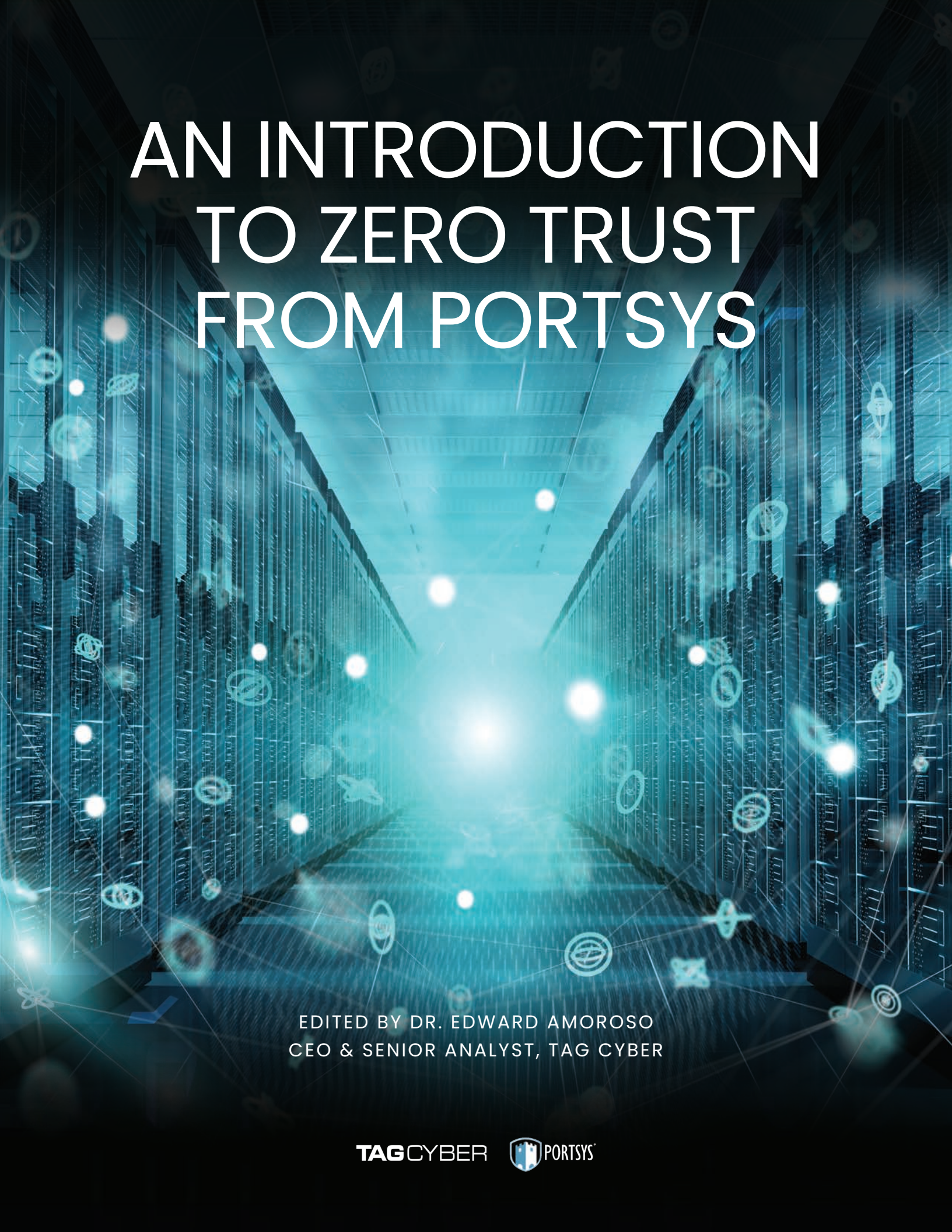


AN INTRODUCTION TO ZERO TRUST FROM PORTSYS

EDITED BY DR. EDWARD AMOROSO
CEO & SENIOR ANALYST, TAG CYBER

TAG CYBER PORTSYS

AN INTRODUCTION TO ZERO TRUST FROM PORTSYS

EDITED BY DR. EDWARD AMOROSO,
CEO & SENIOR ANALYST, TAG CYBER

ACHIEVING ZERO TRUST IS A JOURNEY, NOT A DESTINATION

CHRISTOPHER R. WILDER, TAG CYBER

ZT establishes network trust as a vulnerability and must continually verify every user, device and connection for every transaction or interaction.

