Security
Thought Leadership White Paper

March 2017

Rein in "box sprawl" with an end-to-end Zero Trust approach to security

Deploy strong segmentation and encryption to ensure coherent data protection, enterprise-wide

IBM

Introduction

Cyber attackers are relentless, whether casting a wide net or narrowly targeting your organization. They use multiple methods to compromise your information and infrastructure resources, worming their way into your data and networks wherever they can, with off-the-shelf malware, brute-force password attacks, or phishing and other forms of social engineering.

In the face of these persistent threats, network security—and ultimately, data security—is an ideal to strive for through evolving practices, rather than an outcome to expect from point solutions or any particular security practice in isolation. Attackers go after everything—hacking firewalls, compromising credentials, and discovering both hardware and software vulnerabilities.

In response, the security approach known as "Zero Trust" has emerged to counter the inevitable holes and flaws in conventional security "trust" models by implementing *software-defined* security. And it's changing the way enterprises architect and transform their infrastructures and hybrid cloud environments.

What is Zero Trust?

The thrust of the Zero Trust security approach is to stop trusting applications, users, networking devices or networks by default, and instead implement a regime of continuous verification. Such a system is designed to identify and segregate data streams according to the applications and endpoints involved—a process known as "segmentation." The Zero Trust approach then protects those applications and streams of data from end to end with encryption and intelligent, software-defined security.

That may sound like a radically different approach to security design, but it's really an evolution of established security best practices, reconsidering them as elements of an overall comprehensive approach and secured fabric.

Implementing Zero Trust doesn't mean abandoning your current networking infrastructure, but rather overlaying it as part of a deliberately managed security environment. That means utilizing virtualization, cognitive security monitoring and security information and event management (SIEM) tools to monitor and address intrusion attempts, then coupling those tools with segmented data transmission hardened by strong encryption.

Rather than trusting the intermediate devices that packets traverse, or even trusting by default particular users or endpoints, the Zero Trust approach is to eliminate implicit trust, relying instead on access granted only through strong identity and authorization policies. The goal is to foil intruders who are hoping to take advantage of new vulnerabilities or to cause lateral damage if they can break through a weak point in your environment—and eliminate their ability to traverse east and west within an environment.

To achieve this level of protection, Zero Trust environments virtualize the entire data connection, proactively lock down applications and tightly control who can reach those applications. The Zero Trust approach operates between the edge of your network and the external resources users need to access, as well as within the confines of a networked environment. The technologies that make Zero Trust possible offer fine-grained separation of data connections via micro-segmentation over conventional local area networks (LANs), wide area networks (WANs) via private multi-protocol label switching (MPLS) or commercial broadband connections.

Using the Zero Trust approach, you will choose security policies rooted in business workflow, based on a connection's endpoints and application access—treating each connection differently

based on needs. For example, an enterprise may direct traffic on a virtual private network (VPN) that connects a branch office to headquarters only over a specifically secured link, or it may segregate transactions involving customer data using a dedicated connection.

A typical starting point for the Zero Trust approach is to secure the WAN that bridges endpoints within your organization to those outside it, using a secure software-defined WAN (Secure SD-WAN). Secure SD-WAN service from IBM is designed to harden data connections with end-to-end circuit encryption from premises to cloud using IPSec 256-bit protection.

Securing the WAN through virtualization is one of the most cost-effective ways to get the benefits of Zero Trust, and it is a solid foundation for software-defined security architectures needed in adopting cloud and hybrid cloud environments.

Why Zero Trust?

As data sharing, mobility, user roles and endpoint devices proliferate, security personnel have a lot to keep up with. For example: Specialized security appliances—or servers repurposed as single-tasking security tools—can appear to be an attractive solution that gives overworked network architects and administrators useful building blocks that are easy to plug into a network diagram. But these specialized physical security devices can also lead to "box sprawl," with multiple machines—each assigned to its own task—seeking malware, encrypting traffic, inspecting packets or managing user identity.

That can make for a convoluted flow of data from endpoint to endpoint. More importantly, there are two things they can't do by themselves: provide strongly segmented end-to-end data security, and give deep visibility into data flows across the entire network.

Deep visibility into the network's security posture is important not only for data security, but also for increasingly rigorous compliance demands, flexibility in the face of cloud computing, multi-tenancy, Internet of Things (IoT) devices and business planning.

To achieve a coherent security approach that meets all of these objectives, IBM offers a Zero Trust portfolio that applies to security the principles of virtualization and segmentation that are already simplifying enterprise storage and processing.

