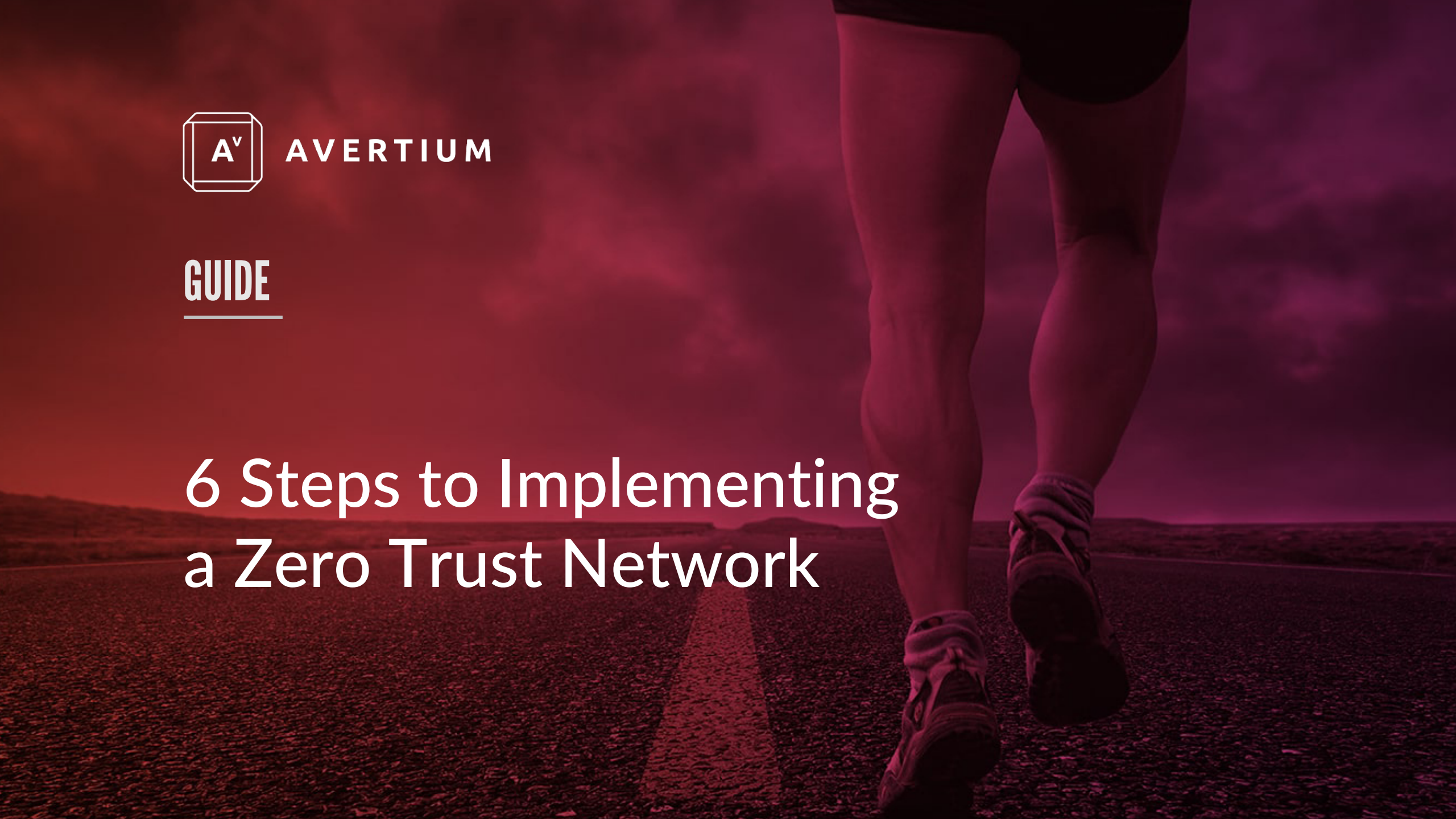


AVERTIUM

GUIDE

6 Steps to Implementing a Zero Trust Network

INTRODUCTION

Zero trust is designed to replace the insecure, perimeter-based security models used by many organizations. Instead of granting any authenticated user full access to an organization's network resources, zero trust provides access on a case-by-case and rigorously vetted basis.

A relevant and responsive zero trust approach can dramatically decrease an organization's exposure to cybersecurity risks, making it an increasingly popular strategy. However, any philosophy is only as strong as its application. Lack of knowledge of how to implement zero trust effectively is a common barrier. Here, our experts provide six steps to implementing a zero trust network (ZTN) access approach to cybersecurity.

STEPS TO ZERO TRUST NETWORKING

Implementing zero trust architecture is often portrayed as a product-focused process. However, choosing the technology to enforce zero trust policies is a relatively minor step toward application. More important are the processes and procedures needed to ensure the rigor, relevance and responsiveness outlined in the following six steps.