Zero Trust (ZT) is one of the most consequential shifts in enterprise cybersecurity strategies. Traditionally, cybersecurity models were centralized, working with the assumption that every user should be trusted and their identities are not compromised. In this scenario, once a bad actor gets access, they can operate at will. Conversely, ZT assumes everything on the network is a threat. As more businesses move their infrastructure to a hybrid cloud and work environment, having a rigid network perimeter is no longer adequate. The shift to remote work, along with changes in how an organization provides its customers and partners with an enhanced digital experience, have resulted in IT and security teams supporting thousands of applications, databases and individuals connecting from home computers outside an IT department's control. Many enterprises currently operate with a poor patchwork of legacy security solutions and outdated tools that lack integration. As a result, security teams spend more time on manual tasks, lacking the experience, context and insight to reduce the organization's attack surface.

Trust is Vulnerability

ZT focuses on addressing the security needs of hybrid cloud environments by providing organizations with adaptive, continuous and proactive protection for users and data. In other words, ZT establishes network trust as a vulnerability and must continually verify every user, device and connection for every transaction or interaction. Applying a ZT framework also helps defenders gain insights across their security business. They can enforce security policies consistently to detect and respond to threats faster and more precisely.

The Journey to ZT

There are as many approaches to ZT as solutions in the market, but there is no argument that ZT requires a broad portfolio of security solutions. There are three key requirements for security teams wishing to take a ZT approach.

- **User Identity and Access:** At the core of ZT, multifactor authentication (MFA) helps teams manage and understand who requests access. Having a detailed access and identity policy structure confirms which resources each user can access based on their identification. MFA and single sign-on (SSO) solutions are essential, and it is important for teams to support other access points, such as portals, remote desktop protocols (RDP), mobile device management (MDM), VPNs, reverse proxies, etc.
- **Data & Application Security:** Even with a strong identity and access policy and measures, data and applications are still open to breaches, even if the data is at rest or in transit. End-to-end encryption, automated backups and hashed data are effective ways of incorporating ZT methods. Furthermore, hosted services and Software as a Service (SaaS) solutions create additional enterprise vulnerabilities. We believe SaaS solutions present other security risks, especially with compliance and third parties, so SaaS providers must enact ZT methods.
- **Context of Access is Key:** Deploying a Zero Trust approach requires enhanced output beyond traditional binary authentication protocols such as login and password. ZT associates details and traits to verify who is connecting, as well as the context of their relationship and access to the network. Each enterprise has various requirements to ensure access and context are applied across the entire organization. It is important to know the differences between information and context; each relies on the other and is essential when making decisions, but context makes information actionable and a foundation for zero trust environments.

In Conclusion

As cyber threats grow more sophisticated, they aim to inflict as much damage as possible while avoiding detection. Determined hackers will target any vulnerability within the enterprise. If an attacking force can break into the network at a weak point—through an application, for example—this shouldn't lead to catastrophic system collapse.

Organizations pursuing a ZT approach take advantage of advanced security functionality to protect all systems, users, workloads and endpoints. Finally, ZT enables security and IT teams to focus their time and efforts on driving the digital transformation that makes their company more competitive, as well as providing a better user and customer experience, instead of dedicating valuable time and resources to fighting attacks.

THE ROLE OF IDENTITY AND ACCESS MANAGEMENT (IAM) IN A ZERO TRUST WORLD

JOHN J. MASSERINI, SENIOR ANALYST, TAG CYBER

Integrated IAM practices should be considered a key element of any strategic risk mitigation program.

Without question, one of the most frequently referenced terms being used in the industry lately is zero trust. Whether it's part of a sales pitch or a strategic part of a CISO's plan, it seems that everyone is hopping on the ZT bandwagon, including identity and access management (IAM) solution providers.

Unfortunately, while many believe ZT will solve all our collective security problems, the reality is that it is only as good as the foundation it's built upon. A significant part of that foundation is identity management, an oft-overlooked practice that addresses many of the risks faced by most enterprises today. Similarly, access management is often relegated to what Active Directory group a user is part of. Sadly, account management, user access and provisioning are all practices that are typically relegated to a first-tier help desk technician, whose job is strictly measured by ticket resolution time. That approach can be short-sighted—not to mention dangerous—when it comes to securing your applications and resources across the enterprise. Instead, integrated IAM practices should be considered a key element of any strategic risk mitigation program. This becomes especially true when implementing a ZT architecture, where both continual and contextual authentication are needed.

When you begin looking at how a ZT architecture will fundamentally change your approach to risk mitigation, you quickly realize how crucial a solid, well-planned IAM program is to the success of your ZT initiative. By having a very high level of trust in your IAM environment, you can develop your ZT architecture knowing you have a strong base to build upon. A key factor in developing a strategic IAM solution is recognizing that it is about far more than just user access. A modern IAM solution supports full integration of all platforms, as well as assigned roles—birthright, departmental, and job function, for example—along with user risk modeling and certification practices with full contextual evaluation and automation across all on-premise and cloud infrastructures.

Conceptually, the idea behind a ZT architecture is that every operation—whether it be a financial transaction, running a report, or just accessing a website—*is authenticated and authorized every time.* Unlike the typical legacy infrastructure where you are authorized at the time of authentication and remain authorized until you log out, in a ZT world, every click of the mouse is re-authorized. If you imagine a modern web application trying to reauthorize millions of transactions daily, you can understand the benefits of having a single source of truth for authenticating access to your resources and applications, wherever they reside, be it local or cloud.

Another key aspect of ZT access management is not just who is performing the operation, but contextually, *should* they be. Many contributing factors should be evaluated when determining when access should be granted and at what level; factors such as location, time and device are just a few indicators that can be used. For example, the company CFO is on vacation and has an urgent transaction to approve on the financial platform. Are they using their corporate laptop or the shared device in the hotel's business center? Did they previously sign on from a location that would be impossible to travel from since the last login? Has someone been trying to use the account surreptitiously between the last valid login and this one?

While the benefits of having an integrated, mature IAM process are obvious on many levels, getting there is not an effort to be taken lightly. In many cases, core infrastructure components such as Active Directory and the human resource information system (HRIS), as well as the corporate and enterprise resource planning (ERP) systems can easily be integrated into an IAM platform. Ensuring, however, that business applications, network devices, Linux/Windows servers and cloud infrastructures are as tightly connected will be no small task. Layering on the complexity of determining which access indicators are crucial will take time and effort—but will have a significant upside in the long run.

While there continues to be significant hype around AI-based solutions, it is more important to get the basics right first. This will have a more significant impact on your security than complicated technologies. AI technologies have substantial promise in evaluating contextual indicators and, in this light, are remarkably well-suited for machine learning. However, without first managing the fundamentals properly, you are still building on a poor foundation.

Make no mistake, deploying a sound IAM solution is as "business transformational" as you can get, especially to the business of IT. However, if your enterprise is serious about moving towards a ZT architecture, the effort to build a true IAM infrastructure is well worth it. Even if there are no plans for ZT, the benefits to your compliance, audit and regulatory reporting efforts—not to mention your overall risk mitigation practices—will benefit significantly.

BEST PRACTICES FOR APPLICATION SECURITY IN A ZERO TRUST ENVIRONMENT

DR. EDWARD AMOROSO, CEO, TAG CYBER

Total Access Control (TAC), allows users to reach applications and workloads safely and securely without compromising the need for single sign-on, role-based access control (RBAC), multifactor authentication (MFA) or even a virtual desktop.

This chapter discusses the best practices and procedures for securing user access to important business applications hosted locally on premises or across multicloud infrastructures.

Modern enterprise users tend to define their work by the applications and workloads they access both locally and in the cloud. In this sense, applications have become the new day-to-day interface for most employees, contractors and suppliers in a typical business environment. While this access might have been secured previously by a traditional perimeter, with users visiting applications across a flat enterprise local area network, today, this access must be secured in the context of a zero trust architecture. This implies the need for a fundamentally different approach to application security.

Next-Generation Secure Reverse Proxy

The good news is that despite the changes inherent in the modern shift from a perimeter-based security philosophy to zero trust, many of the best security methods to provide secure access are based on familiar techniques. This is beneficial for enterprise security teams trying to develop a protection architecture without having to completely modify their approach. One aspect of this familiar toolset is the reverse proxy, which is commonly applied across existing enterprise architectures. The use of reverse proxy methods to service applications in a zero trust scheme remains relevant—albeit implemented in a way that is consistent with digital transformation and cloud hosting.

PortSys Total Access Control (TAC)

One commercial implementation of next-generation reverse proxy for application access comes from PortSys. The solution, called Total Access Control (TAC), allows users to reach applications and workloads safely

and securely without compromising the need for single sign-on, role-based access control (RBAC), multifactor authentication (MFA) or even a virtual desktop. PortSys does this with a reverse proxy that supports browser-agnostic application delivery across any multicloud-based hybrid infrastructure. An advantage of TAC is that is consolidates many existing or planned secure access solutions into one common platform, which helps reduce cost and complexity. In addition, legacy applications are handled in a more flexible and secure manner with a browser-agnostic solution.

