IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

What CIOs Need to Know about Zero Trust

Nathan Howe

Nathan Howe
Vice President of
Emerging Technology
Zscaler

Biography

Nathan Howe is Vice President of Emerging Technology at Zscaler (https://www.zscaler.com).

As a digital transformation and telecommunications expert, he has assisted hundreds of enterprise customers seamlessly modernize their environments adapting to distributed workforces cloud migrations and standing up private 5G networks.

He has more than 20 years of experience in the security industry and previously worked for Nestle and Verizon. He now sets the strategic direction of Zscaler.

Nathan is a regular book author having co-authored several books including: SSE eBook: https://www.zscaler.com/resources/ebooks/selecting-an-SSE-solution.pdf, ZeroTrust book and eBook v1: Published April 2022; ZeroTrust book; and eBook v2: Published August 2022: https://www.zscaler.com/resources/ebooks/seven-elements-of-highly-successful-zta.pdf.

Nathan blogs at https://www.zscaler.com/blogs

Keywords Cybersecurity, Zero-trust, Security, Investment, Infrastructure, Transformation, SSE
Paper type Opinion

Abstract

Zero trust is a cybersecurity strategy wherein security policy is applied based on context established through least-privileged access controls and strict user authentication – not assumed trust. This guiding principle of "never trust, always verify" has been in place since John Kindervag, then at Forrester Research, coined the term. Many Chief Information Officers (CIOs) mistakenly assume that they can leverage their existing IT security infrastructure to introduce zero trust protection. But as the author of this article explains, what CIOs need is a modern approach if they want to harness the full potential of zero trust.

Introduction

CIOs must learn to trust this strategic approach to security – and, eventually, say goodbye to traditional security hardware once and for all. The first thing that a CIO needs to understand about zero trust is that it is not a product, but a strategic approach to security. Forrester first proposed the concept of zero trust in IT security back in 2010. Since then, the initial idea has been developed by other parties; Google fleshed out the concept in its 2014 "Beyond Corp" strategy, and further

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

refinements were added by Gartner and the National Institute of Standards and Technology (NIST) from 2017 onwards. It was NIST that coined the acronym ZTA (zero trust architecture), and the organisation has published guidance documents that describe the disruptive approach – which is fundamentally different from traditional perimeter protection.

Rethink required

In a traditional, data-centre-based security setup, hardware appliances were stacked in racks. With each new security requirement came a new security appliance, with companies ultimately tying themselves up in an intricately woven web of firewalls, VPN gateways, load-balancers, and Denial of Service protection. As each new component was added, the infrastructure became more and more difficult to manage. As data centres relocated to the cloud, these concepts were frequently transferred across to the virtual realm and implemented in all cloud zones or with multi-cloud partners. This approach not only increased complexity and sent the number of security instances skyrocketing; it also increased the organization's attack surface risk, as many of its these components were visible online and therefore vulnerable to attack. Zero trust, on the other hand, reduces complexity and "hides" systems to slash the risk of an attack.

Driven by the shift towards the cloud and hybrid working models, data and applications are no longer solely hosted in data centres, and employees no longer only on company networks; they need to be able to access their work from any location. Accordingly, zero trust does not begin by connecting users to the


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

traditional company network. Instead, its goal is to provide a secure and high-performance connection to the applications that an employee requires – without placing the user on the network at all, and regardless of whether the application is hosted in a data centre or a multi-cloud environment.

These days, it is easy for CIOs to profile themselves as enablers of cloud transformation, as multi-cloud environments have become part of day-to-day life. But there is a lot of catching up to do when it comes to the security transformation that goes hand in hand with the shift in how we access applications and structure our workplaces – and it requires a fundamental rethinking of security.

Here are a few of the main considerations for any organization embarking on their zero trust journey.

Simplify or upgrade?

Just like the shift from combustion engines towards electromobility, switching to a fully zero trust-based approach requires a fundamental change in thinking. It takes a great deal of courage to gradually step away from the network-centric security infrastructure that has been built up over the course of many years. So, it comes as no surprise that many CIOs first attempt to upgrade their existing infrastructure in response to evolving requirements. But, trying to combine zero trust with traditional security hardware simply relocates problems without ever really solving them – just like when a “lift and shift” strategy moves existing weaknesses to the cloud rather than tackling the root cause of the problem. The performance and user experience provided by traditional virtual private network (VPNs) and legacy hub and spoke network architecture cannot match the standards achieved by the secure, high-performance application access of zero trust. Zero trust renders VPNs, which are often associated with poor performance and increased security risks, completely obsolete.

As traditional security hardware is gradually phased out, it can be replaced by a simplified, platform-based model offering security services and a central management platform. Rooms stacked high with appliances – and the administrative complexity they bring – become a thing of the past with a cloud-based Security Service Edge (SSE) approach built on zero trust principles.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Lightweight software on the client, and adjacent to the server in the data centre or in the cloud, replaces the traditional appliance stacks and ensures that all data streams, access rights, and policies can be brokered on a single security platform. This means that zero trust reduces the need for maintenance and, in turn, operational expense. The bottom line? Zero trust replaces the complexity of old with a new, easy-to-manage approach to security – an approach that focuses on the administration of rules for application access, monitoring data streams, and preventing unwanted access to or disclosure of data.

Investment protection or added value transformation?

This radical change can initially be difficult for network and security teams to accept, all the way up to CIO level, because protecting investments is always high on the agenda. Companies want to see their investments in security hardware and IT staff training pay off. Often, write-downs need to be finalized and business cases must be completed successfully before new approaches are evaluated. The CIO also needs to get to grips with the transformation of the business model that is inevitable when infrastructure is taken out of house. IT administrators will need to acquire new skills, and the centralised, platform-based mode of operation will consolidate the business model significantly.

The zero trust access (ZTA) approach gives security teams an insight into all data streams in a single management console. This paves the way for secure digitalization, as even traditional operational technology (OT) or industrial internet of things (IIoT) environments can be secured with zero trust. This holistic approach not only provides users with remote access to applications, but also provides an interface for connecting external parties or technologies and enables external parties to access production environments to perform maintenance.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Infrastructure exposed online or reduced vulnerability to attack?

The most important result that can be achieved with the implementation of zero trust – alongside providing high-performance and secure access to applications – is to effectively eliminate the external attack surface. A traditional infrastructure of firewalls, proxies, and VPN gateways needs to be exposed online in order to work; however, this mode of operation also makes it vulnerable to attack.

Over the past two years, we have all witnessed how vulnerable infrastructures and web services are when malware attackers exploit weak links that have been exposed on the internet. But attackers can't exploit what they can't see. The Log4J vulnerability is just one example of a security concern that caused widespread panic in IT teams around the world as they rushed to patch susceptible systems. Zero trust organizations, on the other hand, could afford to adopt a more laid-back approach, taking their time to decide how to respond. Of course, the vulnerability affected them too – but because their systems were not exposed online, they were able to update the affected servers in their own time, without worrying about getting to the weak link before the hackers.

A zero trust architecture provides effective protection against ransomware attacks because it also addresses other vulnerabilities, that could potentially be exploited by hackers. In particular, it effectively prevents attackers from moving laterally across systems, jumping from the infected system to the next target. The approach has a similar effect to micro- or nano-segmentation, directly connecting the user to

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

their application to prevent other systems from being infected and, by extension, stopping attackers from causing large-scale system failures.

From operational responsibility to business enabler

Compared to the pre-digitalization, pre-IT cloudification era, today's CIOs have a totally different role to play in their companies. Their job is no longer just about keeping IT infrastructure running; it's about achieving the company's objectives, with IT often playing the role of enabler. The value of the new role of IT became clear to all of us at the start of the pandemic. IT teams were required to perform the dual role of keeping operations running while also optimizing business processes, all as employees left the office in droves to work from home due to new social distancing regulations. With IT not only providing secure, high-performance remote access to all systems, but also helping to transform the company's core business, management naturally began to realise the value of the domain.

Mergers and acquisitions are another area that highlights why IT – and zero trust – make such a crucial difference to companies. When a company acquires another business, time-to-value is a critical parameter of value creation. For this to work, two separate IT structures need to be merged to enable secure, bilateral communication – and this needs to happen as quickly and securely as possible.

A zero trust exchange platform can provide secure access to dedicated applications in another network from day one. For example, the SAP or Oracle ERP system, or HR functions, might be made available first; selected employees can be given secure, rules-based access to the system they need using zero trust technology, without needing to join networks or link AD domains. Further down the line on day X, once the contract between the two companies has been finalized, IT can easily enable additional access to applications. Employees can work securely via the zero trust exchange platform, without either side being directly connected to the other company network.

Relocating applications to the cloud and making use of SaaS has become part of day-to-day life, yet security transformation is lagging behind. Opting for a platform-based zero trust concept is a way to holistically protect all a company's digital assets and enable secure business process transformation. The modern, cloud-delivered zero trust platform is continually enhanced, ensuring that any necessary adaptations are made quickly – and providing a sustainable, long-term solution that offers a whole host of benefits for its users.