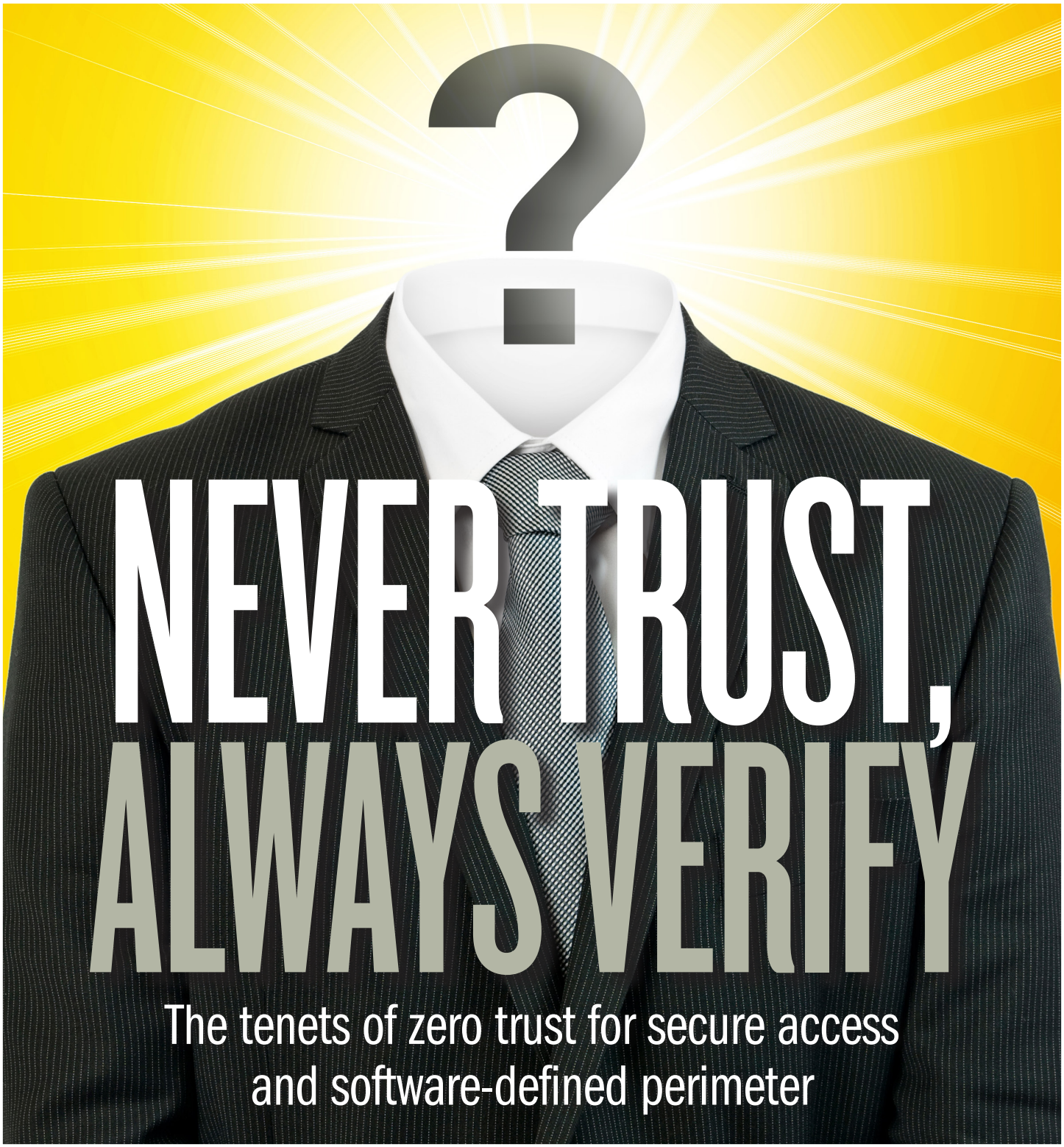
Pulse Secure

ExpertFocus

Brought to you by Pulse Secure

January 2019



NEVER TRUST, ALWAYS VERIFY

The tenets of zero trust for secure access and software-defined perimeter

Building zero trust for secure access and exploring the software-defined perimeter

Our dynamic world of mobile and cloud computing requires advancing secure access capabilities based on continuous verification and authorization – the old moat-and-castle perimeter model is as outdated as, well, moats and castles. Here's why and how to apply Zero Trust model for Hybrid IT access and how software-defined perimeter adoption will expand in the years ahead. Steve Zurier explains.