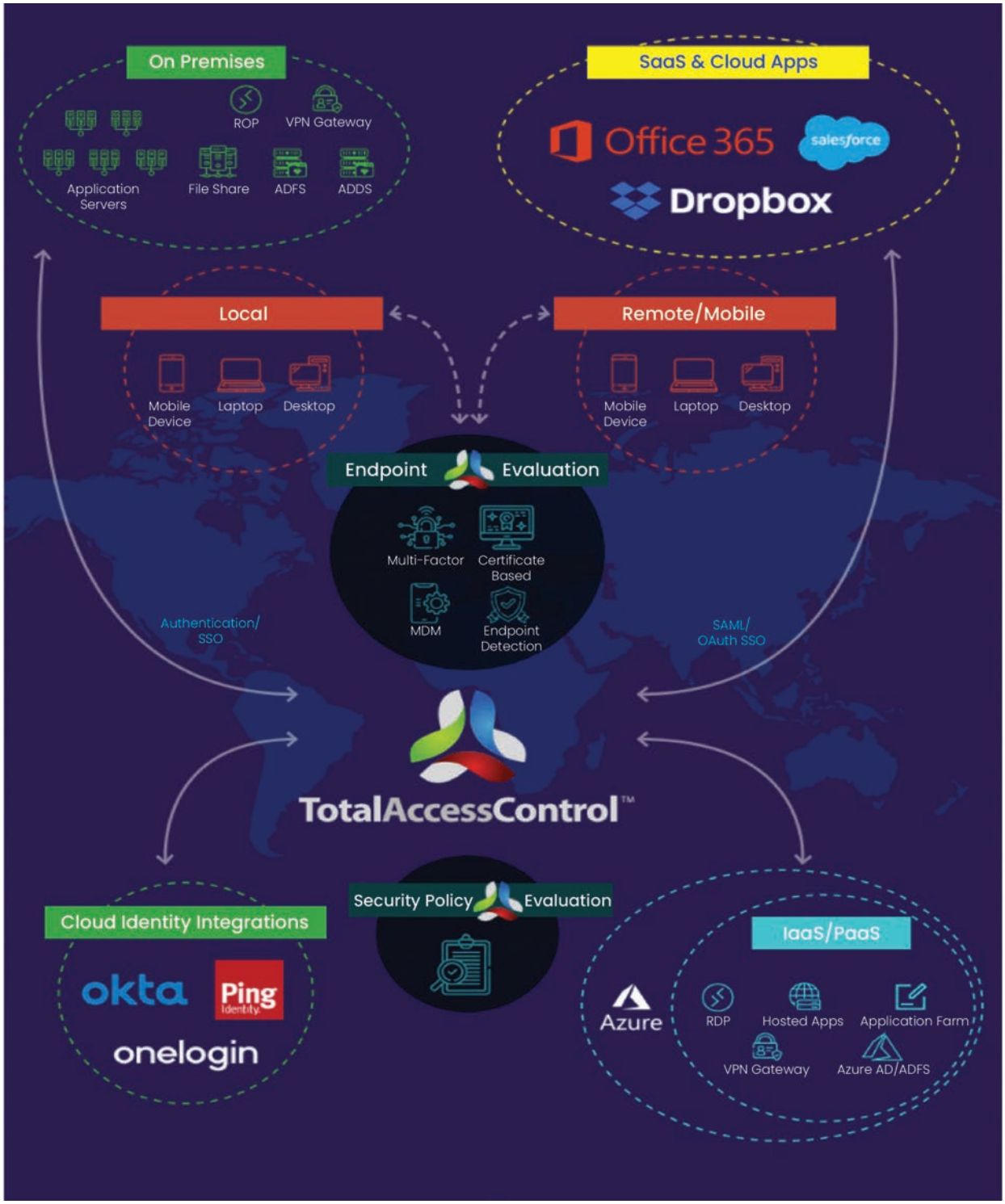


Figure 3.1 PortSys TAC Architecture

Application Security Architecture

The most common architectural deployment for PortSys TAC starts with applications hosted either on premise, in the cloud, or in a SaaS-based infrastructure (as shown in Figure 3.1). Laptops, mobile phones or other devices can then locally or remotely access these applications using the TAC solution, which offers local support for authentication and SSO, as well as cloud/SaaS support via SAML/OAuth. TAC includes cloud identity integration with major commercial identity and access management (IAM) providers such as Okta, Ping and OneLogin. The platform also supports secure access to IaaS/PaaS workloads hosted in the cloud, such as Azure and AWS. These include secure access via RDP or VPN gateways, along with integrated support for Active Directory (AD). The entire capability is governed by security policy definition.

Action Plan for Secure Application Access

Enterprise teams are advised to review their existing secure access implementation to determine whether zero trust principles are being properly addressed. Too many enterprise security teams remain solely dependent on local protections based on perimeter controls from the public Internet. From a TAG Cyber perspective, we believe that secure access via next-generation reverse proxies as implemented by PortSys TAC is a promising option. Enterprise security and network security experts should take the time to review the platform and consider potential integration into their evolving architecture.

USING REVERSE PROXIES TO SECURE ENDPOINTS IN A ZERO TRUST ENVIRONMENT

DR. EDWARD AMOROSO, CEO, TAG CYBER

One effective protection approach found in nearly every modern security architecture is the reverse proxy.

This chapter explores how reverse proxy solutions are useful to secure endpoints in emerging zero trust environments. The PortSys Total Access Control (TAC) system is used to illustrate this approach in a practical enterprise environment.

Different enterprise security architectures deployed across enterprise organizations will vary in their specifics. For example, some enterprise security teams will buy into the full solution suite from one commercial vendor, whereas others might be more comfortable dealing with a variety of tools from a range of vendors. This will have implications on how their solution architecture protects resources, be they local, in the cloud or a combination of both. There are, however, many aspects of modern cybersecurity architecture where high levels of commonality will be found, even across organizations of varying size and scope, as well as different business and government sectors. This is sometimes driven by common compliance requirements, but it is more often led by a shared view of effectiveness. Such agreement helps teams adopt best practices and benefit from shared learning. One effective protection approach found in nearly every modern security architecture is the reverse proxy. This solution has been in place for many years, and unlike firewalls and passwords, reverse proxies are not being phased out. In fact, they are more relevant than ever. This article shows their utility in securing endpoints and enabling zero trust. We reference the solution from PortSys in our discussion below to illustrate this case.

WHAT IS A REVERSE PROXY?

