilege model, enforced access control, log inspection, and defense in-depth.

Didier Hugot

VP Technology and Innovation, Thales

profile

Migration to a full zero-trust security model should be progressive over time. As a good practice, it is recommended, to start by migrating the less critical assets to minimize risks, while taking time to learn and apply the right security configurations. There is no easy way to achieve a Zero Trust model. Each enterprise has to adapt their strategy depending on their business needs and constraints. Some may decide to move everything in the Zero Trust security zone, some may decide to keep all sensitive data on-premises, and some others may choose a hybrid approach.



Jihana Barrett

CEO & Founder, CybrSuite

follow profile

The first piece of advice I would offer is to change how we view security. Just as a person would have a natural suspicion of a stranger he or she encounters in public, the same thing needs to happen with technology. Access needs to be on a need-to-know basis. Micro-segmentation needs to be the default network setup, and multi-factor authentication needs to become as common as a strong passphrase.

Organizations need to take their time when implementing the Zero Trust model. There is a lot that can go wrong with a hasty implementation. I would recommend a multi-phased approach, where network needs are organized based on priority and importance.

Leron Zinatullin

Chief Information Security Officer

follow profile

Device management is the foundation of an effective Zero Trust implementation. Asset inventory in this model is no longer just a compliance requirement, but a prerequisite for managing access to corporate applications. Security professionals should work closely with procurement and IT teams to keep this inventory up-to-date. Collaborating with the Human Resources department to establish processes for maintaining the connection between device management and employee identities, roles, and associated permissions is the key to success.

Haider Iqbal

Business Development Director, Thales

profile

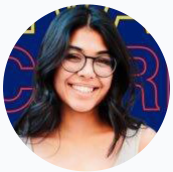
Organizations need to map out their journey as achievable milestones, and then evaluate which capabilities can help achieve those milestones while also remaining mindful of not overthinking the journey. Some common themes in analyst reports about Zero Trust include the advice to use multi-factor authentication and adaptive authentication. Identify such capabilities and start implementing them from the onset of your journey. These quick wins will boost the confidence of all stakeholders involved in this multi-step journey. As always, never trust, always verify!

Christine Izuakor

CEO of Cyber Pop-up

follow profile

The biggest advice that I would give is to treat it as a journey. Treat it as a mindset. Treat it as a culture. There is no single total solution that you can buy, flip a switch, and have effective Zero Trust. There are layers of processes and technology that you need to implement to get to a state where you're aligning with a Zero Trust model. That's important to keep in mind.



Tazin Khan Norelius

Founder, Cyber Collective

follow profile

My advice would be to base threat-modeling from the perspective of human behavior, and not the traditional needs of an organization. What threats may a household face that has employees with access to critical information, but also has children using the computer when their parent leaves the room? To face diverse scenarios, you need a diverse perspective, so engaging with folks outside of the security team can exponentially aid the way your threat-modeling develops.

Stephane Nappo

Vice President Global Chief Information Security Officer

follow profile

The best piece of advice is "Know Thyself". To apply Zero Trust Security and the least privilege principle, you must have robust visibility into your critical assets, and your weak points. Adopt a comprehensive cyber risk management attitude, and evolve your security maturity to a prevention-based strategy with Zero Trust architecture and a collective cybersecurity culture. Zero Trust security is not barricading, but the new DNA of modern, seamless, and efficient security.

Conclusion

In the traditional "castle & moat" security concept, bad actors were considered trusted once inside corporate networks and were free to move laterally undetected. Trust is a blind spot and could no longer be accounted for. Zero Trust security concepts allow organizations to grow securely in the cloud and adjust to borderless and dispersed environments.

The experts' advice indicates that there is no set formula for reaching Zero Trust in any organization. It is clear, though, that organizations must set well defined priorities and measurable goals and objectives to succeed. From strong engagement with staff about the purposes and benefits of Zero Trust, to full leadership support, Zero Trust is achieved only with collaboration.

The modern enterprise security perimeter is no longer a physical location; it is a set of access points dispersed in and delivered from the cloud. Identities are now the new perimeter and should be at the core of access decisions.

The greatest challenge is to employ a comprehensive Zero Trust security solution that covers identities and data end-to-end. With its cloud-based access management and authentication solutions, Thales addresses crucial Zero Trust security needs of enterprises holistically.

SafeNet Trusted Access is the starting point for effective Zero Trust security implementations, meeting the Zero Trust principles by ensuring a 'trust no one, verify everywhere' stance through its ability to continuously protect applications and services at the access point, regardless of the underlying network deployed.

To learn how Thales can help you, read our whitepaper "Meeting NIST Guidelines for Zero Trust Security" here.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <