ComputerWeekly.com | TechTarget

E-guide

CW+ Content

Zero trust: Taking back control of IT security

In this e-guide

In this e-guide:

Dating back over a decade to the early 2010s, the concept of zero-trust security – which was first defined by Forrester analysts – is steadily becoming more and more relevant to the enterprise, particularly as the Covid-19 pandemic renders the traditional network perimeter (at least temporarily) somewhat obsolete.

In this E-Guide we go in-depth to explore the concept of zero-trust. First, Cliff Saran explores some of the basics of zero-trust, exploring how the advent of mobile computing, remote working, and software-as-a-service (SaaS) had already started the shift in security focus away from the perimeter – even before the Covid-19 pandemic, with help from some of Computer Weekly's regular Security Think Tank contributors.

Then, we turn to Nemertes Research's Johna Till Johnson, a regular contributor to SearchSecurity.com, who shares six steps to implementing effective zero-trust strategies, while Nicholas Fearn looks specifically at the question of whether

In this e-guide

zero-trust is an effective means of addressing security concerns around containers.

Finally, we share some more home truths from the Security Think Tank. Airbus Cybersecurity's Paddy Francis explains why zero-trust should be considered as part of a wider digital transformation strategy; Simon Persin of Turnkey Consulting explains why considerations around zero-trust must account for whether it is truly a requirement, or merely an aspiration, for your organisation; and as a counterpoint, Mike Gillespie, managing director and co-founder of independent security consultancy Advent IM and vice president of the C3i Centre for Strategic Cyberspace and Security Science (CSCSS), reveals why he believes zero-trust is not necessarily the answer to all your security problems.

In this e-guide

Zero trust: Taking back control of IT security

Cliff Saran, Managing Editor

In recent years, the elimination – or at least reduction – of trust on the network has been critical for businesses to defend against the multiplying security threats that have emerged in modern computing.

As Fieldfisher LLP partner James Walsh and technology lawyer Rob Grannells note, mobile computing, remote working and the prevalence of software as a service (SaaS) has meant traditional perimeter-based security is easily penetrated. The pair believe trust should be considered a security risk, and additional authentication strategies need to be implemented to ensure each source of data or device has an appropriate level of security.

Zero trust was a term coined by analyst firm Forrester in 2010 to describe the need to cope with ever more complex IT security requirements that put increasing strain on perimeter-based security measures. Forrester is now seeing growing interest in zero trust. Its recent report, *How to implement zero trust security in Europe*, by analysts Paul McKay, Chase Cunningham and Enza Lannopollo, reported that 54% of European enterprise infrastructure decision-makers are actively using public cloud – an increase of 19% since 2016.

In this e-guide

Who do you trust?

For Walsh and Grannells, zero-trust default security means that nothing is trusted outside or inside an organisation's network, so controls must be put in place to reduce risk to an acceptable level. In other words, defence in depth.

They say: "Zero trust changes the traditional model of 'trust, but verify' – where you assume that any device or asset attached to your internal network is likely to be permitted and safe to access internal-only resources, but still verify that this is the case. Instead, that becomes 'never trust, always verify' – where every device must pass authentication and security policy checks to access any corporate resources, and to control access only to the extent required."

Trust involves an interplay between people and technology. According to Walsh and Grannells, the starting point for these trust factors is a well-thought-out and up-to-date set of policies, standards, procedures and work practices, supplemented by detailed, up-to-date network documentation and asset inventories covering information, software licences and hardware.

The pair believe zero trust enables IT security to regain control. "The shift to zero trust is where information security is taking back control of the many new perimeters of the corporate ecosystem," they say. "It shifts security from the address and location layer to a data-centric model. Zero-trust network segmentation also provides visibility into traffic, and allows you to understand

In this e-guide

the 'who, what, when, where, why and how', which are important for managing access, security, monitoring and compliance."

According to Forrester report authors McKay, Cunningham and Lannopollo, non-security executives think zero trust is just a network security architecture. Forrester's research found that network security decision-makers have driven zero trust adoption in Europe so far, with little discussion above chief information security officer (CISO) level. The analysts note: "This could be a result of the high proportion – 42% – of senior-most enterprise security decision-makers reporting into the CIO in Europe." But they warn that if CISOs do not elevate zero trust, their implementation efforts will not achieve their business and security goals.

Looking at the technical implementation of a zero-trust security stance, in January this year, the Zero trust progress report for Pulse Secure found that most investments in zero-trust access technologies are directed towards multifactor authentication (59%), identity management and governance (48%), and single sign-on (44%). This is followed by network access control and web application firewall (43%), privileged access management and micro-segmentation (41%), and virtual private networks (VPNs) (35%).

BCS volunteer Petra Wenham urges CISOs to start with traffic incoming to a network from an external source (such as the internet or a partner network). She says this typically would initially be controlled at the perimeter by a combination of firewalls architected with demilitarised zones (DMZ) supporting

In this e-guide

proxies, reverse proxies and terminating equipment that offer email, VPN and client access termination from external networks and web browsing of the internet from the internal network.

These proxy and terminating devices would typically run anti-virus, malware and spam prevention technologies and, where needed, provide access authentication and authorisation (AAA) services (proxied from an internal AAA system). Application-level firewalling (such as HTML or SQL) might also feature in the services offered on the DMZ.

According to Wenham, a new generation of security devices are now coming to market that integrate some or all of these features and so can, in turn, offer network managers a unified view of their operation. “The design of the internal network can then add further controls, such as network segregation and additional anti-virus and malware detection technologies, together with AAA controls over system and file access,” she says.

For instance, in network segregation, Wenham says the recommended practice is that key servers and services (such as network-attached storage and storage area networks), company and guest Wi-Fis, are given their own networks and larger organisations can give thought to putting some departments (such as human resources, finance and R&D) on their own networks.

“All these networks would then be connected together via firewall technology, which could be discreet firewalls, or utilise the firewall capabilities found in

enterprise-level Ethernet switches, or be connected to an enterprise-level, multi-ported firewall, or a mix of all three approaches," she says.

Elements of a zero-trust architecture

Zero trust typically combines these control elements to manage the device, user and trust level for anyone wanting access to corporate resources:

• Unified endpoint management: The ability to enforce and monitor the compliance of all endpoint devices, whether corporate owned, BYOD (bring your own device) or contractor provided. This means you know your device estate and specific security threats, such as a device operating system going out of date.

• Single sign-on: One sign-on point, passing fully validated credentials from system to system. A single version of the user ID truth and a single point of entry that validates a user's credentials, and logs access in and out of corporate systems, is important for an easy user experience in a zero-trust environment.

• Multifactor authentication: A trusted device, a hardware security key, a biometric measure, behavioural analysis, location data, time-based restrictions, and so on, can all be combined to make a "profile" of multiple factors to establish a user's credentials. When every user must be validated, relying on a single factor is no longer an option.

In this e-guide

Source: James Walsh and Rob Grannells, Fieldfisher LLP

Forrester has found that one of the concerns about the adoption of zero trust is the cost of implementing the model. The analyst firm has developed a core zero-trust model that it says emphasises gradual evolution towards the zero-trust principles by starting with identity and other foundational security controls and reducing the attack surface using your existing control footprint.

Forrester analysts McKay, Cunningham and Lannopollo urge CISOs to follow a gradual approach to deploying zero trust across their organisations by starting with their existing security systems. “As you master those areas, you can then invest in new areas, like enhancing the range of security monitoring use cases to gain greater visibility and automate manual security tasks and increase your zero-trust maturity,” they say. “If you can demonstrate that zero trust is not yet another excuse to buy lots of shiny new security widgets, you’ll gain further trust in the boardroom.”

In fact, the Zero trust progress report found that a quarter of organisations are augmenting their current secure access infrastructure with software-defined perimeter technology, which effectively provides zero-trust network access.

In this e-guide

Planning a zero-trust strategy in 6 steps

Johna Johnson, President and Senior Founding Partner

Zero trust isn't a turnkey proposition. Enterprises must create a zero-trust strategy that addresses how the organization will approach the move and who will lead the effort, among other important factors.

Before planning starts, however, make sure the cybersecurity team is on the same page about the attributes of zero trust.

- **Zero trust is highly granular.** Only the minimum possible access is granted to the smallest resource unit.
- **Zero trust is dynamic.** Trust is constantly reassessed through the interaction between user and resource.
- **Zero trust is end to end.** Security extends from the requesting entity to the resource requested.
- **Zero trust is independent of preexisting classifications.** The terms *inside the perimeter* and *outside the perimeter* have no meaning in the world of zero trust.

Once everyone is set on the foundation of zero trust, cybersecurity teams can create a strategy based on six steps.

Step 1. Form a dedicated zero-trust team

Zero trust is one of the most important initiatives an enterprise can undertake. So, rather than making "move to zero trust" a task that ranks below everyone's top to-dos, dedicate a small team tasked with planning and implementing the zero-trust migration.

This team should include members from applications and data security, network and infrastructure security, and user and device identity because those areas are the three easiest on-ramps to zero trust. The team should also include members from security operations -- particularly the security operations center -- and risk management.

Once everyone is set on the foundation of zero trust, cybersecurity teams can create a strategy based on six steps.

CEO, Nemertes

Johna Till Johnson

Step 2. Assess the environment

Understanding the controls across the environment will make deploying a zero-trust strategy more straightforward. Here are some questions to ask.

Where are the security controls?

In a network environment, these controls include firewalls, web application gateways and the like. In a user/identity environment, the controls might be endpoint security -- endpoint detection and response or extended detection and response -- and identity and access management (IAM). In an applications and data environment, these include container security, data loss prevention, microservices authorization and similar controls.

To what extent do these controls provide dynamic, granular, end-to-end trust frameworks that don't depend on preexisting classifications?

Firewalls typically aren't granular, end-to-end or dynamic and rely on simplistic classifications -- outside = bad and inside = good.

What are the knowledge gaps?

It's impossible to provide granular access to data if you don't understand the security classification of that data. Unclassified data represents a knowledge gap that will need to be addressed in a zero-trust strategy.

Step 3. Review the available technology

Either at the same time or following the assessment, review emerging technologies for your zero-trust initiative's on-ramp. Next-generation networking

equipment includes capabilities like deep segmentation -- or microsegmentation -- virtual routing and stateful session management that can turn these devices into key components of a zero-trust architecture. IAM capabilities are quickly becoming more granular and dynamic.

Step 4. Launch key zero-trust initiatives

Compare the results of your technology review with the technologies you need. The comparison will inform how to develop, prioritize and launch initiatives such as "upgrade existing network infrastructure to equipment capable of deep network segmentation" or "deploy microservices authentication."

Step 5. Define operational changes

Zero-trust strategy can fundamentally change security operations. For example, as tasks are automated, corresponding manual tasks might need to be modified or automated to keep pace and prevent gaps in security.

Step 6. Implement, rinse and repeat

As the organization deploys new technologies, assess their value according to security KPIs, including the mean total time to contain incidents, which should decrease dramatically the closer an organization moves to zero trust.

How to apply zero-trust models to container security

Nicholas Fearn,

Organisations are increasingly replacing archaic software development approaches with containers, which allow them to develop, deploy and scale applications much more quickly than traditional methods.

But despite these benefits, containers are not perfect. Their adoption has also resulted in new challenges for security teams, particularly around data protection, container image vulnerabilities, cyber attacks, unauthorised access and a whole host of other risks. Could zero-trust models mitigate these? And if so, how can organisations apply them to container security?

Although containers provide greater efficiency and scalability for development teams, they can have significant implications for security. Often, traditional

In this e-guide

perimeter-centric security models are not suitable and new approaches are needed.

Kevin Curran, IEEE member and professor of cyber security at Ulster University, says: “The dynamism of containers can cause problems for traditional security environments, due to the complexity involved in networks, overlays and dynamic IPs, mixed with the limitations of traditional firewalls which struggle to identify nefarious activity.”

But that is where zero-trust security models can help. Curran explains that when combined with policies based on identities of workloads, they allow enterprises to build a picture of what is communicating over their network. “Here, zero-trust based on identity can prevent compromised workloads from communicating as each identity will not be recognised,” he tells Computer Weekly.

“The need for a zero-trust security model has arisen in part because enterprises no longer tend to host data in-house, but rather through a variety of platforms and services that reside both on- and off-premise, with a host of employees and partners accessing applications via a range of devices in diverse geographical locations. This means the traditional security model is no longer fit for purpose.”