A reverse proxy is a piece of software that intercepts and forwards requests from browsers to back-end applications to improve security and performance. Client users view the interaction as being with the

back-end application directly—hence, the term proxy. This is useful for security teams tasked with minimizing user friction. Forward proxies, by the way, are used to securely obtain Internet resources on behalf of corporate users. Reverse proxies are especially useful when it comes to enforcing security policies, as well as other security functions such as HTTP header inspection and support for TLS. A reverse proxy also offers many non-security benefits for legacy and hosted web applications. For example, they can help balance network delivery, compress traffic, cache content, and reduce the load on servers supporting the application.

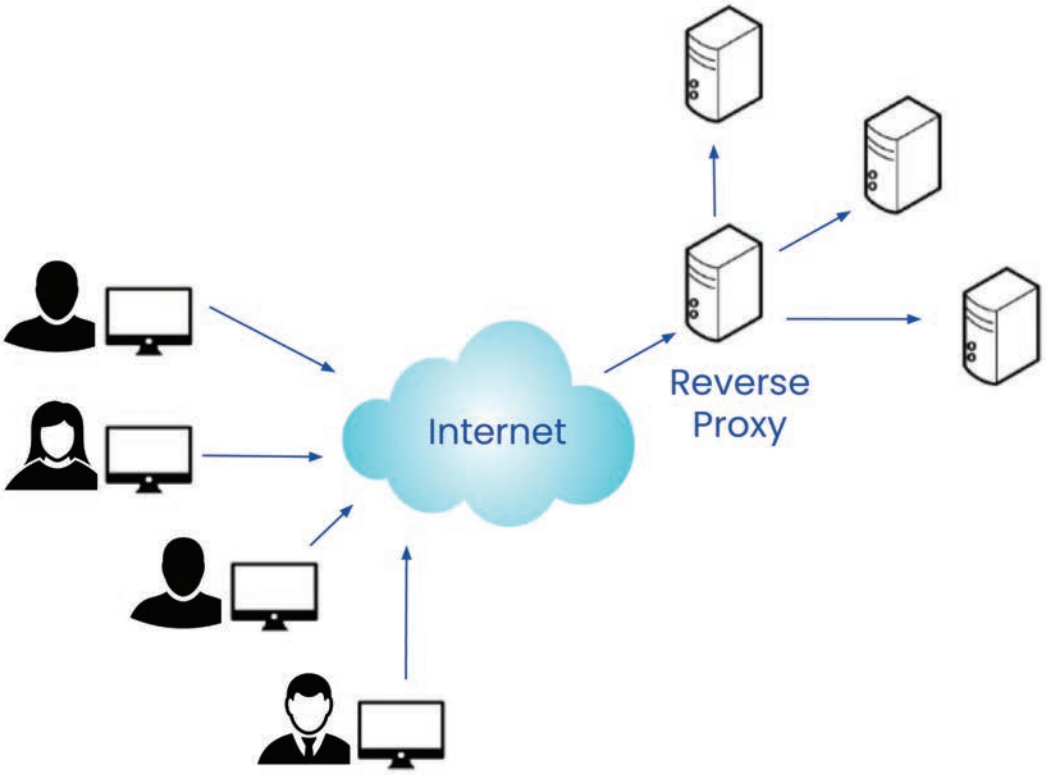


Figure 4.1 Reverse Proxy Operation

How do Reverse Proxies Support Endpoint Protection?

As one would expect, the use of reverse proxy solutions for legacy and web applications have a positive, holistic impact on the overall protection profile for both the secured application, as well as any accessing clients. This implies that the deployment and use of reverse proxies across enterprise and Internet infrastructure actually reduces the burden of endpoint detection and response (EDR) solutions to protect PCs and other user devices. This is evident in TAC, which deploys into the enterprise as a reverse proxy, enabling a range of endpoint protections. For instance, TAC is designed for zero trust access from managed and personal devices coming from a range of different locations—both local and remote. Rather than implement endpoint security to enable access, TAC can be inserted to enable properties such as zero trust, as well as features such as single sign-on.

How do Reverse Proxies Support Zero Trust?

