www.pipelinepub.com
Volume 19, Issue 1

Closing the Top Five Cybersecurity Gaps

By: Koroush Saraf - VP Product Management, ZPE Systems

Although cybersecurity is a $155 billion industry with more than 1,800 vendors, companies still struggle to assemble holistic cybersecurity. According to IBM’s 2022 Cost of a Data Breach report, ransomware breaches increased 41 percent in the last year and now cost $4.54 million on average. With many great products available and increasing investment in cybersecurity, why aren’t these attack trends decreasing? Why is it so difficult to protect digital assets? Working with Big Tech, ZPE Systems has developed a reference architecture—a network automation blueprint—as the best practice to cover the security gaps that remain open.

Five cybersecurity gaps to close

Digital services—otherwise known as applications, data, and the platforms that host them—now live across a mix of public-cloud (Azure, AWS, GCP) and private on-prem colo, branch, and edge locations. During the push to adopt the cloud, this hybrid model helped companies meet increasing customer demands to deliver applications quickly and at scale.

This hybrid infrastructure (including edge computing), however, spreads applications, data, and systems that protect them across more locations, creating a large, porous attack surface. Today’s infrastructure presents so many vectors that attackers can use to exploit things like leaked passwords, buggy software, and disjointed solution integrations, among others. Let’s examine the five gaps that organizations must close in order to achieve holistic cybersecurity.

Credential theft

Hybrid infrastructure has caused an explosion of apps and platforms that require authentication. This presents many opportunities for cyber criminals to steal credentials. Research from Digital

Shadows states that in 2021, there were more than 24 billion credential pairings available for sale on the dark web.

zpe
Network Automation Blueprint
Download the sneak peak of our
Network Automation Blueprint
DOWNLOAD

Even with multi-factor authentication, credential theft or bypass still happens when systems go unpatched. Recall the SQL injection or the Active Directory attacks, where hackers were able to bypass authentication altogether and pivot to other systems. Preventing credential theft requires diligence on the part of the organization, with programs to educate employees about vulnerabilities, performing regular pen testing, and continuously patching all network infrastructure.

Unpatched infrastructure

In 2021, there were 28,000 vulnerabilities and exposures (CVE) reported and cataloged at the government-sponsored website for Common Vulnerabilities and Exposures. Many of these common vulnerabilities can be exploited for successful cyberattacks. For this reason, an application and infrastructure patch management strategy is the cornerstone of protection; however, teams are reluctant to update systems, and for good reason. What if the software upgrade includes an undiscovered vulnerability that blows open an attack vector in an otherwise-protected system? Imagine executing the Friday-night upgrade using the latest software, only to have a bug or CVE bring down the network and force the weekend shift to restore services.

The fact is that system upgrades always come with the risk of reducing the security posture of the whole infrastructure. I worked at Fortinet for 10 years and it is a fantastic company, but this Fortinet CVE is a perfect example of why teams need a solution to quickly deploy updates and fixes without having to worry about breaking their networks. Customers upgrading from a more secure FortiOS 6.2 to 7.0 found themselves suddenly vulnerable. In this very typical scenario, the only solution is to be able to upgrade or downgrade at any given time. But teams need to ask, “What is the proven best practice for upgrading or downgrading without breaking things?”

Inability to deploy the right security tools

With the hybrid infrastructure model, the public cloud portion is the easiest part to secure because there are well-known use cases and associated security tools for Big Tech cloud platforms including AWS, Azure, and GCP. For example, most cloud security products can be turned on from their respective app store; from there, they assess virtual public cloud instances, toggle the appropriate switches, and insert themselves into the traffic path.

However, imagine you want to manage your on-prem infrastructure, such as in a hospital or manufacturing plant, in the same way. Consider the digital services stack of:

1. Connectivity: MPLS/DIA/LTE CPE ISP WAN devices, HA Pair of WAN routers, NGFWs, SD-WAN devices, Wireless APs, PoE Switches
2. Out-of-band infrastructure: Serial consoles, UPS systems, smart PDUs, and machines to run observability agents, network taps, and jump boxes
3. IT equipment: PCs and servers (for example, an ESXi server to host local applications)
4. IoT/OT devices: Digital signage, smart speakers, sensors, security cameras, building automation systems, printers, PCs, smart conference rooms, and VoIP systems
5. IoMD devices: Pill dispensers, imaging equipment, robots, and safety sensors

In Figure 1, you can see only a fraction of available security players and products required for a defense-in-depth strategy.

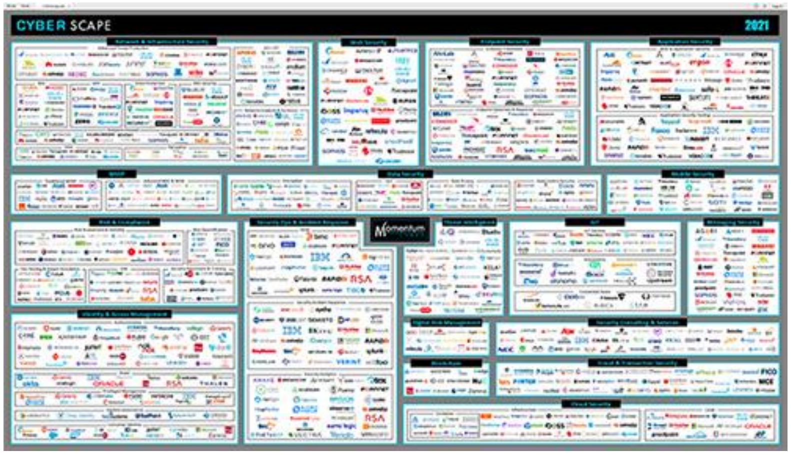

Figure 1: Too many cybersecurity products from too many vendors.
Courtesy of: The Momentum Cyberscape 2021
(*Click to Enlarge*)

The challenge for IT is figuring out how to deploy a mix of products that work best for them, and that also provide cybersecurity coverage for different locations across the infrastructure. The common approach is to use the one or two solutions that are easiest to deploy. In addition, some organizations address the remaining gaps by purchasing costly cyber insurance.