Curran says zero-trust security can be implemented by updating network security policies, validating each device logging into the network, securing networks with a variety of network, perimeter and microsegmentation,

implementing multifactor authentication and conducting periodic reviews of user access.

He adds: “The main applications for zero-trust security require new approaches, such as using network/microsegmentation based on users and locations. It also requires enforcement of identity and access management [IAM], next-gen firewalls, orchestration, multifactor authentication and file system permissions.

“Ideally, this is something that is done slowly in steps, as it entails pilot projects and tweaks in a lab environment before deploying. It is crucial to ensure that the zero-trust infrastructure is seamless for employees.”

Catalyst for zero-trust

Many experts believe the need for zero-trust security models is growing along with the increased adoption of containers across the enterprise landscape. Neil Thacker, CISO of software firm Netskope, agrees with Curran that such models are paramount for security teams deploying containers.

Thacker says: “Cloud-based applications and container-based applications – not to mention cloud-based, container-based applications – are a further catalyst for interest in zero-trust network access [ZTNA], specifically because of the disregard both cloud apps and containers have for traditional perimeter approaches to security.”

He says security teams need consistent security controls across all applications as a fundamental rule, regardless of whether they are based on a traditional stack, are virtualised or hosted in containers.

“While security must not stand in the way of the inherent benefits of containers, such as portability, the controls and methods of securing access to containers is key,” says Thacker. “Firewalls aren’t useful because they are not app-aware, and even next-gen firewalls that apply controls to the application layer still require illogical network arrangement and overly permissive security policies to account for the rapid changes of network IP addresses within containers.

“This is why cloud-based ZTNA appeals to organisations, because instead of restricting connectivity and restricting the potential benefits that containers offer, ZTNA can prioritise the application, however and wherever it is hosted.”

Making containers impenetrable

Containers may be a powerful tool for developers, but they are becoming a security nightmare as cyber criminals increasingly target them. By gaining unauthorised access to containers, hackers can cause all sorts of mischief, potentially across a large virtual environment.

David Warburton, senior threat evangelist at application threat specialist F5 Labs, says: “If an attacker can leverage vulnerable code within a container, they

may be able to impersonate that service and access data never intended to be made available. Decades-old vulnerabilities, such as injection attacks, apply just as much to modern code running inside a container as they do traditional, monolithic apps.

“The difference now is that containers, and the microservices they provide, have exponentially increased the surface area available for attack, putting data at greater risk. In addition, network-related problems, such as access control, load balancing and monitoring, that had to be solved just once for a monolith application, must now be handled separately for each service within a cluster.”

By applying zero-trust models, security teams can mitigate these threats. Warburton adds: “A key tenet of zero-trust is that every single request should be secured, regardless of who or where it came from. This model needs to be applied to containers so that all communications are encrypted, even those between internal services.”

To prevent unamortised access, organisations must enforce strong authentication mechanisms for their containers. “Mutual digital certificates should be used to ensure only trusted containers can communicate with one another. Finally, strong, role-based access control is needed to ensure only authorised users and services are performing actions that they have explicitly been given permission for,” says Warburton.

In this e-guide

“Create a service mesh security to be handled in a more efficient way by combining security and operations capabilities into a transparent infrastructure layer that sits between the containerised application and the network. Emerging today to address security in this environment is the convergence of the zero-trust approach to network security and service mesh technology.”

Sandy Carielli, principal analyst at market research company Forrester, warns of a disconnect between developers adopting containers and security teams left to pick up the pieces. She says: “Development teams are eager to adopt containers due to their scalability and cost-efficiency, but one of the realities is that dev makes the containerisation decision, and then security finds itself going along for the ride and figuring out the security implications and requirements.” Overstuffed images, in particular, are a major challenge in container security, says Carielli. “Developers typically pull images from repositories, and those images contain more tools, features and permissions than the developer needs for their particular use case,” she explains.

“However, dev teams rarely have time to scale down the image to just the essentials. DevSecOps teams need to set time aside to look at the images they are using and remove the functions and permissions that they don’t need. As a basic example, don’t run containers with root permissions.”