An additional useful feature of reverse proxy usage is that it enables application access from a more generalized set of locations. In other words, by protecting hosted resources, organizations can allow users to gain access from virtually any type of environment, including remote access, work-from-home, or other modern virtualized arrangements. This is typically a major requirement for enterprise work today. In this sense, reverse proxy capability—such as that implemented by PortSys—helps drive the adoption and use of zero trust initiatives. The transition from perimeter-based security to zero trust-based architectures is a useful advance in enterprise security design, because it reduces dependence on the corporate firewall. As such, reverse proxies help streamline this design approach, ultimately reducing overall cyber risk.

AN OVERVIEW OF TOTAL ACCESS CONTROL (TAC) FROM PORTSYS

DR. EDWARD AMOROSO, CEO, TAG CYBER

The primary functional capability that enterprise teams will benefit from through the deployment and use of the PortSys TAC solution is secure access to local and cloud resources for end users.

In this chapter, we examine how Portsys Total Access Control (TAC) works, along with guidance for enterprise teams on how the reverse proxy and remote access features can be used to drive zero trust and other desirable security attributes for their enterprise.

The Total Access Control (TAC) platform from commercial cybersecurity vendor PortSys provides a range of useful cyber protection features for the typical enterprise team. These protections focus on advancing support for zero trust and secure access across the organization. This brief chapter offers an independent explanation of how this security platform works and how it can be deployed into a modern enterprise network.

Major TAC Functionality

The primary functional capability that enterprise teams will benefit from through the deployment and use of the PortSys TAC solution is secure access to local and cloud resources for end users. This includes employees, suppliers, partners and customers. Applications are made available to users with authenticated and authorized permission, as per the reverse proxy nature of the TAC platform (see Figure 5.1).