When China started building its Great Wall more than two millennia ago, the technology was appropriate to keep invaders out and protect the Chinese people's lives and property. Today, that technology is, for the most part, obsolete. Functionally it would keep out only the most basic ground attacks, not unlike the traditional technology designed to protect network perimeters.

But basic network devices from just a decade ago are hardly a match for today's sophisticated attacker in this age of mobile devices, cloud applications and anywhere anytime access. How can security managers protect the company when such a large percentage of the staff works outside the corporate environment and the vast majority of users now run cloud apps, mobile devices and other non-corporate computing technologies? Clearly, something has to change.

While traditional perimeter defenses are still crucial to set corporate boundaries on the internet, along with the use of firewalls, virtual private networks (VPNs) and network access control (NAC) technologies to assure role-based and segmented access to network resources, the security industry has been implementing a Zero Trust model to mitigate malware, attack, breach and data leakage risks. A Zero Trust model applies authentication, authorization and verification controls to users, devices, applications and network resources as part of perimeter-based access security. This is all about proving identity, location, device, and security state before and after being granting access based on least privilege to applications and resources in the data center and multi-cloud.

Scott Gordon (CISSP), chief marketing officer at Pulse Secure shared that "the dynamic provisioning of virtual network and cloud applications and resources, as well as the diversity of users and devices requesting access have materially contributed to the security breaches and identity theft that are in the headlines. One gap is visibility. Enterprises do not have accurate data or insight into who or what is accessing their resources. IT can not see the insecure devices and connections that are propagating viruses or leaking sensitive data. IT can only

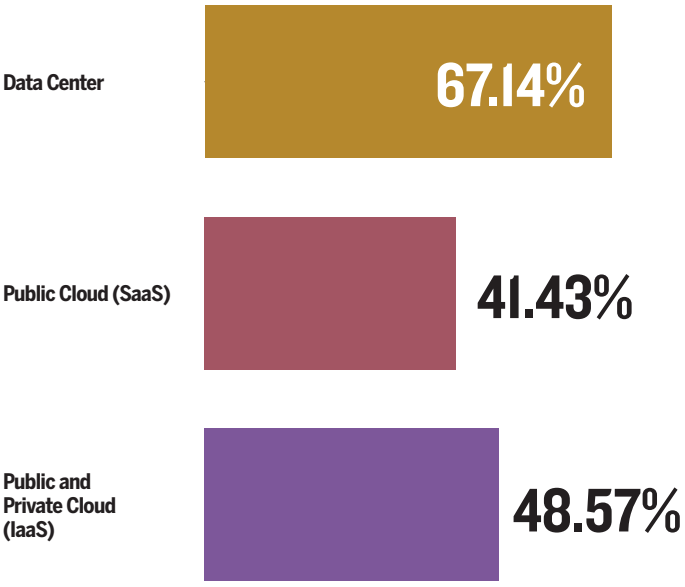
"Think of Zero Trust as a security model and SDP as the upcoming security architecture that companies will use to manage access security for hybrid IT"