Step 1: "Know Thyself"

The first step in implementing zero trust within an organization is gaining an understanding of the core requirements and applying a deep knowledge of your data, users and setup. Examples of important information to have includes:

- **Data Types:** What types of data does the organization have within its possession? Is there proprietary internal information, sensitive customer data, etc.?
- **Data Classifications:** How is data within the organization's ecosystem classified? What are the required security controls for each class of data?
- **Data Locations:** Where is the data located within the organization's ecosystem (on-premises, cloud-based infrastructure, in software as a service solutions)? What types of systems is it stored on? All these factors impact how access controls can be implemented within the network.
- **Users:** What kinds of users are present within your environment? Where are your users located? Are they in physical offices, remote, a mix thereof?
- **Data Access:** What data or resources do your users need to access? What systems need to communicate programmatically within your workflow?
- **Network Architecture**: What are your environment's logical network boundaries? How are your multiple locations interconnected? What mix of cloud resources exist within your network boundary?
- **Infrastructure:** What types of systems exist within the organization's network infrastructure? Does a ZTN solution need to manage access to only traditional compute devices and resources or are Internet of Things (IoT) devices or industrial control systems (ICS) present as well?
- **Regulatory Requirements:** Different types of data are protected by regulations, and these regulations define certain requirements for collecting, storing, processing, and accessing this data. Any ZTN solution should be capable of meeting the requirements of applicable regulations.

These questions define the problem that a zero trust solution attempts to solve. Once you have the answers, you can develop policies and procedures to ensure compliance with internal security policies and regulatory requirements.

Step 2: Define Identity Management Processes

Strong identity management lies at the core of zero trust security. To only grant access to resources and data to authorized users, it is vital to strongly authenticate a user making a request and to know their level of authorization.

Achieving this requires more than just a robust authentication process: When defining a zero trust strategy, it is also necessary to interlace it within the organization's Identity Lifecycle. If you don't have a well-governed Identity Lifecycle enabled within your organization, start by creating the following processes:

- **Onboarding:** Users are granted initial access to the system and assigned the roles that define their access. An onboarding process should include guidance on how to appropriately assign roles to a user based upon their duties within an organization.
- **Maintenance:** Over time, employees can change roles within an organization, hand off some duties, and acquire others. A zero trust strategy should have processes in place that are used when these changes occur and during regular reviews to ensure that every user has exactly the access required by their roles and duties.
- **Offboarding:** When an employee leaves the organization, processes must be in place to terminate their access to the organization's resources. These should be clearly defined and regularly reviewed to eliminate the chance that an oversight grants unauthorized access to any potentially disgruntled former employees.

Done properly, these processes should ensure that a user only has the access and permissions they require to do their job. This is a core tenet of zero trust and is essential to minimizing an organization's cyber risk and the potential impact of a security incident.

Step 3: Identify Use Cases

Zero trust networking is based upon the concept of roles. By defining responsibilities and associating access and permission with these roles, it is possible to scalably and effectively assign rights to employees across the organization.

To determine the rights needed by employees, it is helpful to develop specific use cases. A common starting point (especially in the time of COVID-19) is remote access. Flesh out a use case by determining exactly what functionality and data a remote user needs and to access. This lays the groundwork for defining permissions and roles in the zero trust system.

Step 4: Select and Implement a Zero Trust Platform

Often, implementing zero trust is seen as a product-driven endeavor. To effectively use zero trust, organizations believe that they need to rip out a great deal of their network infrastructure and install a next-generation firewall (NGFW) capable of enforcing zero trust policies.

While this is one possible approach and may be the right choice for some organizations, it is not the only option available.

Organizations can instead take a software-based approach to implementing zero trust. With this approach, software agents are deployed to endpoints and have inline control over the device's traffic. This enables them to enforce on-device zero trust policies, making it impossible for a user to access resources without authorization. A software-driven approach also greatly simplifies consistent application of entitlements across a user's various devices and locations.

Step 5: Create Entitlements

Building on use cases, you're ready to create identity and access management entitlements. To clarify, use cases describe how a user will use the network and the types of access that they will need, entitlements designate how use cases are implemented within a zero trust solution.

Also known as "authorizations", "privileges", "access rights", "permissions" or "rules", entitlements define the allowances and access controls to implement in the zero trust platform and assign to users via their roles.

Remember, any time provisioning is considered, de-provisioning must also be considered. Be sure to include policies and procedures to accommodate terminations, transfers and lateral movement of employees.

Step 6: Roll Out

Once a use case and its entitlements have been implemented within the zero trust system, it is time to roll out the system to users by deployment of technology, testing, onboarding users, and providing training.

This stage of the process is best started using a small pilot group. This makes it easier to solicit feedback, gather metrics, correct errors, and improve the process without having a significant impact on business operations. Once any issues have been overcome, the solution can be more broadly deployed to the rest of the organization.