Carielli says microsegmentation is another aspect of zero-trust that applies to containers. “Organisations leverage application microsegmentation tools to evaluate both north-south and east-west traffic and manage the flow of data

among application components – these could be containers, APIs or serverless functions," she says.

"Runtime container security tools map the flow of data between containers, allow you to set policy on how containers interact, and can spin down containers that unexpectedly change configuration."

Creating an effective security strategy for containers

When deploying containers, organisations are effectively exposing themselves to myriad security problems that must be mitigated if they want to get the most out of these technologies.

Benoit Heynderickx, principal analyst at the Information Security Forum, says: "The lightweight nature of containers removes the need for traditional IT infrastructure security controls such as a constant patching cycle and the extreme reliance on the firewall for protecting a network-based perimeter.

"But it brings new types of risks due to the rapid lifetime of containers, while adding increased networking complexities and placing emphasis on the need to apply secure design principles early on, such as secure coding practices."

In this e-guide

With a zero-trust model, organisations can ultimately create an effective security strategy for containers, says Heynderickx. “By focusing on authenticated identities, least privilege principle, defined microsegmentation, traffic monitoring and logging, the model relies on the principle of ‘never trust, always verify’.

“This is a paradigm shift from traditional security models and can only be addressed by deploying it in a phased and defined manner, focusing on specific groups of applications, such as the most sensitive ones for a start.”

Heynderickx says organisations applying zero-trust models to container security should be supported by strong coding practices for all application development activity. This, he says, will put the organisation in a strong position to respond to the growing demand from developers to use rapid deployment platforms such as application containers.

Heynderickx adds: “Modern businesses can therefore benefit from using agile development technologies to deploy secure applications in a fast manner for their demanding customers.”

Understandably, organisations want to roll out new software quickly and efficiently to stay ahead of the curve and achieve competitive advantage. So containers are the perfect answer. However, their adoption has resulted in clear security challenges, and it is crucial that firms take steps to address these if containers are to return value on investment. Therefore, developers must work with security teams when they look to adopt and use containers.

In this e-guide

Security Think Tank: Zero trust strategies must start small, then grow

Paddy Francis,

It is widely recognised that the traditional boundary protection approach to security is broken, particularly in the era of cloud services and remote working, where it is no longer possible to identify your perimeter, or trust those who purport to be users on your network. This is where the zero trust concept can provide a solution, with the right planning and implementation.

Zero trust can mean different things to different people. At a high level, it is about trusting nothing and no one, on the assumption that all users, devices and transactions are compromised. In terms of technology, many familiar elements underpin the concept, namely identity and access management (IAM), mobile device management, multifactor authentication, and so on.

However, at the core of zero trust is fine-grained micro-segmentation and adaptive policy enforcement that allows security controls to be applied to individual workloads across the datacentre. This can then be complemented with user entity behaviour analytics (UEBA) to monitor who is accessing what, and encrypted (TLS) connections between every user, application and data store to prevent a user breaking out and lateral movement.

All this is done at the application layer, so there is no user access to the lower layers, which significantly reduces the attack surface. Essentially, all users whether they are remote, inside the network or accessing cloud data, are treated the same and must be authenticated before they get access to any data or services.

The best approach will depend on the nature of the specific system, including where data is stored and what services are provided. And all this while considering the use of cloud, hybrid-cloud and remote access.

However, it is usually best to implement zero trust incrementally, first addressing the most valuable data assets and most vulnerable users. This will give early benefits by addressing the highest risks first. This should also include the application of zero trust to all security components.

As with any other change, there are prerequisites, and planning ahead is essential. Before starting any implementation, you need to know your data assets, your physical assets (servers, hosts mobiles, and so on) and your users. You will also need to understand the data flows between clients and servers and also between servers (north-south and east-west, in SDN speak).

This is necessary to understand who is accessing what, so that the access control permissions can be defined and the data assets and applications segmented appropriately. This can be done by moving the data into its own network segment and capturing the system transaction using that data.

This will identify how to segment the data and architecting by placing network segmentation gateways with the appropriate policies in front of the data. Defining and configuring the access control is probably the most complex part of a zero-trust implementation, which is another reason to start small and build out.