– Rob Koeten, chief software architect, Pulse Secure

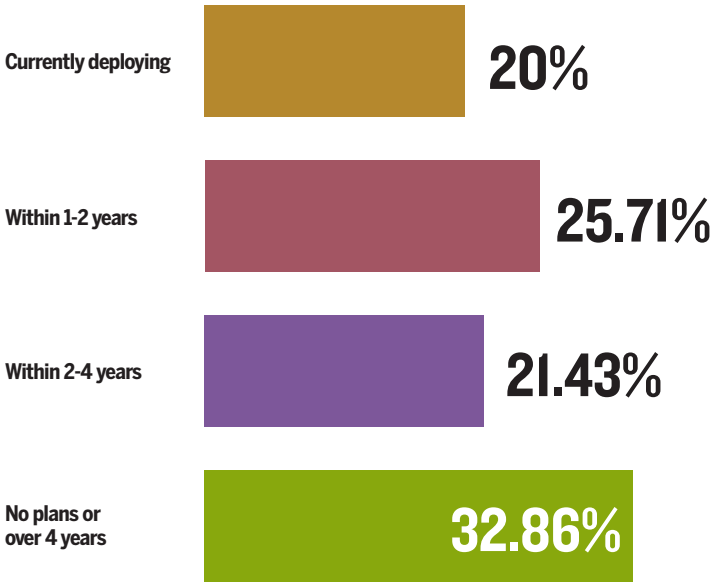
account for 70% of devices on their network and are thus susceptible to IoT exploits. Another gap is access policy granularity and enforcement consistency. When IT staff have many disparate security systems and policy components to manage, an enterprise's secure access controls can not be broadly instrumented, and orchestration becomes cumbersome if not piecemeal. This also impacts user productivity as employees content with multiple login requests, lost passwords, and unavailable services."

Gordon adds: "So where is this all heading and how can secure access be fortified? As businesses take advantage of mobile workforce and consumers, they have also been actively migrating their data centers and "webifying" applications to the cloud. To this end, security professionals have been building out an application-based access security architecture called Software Defined Perimeter (SDP). SDP leverages the Zero Trust tenet of 'never trust, always verify' by essentially enabling secure access directly between the user and their device to the application and resource no matter the underlying infrastructure - but in a scalable way and according to policy. In a sense, SDP enables Secure Access elasticity as users gain easy means for access protection which travels with them everywhere they go, with what devices they use, and

How does your company deliver/consume corporate applications and computing resources?



When do you expect to fully deploy a Software Defined Perimeter platform across your hybrid IT environment?



"SDP leverages the Zero Trust tenet of 'never trust, always verify' by essentially enabling secure access directly between the user and their device to the application and resource no matter the underlying infrastructure - but according to policy."

– Scott Gordon, chief marketing officer, Pulse Secure

where ever the application resides."

Rob Koeten, chief software architect at Pulse Secure, explains that SDP works hand-in-glove with the Zero Trust architecture. With Zero Trust, the network treats everyone the same — suspiciously and with no trust — and does not grant access until the users has been validated by the SDP system.

"Think of Zero Trust as a security model and SDP as the upcoming security architecture that companies will use to manage access security for hybrid IT," Koeten says.

"Pulse Secure's approach to SDP extends access all the way from the user and device through the data center or multi-cloud, leveraging Zero Trust functionality," says Prakash Mana, Pulse Secure's vice president of product management. Before granting access, an SDP system will take five distinct actions:

Survey respondents optimistic about SDP

A recent poll of security professionals by SC Media found that while security professionals believe that a software defined perimeter (SDP) can dramatically improve security, a transition to this new model will take several years.

The survey found that 78 percent of respondents thought it was very likely or likely that SDP could isolate apps from an untrusted network. Seventy percent say SDP will improve DevOps security and 62 percent say it can improve IoT threat management.

Overall, 64 percent of the respondents were either extremely confident or very confident that SDP could manage security access requirements from the data center and across the cloud.

"The survey shows that the respondents think that security is gradually getting better," says Chris Christiansen, a senior analyst with the Hurwitz Group. "I think if you separated it out by vertical, the financial sector would have much higher confidence and with manufacturing and medical it would be much lower."