How does Zero Trust work?

The intelligence it takes to segment, encrypt and direct connections in a Zero Trust environment is centered in an edge device—hardware that sits at the edge of your network—that hosts software-defined security modules. These software modules, known as virtual network functions (VNFs) are the key to Zero Trust security; each VNF module runs together on a standard platform to perform a particular function, such as firewall protection or encryption. The configuration of these modules is what defines the Zero Trust network itself by identifying, prioritizing and assigning network paths to applications, network destinations and users.

Zero Trust allows you to employ a multi-vendor security ecosystem running on a single edge device at each location from various IBM security partners such as Palo Alto, Fortinet, Checkpoint and others capable of running the VNFs to suit your security application and business priorities..

The Zero Trust approach encompasses six areas of today's enterprise networks: WANs, LANs, cloud services, enterprise data centers, IoT devices (including specialized appliances and environmental sensors), and services such as blockchain for recording the history of transactions. The Zero Trust goal is to create connections that are locked down end-to-end, secured from the user all the way to the application.

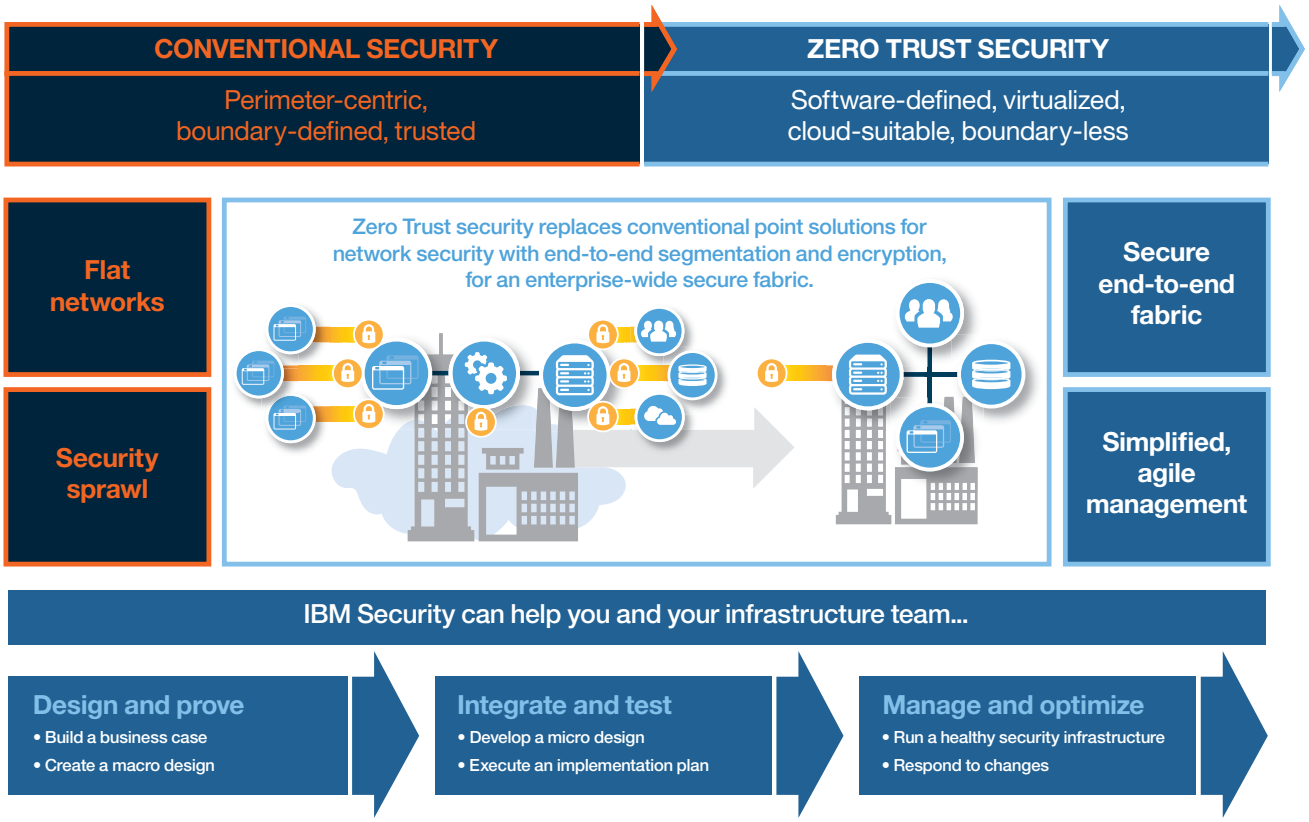

Figure 1. Next-generation architectures and virtualization technologies put the advantages of Zero Trust security in affordable reach for enterprises.