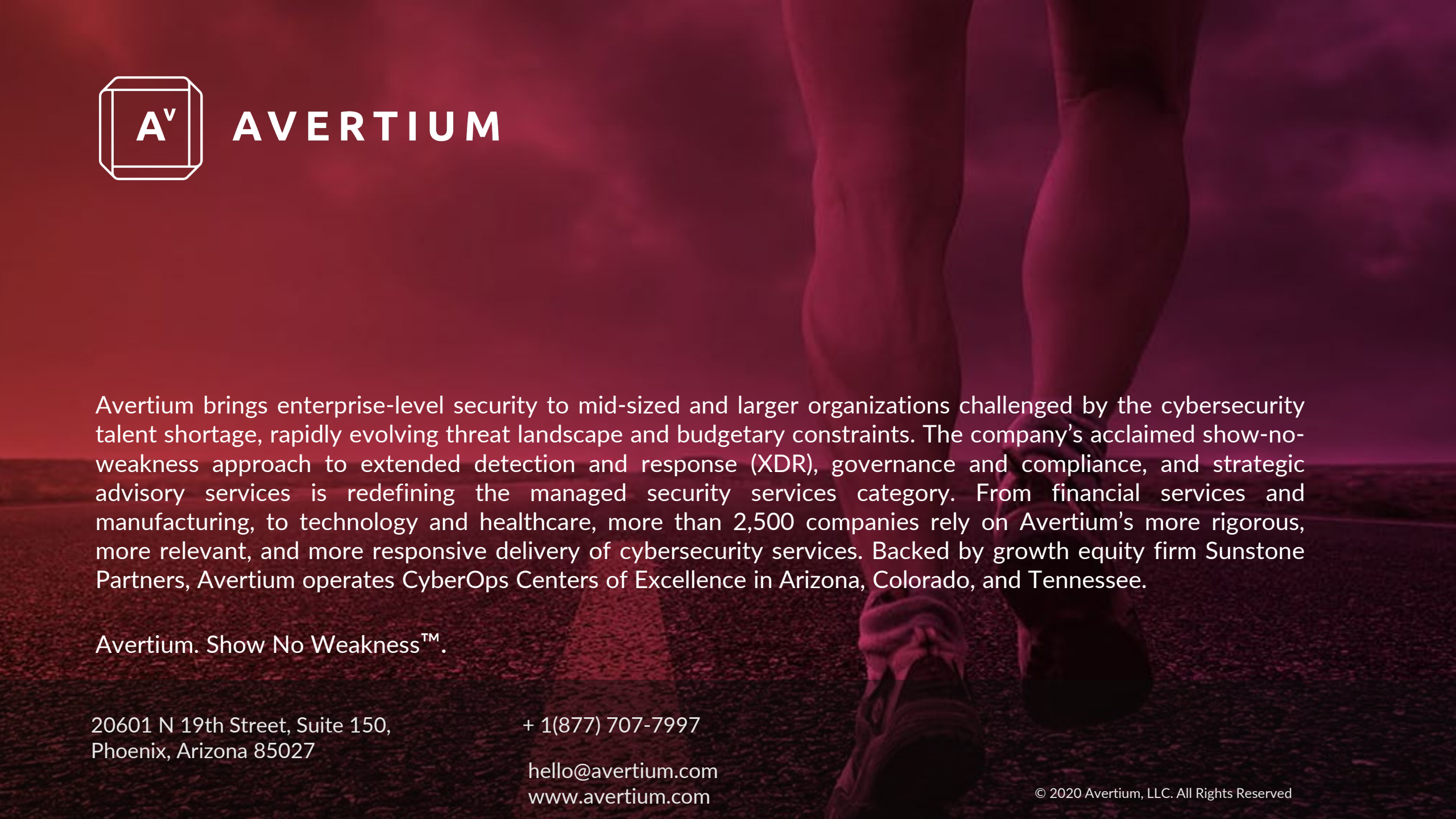
Done well, a fully realized zero trust architecture is nearly transparent to the end user, but periodic reinforcement of the ideology driving zero trust – Need to Know – is important to add to your regular security awareness training.

MAKING THE MOST OF ZERO TRUST

The process for implementing an effective zero trust policy can be summarized within six steps, but rigorous application requires deep knowledge of an organization's operations and cybersecurity expertise.

It's also important to remember that ZTN is an on-going effort and must be maintained. Processes and procedures themselves as well as enforcement must be reviewed and adapted on a regular basis to ensure the rigor initially applied endures.

For organizations interested in implementing zero trust but lacking the resources or expertise, Avertium can help. Our experts are here to guide you through the process of defining, implementing, and enforcing a robust zero trust policy to improve your cybersecurity posture and reduce your vulnerability to cyber threats.



AVERTIUM

Avertium brings enterprise-level security to mid-sized and larger organizations challenged by the cybersecurity talent shortage, rapidly evolving threat landscape and budgetary constraints. The company's acclaimed show-no-weakness approach to extended detection and response (XDR), governance and compliance, and strategic advisory services is redefining the managed security services category. From financial services and manufacturing, to technology and healthcare, more than 2,500 companies rely on Avertium's more rigorous, more relevant, and more responsive delivery of cybersecurity services. Backed by growth equity firm Sunstone Partners, Avertium operates CyberOps Centers of Excellence in Arizona, Colorado, and Tennessee.

Avertium. Show No Weakness™.

20601 N 19th Street, Suite 150,
Phoenix, Arizona 85027

+ 1(877) 707-7997

hello@avertium.com
www.avertium.com