Christiansen adds that like in many other situations a small percentage of early adopters will lead the way. He points out that while confidence remains high, roughly one-third still have no plans to deploy SDP in the next four years. Only 20 percent were currently deploying SDP and 26 percent planned to deploy it in the next two years.

"SDP requires that people think about security in a different way," Christiansen says. "Most people still view security as an obstacle. The way SDP will sell with people is if the vendors focus on what it will do for the business. In the future, security will be baked into the applications and it will let people do their jobs easier, faster and without fear that the lack of security will cripple their businesses, causing extended litigation and a costly forensics process." — SZ

"Gradually evolving to the new SDP security methodology is, in the long-term, best interests of the business."

– Chris Christiansen, senior analyst, the Hurwitz Group

5 questions to ask before implementing SDP

Chris Christiansen, a senior analyst with the Hurwitz Group says there's a long laundry list of questions security managers should ask before deploying a Zero Trust security stance with a software defined perimeter (SDP), along with offering suggestions on how to move forward.

1. Do you have a consensus on the level of risk the company is willing to take? Explain to management that in this mobile world based on clloud applications the old way of doing security is no longer the recommended option. Explain that moving to SDP will take time and that while there's a certain level of risk to deploying a new technology, gradually evolving to the new SDP security methodology is, in the long-term, in the best interests of the business.

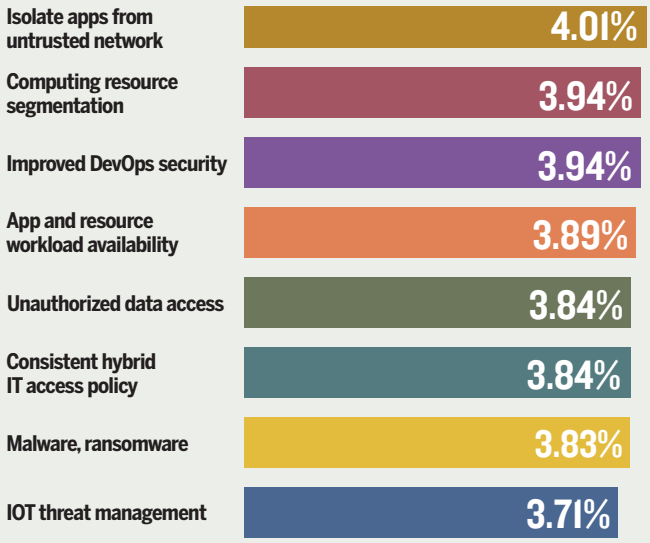
2. What is your corporate access policy? Figure out what your policy is today and what you need it to be going forward. Do you want to go from simple passwords to complex passwords and two-factor authentication? How can you best do that?

3. Have you talked to your DevOps people? Work with the DevOps team and get them on board with embedding secure access into all the applications they develop. Odds are they will be receptive to working in this manner because they are typically well-schooled technologists who understand what is at stake.

4. What regulations impact the company? All public companies are subject to *Sarbanes-Oxley Act* (SOX) and have requirements that specify different levels of information access. SDP can play a huge role in helping a company meet those requirements in a much more secure way. The same holds true for companies that must abide by the Payment Card Industry Data Security Standard (PCI DSS) and *Health Insurance Portability and Accountability Act* (HIPAA) requirements. Only companies that accept or process credit or debit cards must comply with PCI DSS, but any company that offers medical benefits or handles medical data must comply with HIPAA.

5. Does our potential SDP vendor "talk techie" or do they focus on business benefits? Too many vendors lose potential customers by explaining the intricacies of SDP. Find a vendor that has podcasts, videos, and webcasts that can explain to the rank-and-file staff within the business how these new security measures will help them do their jobs more efficiently and securely.

What is the likelihood that the following vulnerabilities would be addressed by applying software-defined perimeter/hybrid IT secure access technology? (Weighted avg.)



"Pulse Secure's approach to SDP extends access all the way from the user and device through the data center or multi-cloud, leveraging Zero Trust functionality."