Because zero trust changes the way users access services and data, a move to zero trust is best treated as part of an overall digital transformation project to adopt cloud technologies, rather than just an update to a legacy system, as this could risk creating new vulnerabilities and failing to remove some of the problems it is intended to fix.
Many companies offer zero-trust technology and they may be able to help with the architecture and planning, but only the business owner of the system can identify critical assets and applications. The same applies to the data flows between them and defining the access control needs.

Also, the operational team overseeing the implementation should have a degree of expertise in zero trust and, ideally, the technologies being used. This may require additional training or bringing in more expertise. Because of the transformational nature of adopting zero trust, the CIO, CISO and other board members should be involved early in the planning to help with the prioritisation of assets and services that are migrated to zero trust and help minimise any business impact.

In summary, a zero-trust approach can help protect today's systems in a way that perimeter security cannot. However, preparation is essential, particularly in

identifying assets and the access control requirements and ensuring the necessary skills are available. It is probably best to start small with the most sensitive assets and services and build out, if appropriate, with less granularity than for the most sensitive assets, which will simplify access control management.

Security Think Tank: Ask yourself if zero trust is right for you

Simon Persin, Director

Digital transformation means today's organisation is no longer limited to undertaking its operations within the confines of its own network. But this paradigm shift, which includes adopting cloud-hosted systems and services and outsourcing core business processes to expert technology partners, blurs the lines of control and responsibility for the devices, systems and applications that reside on this extended network. The result is an exponential increase in security challenges.

This is exacerbated by shadow IT, as individuals and departments purchase technology that, although it enables their roles, is outside the remit of the IT department and therefore not subjected to the organisation's standard security processes.

These changes are eroding the usefulness of the traditional perimeter-based tactics of network security. Instead, the focus is on securing what actions can be performed within the network, with the zero-based trust approach to internal permissions assuming that even authenticated users could act maliciously.

But while zero trust may be a straightforward concept, because its premise is to mistrust everything, it can be complex and resource-hungry to implement and manage. It may also introduce a level of security that is over and above the real needs of the business, thereby compromising operational efficiency with security that is both heavy-handed and superfluous. The initial consideration should therefore be whether zero-trust architecture is a requirement or an aspiration for the enterprise in question.

Whether inbound and outbound traffic can be controlled is a key factor. For example, a strategic decision to allow customers to see stock availability via web shops requires inventory details to be publicly available, and therefore visible to non-trusted people. Similarly, governments in some countries can legitimately request access to corporate data, while in other regions, technical encryption levels are not adequate. The decision whether to pursue a zero-trust policy will come down to the organisation’s risk appetite as well as what is technically possible.

Risk-based approach

If zero trust remains a strong objective, it is important to acknowledge that implementing it as a single step-change is impractical, and potentially impossible. The volume of exceptions and business disruption likely to result from them, not to mention the direct costs of the implementation, make it unrealistic, at best.

Therefore, it is important to use a risk-based approach to identify which applications, servers, devices, users and data need to be protected. Those that are more critical to the organisation should be prioritised from a control perspective so that defences are enhanced and zero trust introduced. Operational processes can then bed in, while exceptions are contained to critical assets only.

At the same time, this acts as a prototype for the rest of the network and a “core” around which devices are built. Critical applications with the most high-risk and complex threats will be enhanced first, thereby providing the best investment value. The key is to understand what needs to be done and how aggressive it should be.

Prioritisation also determines the roll-out approach, with security operations and monitoring on key areas of the network increased gradually and additional

security (access-driven malware scanning, for example) on business-critical applications introduced based on criticality.

Technical specifications

The technology systems selected and deployed need sufficient power to monitor and detect everything – known and unknown – that might be mistrusted. In general, although one-stop solutions can seem appealing, they are likely to be more costly and difficult to implement and operate in the long term.

Applications and devices that have zero-trust capabilities built in prevent additional work, but legacy systems, which may require extra components in order to comply with the model, also need to be accounted for. Solutions need to be scalable to match business growth, as well as future-proofed, so they can evolve at the same (rapid) pace as the threat landscape.

Trusting nothing results in an extensive amount of exceptions to the defined goal. Monitoring resources therefore need the manpower and bandwidth to respond to all incidents that are raised to avoid business disruption or an immediate erosion of the trust objective.