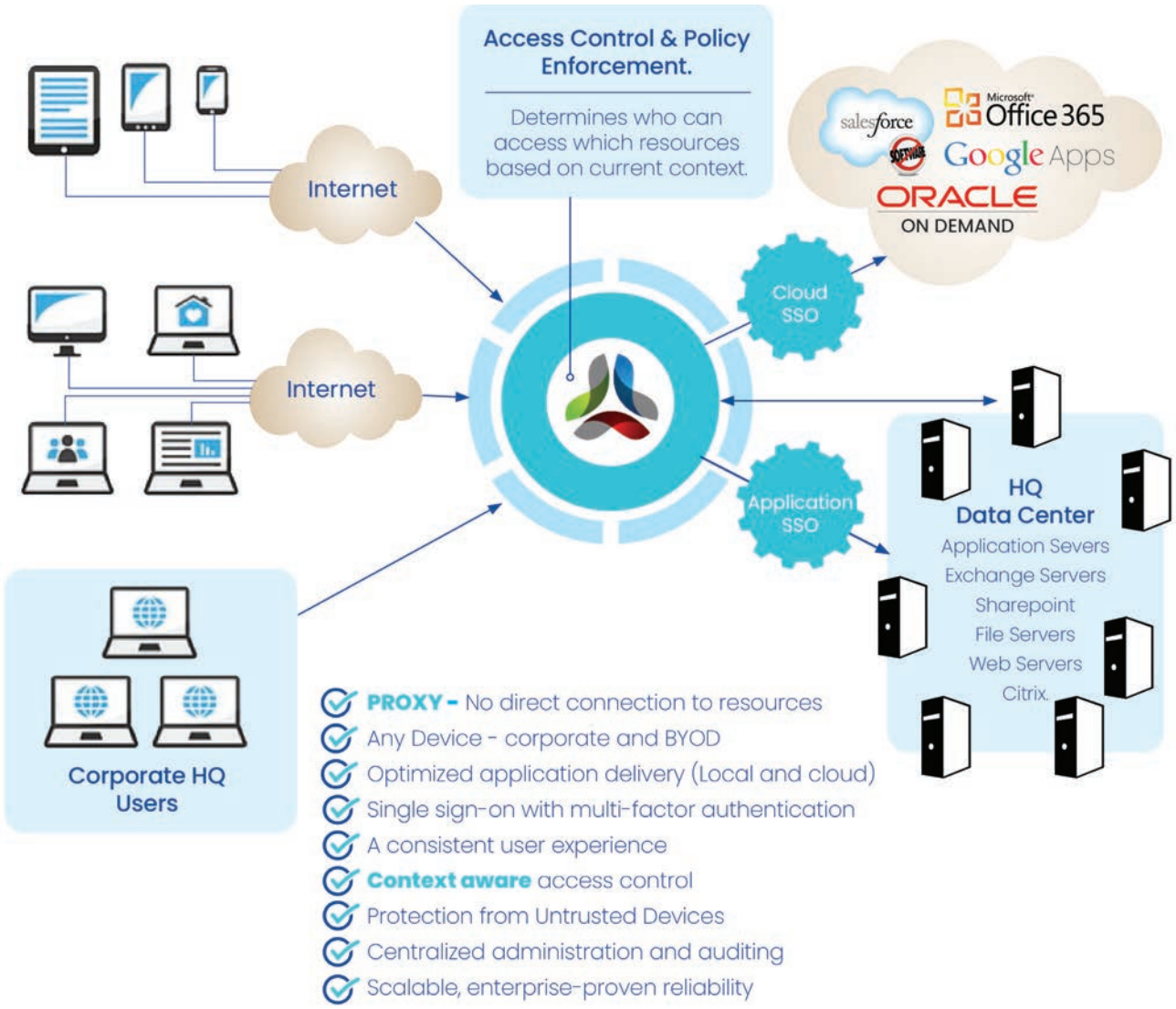


Figure 5.1 PortSys TAC Functionality

It is this policy-based enforcement of access that allows enterprise security teams to transition their traditional access control mechanisms to a more flexible virtualized infrastructure. The result allows security teams to leverage the following capabilities:

- **Proxy Connections:** This ensures no direct access to applications.
- **Device Support:** Access is supported for a range of devices, including those that are personally owned.
- **Persistent Authentication:** Applications can be connected to single sign-on (SSO).
- **Context Aware:** Policy enforcement and access control context.
- **Administration:** Centralized management and monitoring can be enabled.

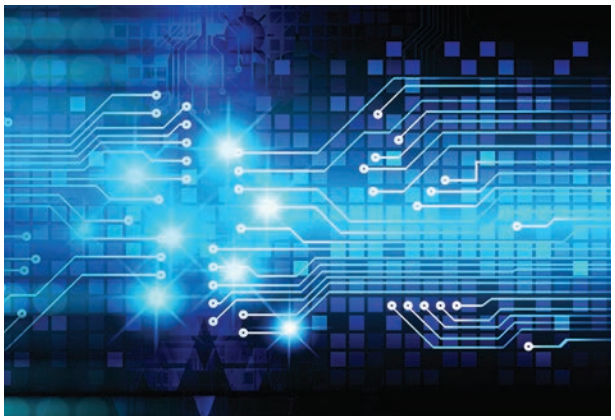
These functions support use cases involving access by users from corporate headquarters and the internet to applications that might be hosted in legacy environments, as well as through public and private cloud-based services.

Support for Remote Access

In addition to reverse proxy separation, the TAC platform enables highly secure remote access. In fact, this solution serves as an effective replacement for awkward virtual private network (VPN) platforms and infrastructure. The simplicity of managing TAC for external access, along with its centralized administration, makes it an excellent solution for achieving zero trust.

Advancing Zero Trust

As suggested above, zero trust is dependent upon proper protection of endpoints, secure network connectivity, and run-time security for applications—usually hosted in a virtualized environment. The PortSys TAC solution supports these goals through a separation of users and applications via the proxied connection. This ensures that policy enforcement can be performed effectively for all sessions.



ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective..

ABOUT PORTSYS

PortSys, Inc. is a global innovator in information security and Zero Trust access control. Enterprise organizations around the world rely on its Total Access Control (TAC) reverse proxy technology to strengthen, simplify and unify IT security, making the lives of administrators and end users easier.