– Prakash Mana, vice president of product management, Pulse Secure

1. Identify and authenticate the user. Is the user an employee or a third-party contractor and in what department do they work? This step identifies the user to ensure that they have appropriate rights to access not only the network, but also the data they are requesting.

2. Authenticate and assess the device. Is it a desktop computer that sits on the internal network or perhaps a mobile device owned by an authenticated user? At this point the software identifies not only the device, ownership and operating system, it also confirms compliance configuration and if the device is authorized to access the app or resource. It determines the security state.

3. Determine the network. How is the user trying to access the network? Is the user coming from the corporate network, an airport, or a local coffee shop network where security is typically less secure? Perhaps the user is trying to connect from a home network with a router issued by a cable company. Authenticating the user's location can help determine if this is really the user or someone using compromised credentials, trying to access from a location inappropriate to the user.

4. Assess the service request. For which services (applications and resources) is the user authorized to access? Is the service from the data center, the cloud, or perhaps a client-server application service? And what access rights do they have? If the user is a company salesperson, for example, he or she should have access to client lists, sales forecasts and quarterly results reports, but not human resources information on employee salaries, sensitive medical records, or any proprietary intellectual property.

5. Establish secure connection. An SDP Controller will communicate to the endpoint and the network resources closest to the application and data to determine if the access request should be granted according to policies maintained in the SDP Controller. If access is granted and the security state has not changed, the SDP Controller will send instructions to the respective entities in order to establish a protected connection between the device and the application.

Zero Trust in action

At Borgess Health Alliance in Kalamazoo, Mich., a top priority has always been protecting the private health records of its sensitive patient data. However, over the past several years, the physicians have been looking for a way to view electronic medical records remotely, so protecting patient data is more problematic since the user is often remote. Many of the company's employees work at different facilities and they all wanted the convenience of accessing work information at home or while traveling from site to site.

While the hospital's administrators wanted to grant the medical staff remote electronic access to patient information, they had to ensure that the technology was secure and offered the ability to restrict access based on a person's role within the hospital system. Doctors and nurses would get different levels of access to patient information than administrative staff or medical technicians, for example.

By implementing a zero trust-based approach, Borgess extended data center and cloud access out to 1,200 employees, not just the medical staff, also making it possible for employees to work remotely. Pulse Secure's approach let them customize access policy based on

"You can call it SDP if you want, but the bottom line emphasis will be less on firewalls and more on access management."

– Edward Amoroso, CEO, TAG Cyber

department, position and role within the company, ensuring they were continually protecting the private medical information of the more than 1 million patients Borgess serves.

"Pulse Secure not only generated immediate cost savings for our organization, but it also saved our physicians' valuable time. The benefits were also passed on to our patients – our top priority – ensuring their private medical data remained secure, while at the same time enabling their doctors to focus more on care and less on logistics," said Jeff Johnson, information security technical specialist at Borgess Health Alliance.

Pulse Secure's granular access policy engine supported data privacy compliance regulations and fostered a better work-life balance for their practitioners. Medical staff could now leave work at more reasonable hours knowing that they could check records and complete paperwork from anywhere and on the device of their choice. More so, they did not have to understand the intricacies behind the technology; it just worked with no disruption of workflow.

Use cases for SDP

Koeten outlines three use cases for companies to transition to a Zero Trust security model based on an SDP architecture.

Secure cloud apps: As companies move applications such as email, timesheets, and travel and expense reports to the cloud, the old perimeter methods of security do not work. The security team can provide better security by having a perimeter model based on access rights that a company can extend outside the traditional data center. Based on specifically assigned roles and permissions, users are granted access to each, discrete business application.

Secure DevOps teams: The rise of the cloud has also seen the emergence of the DevOps. With cloud apps, the gateway must be deployed dynamically within the apps as they are developed and deployed. Based on this approach, security and access rights get rolled into the application, so no application ever gets deployed without building SDP in from the outset.