Zero trust in practice

Strong identity management and device management are essential. Users and devices that are not recognised by the system in which they are required to operate should be rejected from accessing anything.

Mapping data flows shows how things are accessed and updated, and where data comes from and goes to. Applications that don't need to be online or to access file servers can be blocked.

Despite the best intentions to include all business processing activities, elements can be missed. Previously unknown "key" business process steps are often identified at this point, flagged by the disruption caused through suddenly disabling an application whose function is still required.

Shadow IT environments amplify the likelihood of this happening because IT security teams are more likely to unilaterally block a business solution without warning if they don't know about it. Repairing the service requires IT to react rapidly to update the false positives flagged by zero trust, while business representatives must learn quickly about using the technology in a way that is secure – and, in the longer term, the need to engage with IT security and operational teams earlier and more effectively.

In this e-guide

Data flows between different parts of the network, applications and the internet can be managed in one place with data integration tools. Assuming that the non-technical information, such as business justification and agreed contractual terms, also flows effectively through the technical channels, this enables appropriate protection protocols to be deployed.
Regular device discovery checks ensure that no rogue devices have been connected, but they need to be reinforced with plans to deal with any unexpected devices, should they appear. Correctly set-up identity and device management should prevent unauthorised communication with anything, but rogue devices can lead to other controls being bypassed, or can indicate that the business has made a change without updating the IT security team.

An organisation’s network needs to change as the organisation evolves. A zero-trust model must adapt to the introduction of new applications or new access methods without compromising the zero-trust status of the rest of the IT estate.

Drives for business effectiveness and efficiency increasingly demand porous network perimeters. Zero-trust architectures offer a modern-day solution – but they are not a panacea. Like all IT investments, they require robust assessment to ensure they are the right “fit” for the organisation and the security problem in question.

In this e-guide

Security Think Tank: Zero trust is not the answer to all your problems

Mike Gillespie,

I can barely open my inbox these days without the words zero trust appearing. Opinions of it as an information risk methodology vary, and for good reason. You are effectively classifying your employees in a way that they may not find edifying or complimentary. Many people say this is the price you pay for robust security and, clearly, there are a heck of a lot of products relying on you believing that too.

I feel what you gain in security, you may lose in demotivated people and increased staff churn and low morale. If you want a good example, look at your average call centre.

There are certain applications for zero trust that have been in place for years already, I am thinking about parts of the nuclear and finance industries, for instance. The convoluted user needs here make zero trust a very attractive proposition and effectively make the security team's life a lot easier.

However, the trend toward zero trust in a range of business areas as a kind of blanket solution seems more like giving up entirely on risk management and taking the path of least resistance – user be damned.

As you can imagine, this is not something I would ever propose and there are several reasons for this, some of them relating to security, and some to leadership:

- It feels too much like an extension of the "stupid users" trope we have been trying to shake off for years – they can't be trusted, eye-rolling ensues, and so on.
- It feels like an extension of "security says no" – see above.
- Staff retention is cheaper than recruitment. When you have good staff, you want them engaged, enabled and growing. Most importantly, you need them to stay. Inappropriate use of zero trust will totally stymie this.
- Innovation comes when the work environment is not restrictive. Although zero trust may not affect some people in terms of their ability to conjure greater efficiencies, good ideas and new thinking, many will be affected.
- Security will always be seen as a challenge by those who seek to break it. Yes, this will limit the opportunity, but the challenge will remain at the same time as everything else being limited.

I am prepared to have a debate about zero trust and its applications – so far, I remain unconvinced that it is the best we can come up with. Businesses already display a "hands off, keep away" approach to security as they would prefer to buy a solution that they can imagine will solve all their problems, rather than get involved (yes, I know I am generalising).

I feel widescale application of zero trust will merely legitimise this approach and the users will lose out, quickly followed by the businesses themselves. We are in danger of abandoning culture and education entirely in a belief that the technology will save us.

The first danger there is that we know organisations are less than great at maintenance – you only have to look at WannaCry and NotPetya to see that. Even when a new patch is issued, there are *still* those that don't bother to use it. And human error is still the biggest factor in breaches and incidents. An authorised human error is still human error.

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

In this e-guide

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com