The IBM Zero Trust portfolio

The IBM® Zero Trust portfolio comprises a mix of hardware, software and services that can be tailored to your enterprise, based on your highest-priority data-security needs. Segmentation (at the application, connection or user level) and encryption remain the basic tools of Zero Trust, but the tools in the IBM portfolio also focus on proactive security, by monitoring and reacting to what's happening in the entire data environment.

Once the Zero Trust-ready hardware infrastructure is in place, you can deploy software security solutions in minutes with no changes to routing, firewall, network address translation (NAT), network or applications. No configuration is needed other than defining which applications are to be protected.

Security policies are defined by your enterprise's security administrators, not hard coded or under the control of a third party but through an orchestration process. Because the intelligence of the Zero Trust implementation is based on ongoing verification, no

configuration is necessary for remote hardware or software. Once traffic is directed through the Zero Trust infrastructure, the edge-based VNFs segment and secure applications that are encrypted via automated network tunnels for data in transit.

A range of security tools rounds out the Zero Trust infrastructure to add analytic and other capabilities:

- Authentication via IBM MaaS360® to manage who is allowed to reach the Zero Trust secure applications
- Monitoring and analysis of all traffic by IBM Security tools including IBM QRadar®, IBM Security Guardium® and IBM Watson® for Cyber Security
- Secure, scalable VPN connectivity, interoperable with legacy, existing enterprise networks, to help reduce the attack surface available to an attacker
- Security analytics and a Representational State Transfer (REST) application programming interface (API) to enable anomaly detection via third-party behavior analysis tools
- Security compliance analytics that turn the Zero Trust model into a tool for regulatory compliance
- Automated IPSec tools for verifying network path integrity, even over private circuits

Zero Trust use cases and advantages

Zero Trust can help secure connections to remote data stores, remote compute sessions, IoT devices, ATMs, and mobile employees' computers or mobile devices. In all these cases, the IBM Secure SD-WAN can provide a secure overlay for data protection, while providing IPSec encryption for end-to-end protected data handling.

With virtualization at the heart of Zero Trust, system administrators have fewer boxes to deal with, which means using less rack space, cooling and power, all of which can be costly. Installation is quick, simple and safe, with automated, zero-touch deployment the security edge; deployment for branch offices in minutes; and strong encryption of data transmissions provided by the IPSec protocol. Once installation is complete, administrators also have a simpler set of upgrade and maintenance tasks. All told, replacing disparate tools with a Zero Trust environment can yield significant cost savings.

To enable Zero Trust, start with Secure SD-WAN

With rapid cloud adoption as both a business and IT goal for many organizations, the need to secure the WAN that connects an enterprise to the cloud has become a high priority. The overarching fact is that SSL/TLS data flowing into or out of your enterprise is most exposed (and least under your control) when it is outside the other network-edge security tools you have in place.

One of the most important reasons for employing Secure SD-WAN is simply the fact that more data, from more sources, is flowing over your network, and it needs to be secured. This is happening thanks to the growth of cloud computing and virtualization, as well as the increasing number of IoT devices.

Additionally, because data can be captured and stored outside of your network, it's important that anyone with the ability to eavesdrop on your data be denied access to meaningful information. The end-to-end encryption provided by the Zero Trust approach to security means that an eavesdropper lacks the ability to profit simply by intercepting data flowing into or out of your organization.

You can deploy Secure SD-WAN when and where you need it. This means it can be phased in as an overlay across branches and traffic types, starting with the data that calls out for the most protection, such as sensitive customer information, financial transactions or intellectual property. In addition, IBM provides a security hub with full integration for Secure SD-WAN that provides Network Function Virtualization (NFV) security services at the entrance point for cloud providers that can reduce latency as it increases security for hybrid cloud environments.

Once you secure the WAN to protect the most vulnerable portions of your network, you can use the same principles to secure the software-defined LAN and other parts of your network, for a complete Zero Trust environment that extends from the cloud to the endpoint, secured and encrypted for the entire path.

For more information

To learn more about the IBM Zero Trust portfolio, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

SEW03154-USEN-00