Secure privileged access: Start-up companies that deliver cloud apps to customers have pioneered an approach of micro-segmentation in which an application gets divided into two parts: the piece that is available to the user and the portion that the administrator can access. In the SDP model, it is now possible for most any company to realize Zero Trust advantages with built-in security for everyone who accesses an application. In many situations, companies will increase the requirements for administrators to get access to privileged segments. So based on access rights, users gain access to the basic features of the application, while administrators can gain privileged access to update tables, delete tables, or add another databases instance.

Koeten says he expects companies to migrate to SDP over several years, adding that it will not require a rip-and-replace of the company's security infrastructure.

"Companies will take an evolutionary path to an SDP architecture," Koeten says. "Certainly the early adopters will be more aggressive, but as companies deploy more cloud apps, they can simply build SDP into the new apps. The idea is that over time, the company can get more consistent coding security into the application and there will be

"Pulse Secure not only generated immediate cost savings for our organization, but it also saved our physicians' valuable time."

– Jeff Johnson, information security technical specialist, Borgess Health Alliance

less room for errors. This will lead to many fewer misconfigurations."

Edward Amoroso, CEO of security consultancy TAG Cyber, says, "Secure access is the new perimeter. You can call it SDP if you want, but the bottom line emphasis will be less on firewalls and more on access management."

Amoroso explains that enterprises will find that rehosting enterprise workloads, one-by-one, into a virtualized data center or cloud ecosystem, will become the best way to manage data and applications. Each time a workload gets hosted, it should receive micro-segmented security protection, which allows security pros to simplify the DMZ firewall ruleset. The end goal becomes zero-trust, with device-to-cloud access of hosted workloads in the cloud with no perimeter in the traditional sense.

Amoroso agrees with Koeten that companies will migrate to SDP over time. He says there is no reason to take all the firewalls down mainly because many of the audits are based on firewall logs; companies just cannot go off that system all at once. It is going to take them time to adjust to the new model as they migrate more of their business applications to the cloud.

"The perimeter works about as well as police tape around a physical crime scene" Amoroso says. "It prevents honest people from entering a clearly delineated space but does nothing to stop determined and capable actors from climbing underneath or going around. The new solution requires distributed, virtualized, compartmentalized data protection. So people ask me 'Is the perimeter dead?' I tell them, 'No, it's not dead; it's just changed.'"

Effectively the perimeter exists wherever people work. Security professionals cannot build a line in the sand and guarantee that from a certain point at the edge of the network bad threat actors cannot penetrate the corporate network. One can think of SDP as an extended perimeter that goes with employees and business partners wherever they go. Moving forward, company networks will trust no one and users will only have access to the applications and data set in policy rules.

The *raison d'etre* for Zero Trust and SDP, the company maintains, is that if you cannot prove who you are, prove the device is yours, prove you are running over a secure network, and prove you are allowed to use that service or application, you should not gain network access. This will make life much more difficult for the hackers who have preyed on misconfigurations and poor access and password management.

With SDP, supporters of a Zero Trust model maintain, the hackers will have to wind their way through multiple access barriers, something that will knock out many of the low-level players. While there will always be threats, Zero-Trust offers companies a fighting chance to stay secure. ■

Pulse Secure offers easy, comprehensive Secure Access solutions that provide visibility and seamless, protected connectivity between users, devices, things and services. The company delivers suites that uniquely integrate cloud, mobile, application and network access to enable hybrid IT. More than 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net

Get Your Head out of the Clouds.

Zero Trust Access Security for Hybrid IT

Your business is taking advantage of cloud, and taking on increased malware, IOT, availability and data leakage risks.

More than 20,000 enterprises entrust Pulse Secure to deliver Zero Trust security to empower their mobile workforce to access resources from the data center to the cloud while ensuring business compliance.

Learn why at **pulsesecure.net/zerotrust**

Pulse Secure®

pulsesecure.net

Copyright 2018 Pulse Secure, LLC. All rights reserved. Pulse Secure and the Pulse Secure logo are registered trademarks or Pulse Secure, LLC.