Organizations need to be able to bring together the solutions that are best suited to defend their on-prem infrastructure. These include third-party applications and solutions of their choice.

Unnecessary exposure of management portals

During the pandemic, IT teams needed remote access to equipment. This caused many to expose management ports—even of remote desktops—directly to the Internet. Adversaries were able to find this equipment and attack using the exploits described earlier (stealing credentials, breaking through unpatched systems). Had teams deployed private out-of-band infrastructure, these systems would have remained protected while still allowing them remote access.

Human error

There are two categories of human error: slips or lapses, which are small mistakes (as in typos and configuration errors) that occur when performing familiar tasks or activities, and decisions (like delaying updates or patches), which occur from a lack of gathering and processing information necessary to make the right decision. The Global Risks Report released by the World Economic Forum, as well as IBM's Cyber Security Intelligence Index in June 2022, both revealed that 95 percent of cybersecurity threats organizations have faced have been caused by human error. Similarly, Verizon's 2022 Data Breaches Investigations Report shows a survey result of 82 percent caused by human error.

From a cybersecurity standpoint, these can cause security breaches to occur and spread. The key to solving human error is to reduce the need for humans to intervene and thus the risk of introducing mistakes. For large tech organizations, this means completely removing the human element because of the need to scale to and operate thousands of nodes. To do so requires capturing the decision matrix and using automation to address both categories of error and minimize the risk that humans introduce.

Seamless cybersecurity: hyperautomation, open cybersecurity platform, and out-of-band

The problems above have a common thread: they lack a seamless way to automatically deploy the right combination of different products at various locations. To address this gap, tech giants have taken a three-pronged approach that includes hyperautomation, an open cybersecurity platform, and out-of-band infrastructure.

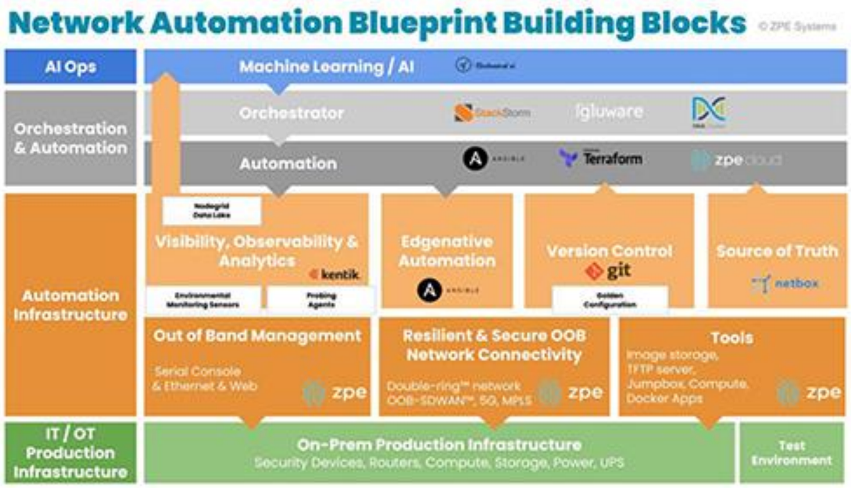
Network Automation Blueprint Building Blocks
© ZPE Systems
AI Ops
Machine Learning / AI
Orchestration & Automation
Orchestrator
StackStorm
itgluware
Automation
ANSIBLE
Terraform
zpe cloud
Automation Infrastructure
Nodegrid Data Lake
Visibility, Observability & Analytics
kentik
Environmental Monitoring Sensors
Probing Agents
Edgenative Automation
ANSIBLE
Version Control
git
Golden Configuration
Source of Truth
netbox
Out of Band Management
Serial Console & Ethernet & Web
zpe
Resilient & Secure OOB Network Connectivity
Double-ring™ network OOB-SDWAN™, 5G, MPLS
zpe
Tools
Image storage, TFTP server, Jumpbox, Compute, Docker Apps
zpe
IT / OT Production Infrastructure
On-Prem Production Infrastructure
Security Devices, Routers, Compute, Storage, Power, UPS
Test Environment

Figure 2: Network Automation Blueprint Building Blocks
(Click to Enlarge)

Hyperautomation is important because it enables many IT and business workflows to be automated, using orchestration technologies that greatly reduce manual workloads and the risks of human intervention. An open cybersecurity platform is critical for hosting an organization's choice of physical and virtual solutions, allowing agile operations and reducing the need for many physical devices in the stack. Private out-of-band management infrastructure is the final key piece to safely managing and recovering systems—and allowing IT teams to gain manual control of their automation pipeline when necessary.

However, implementing these concepts comes with a high degree of ambiguity, given there is no correct reference design available. This has led to the development of a validated reference design called the network automation blueprint, which is a key enabler for organizations that wish to achieve holistic cybersecurity.

Cybersecurity with the network automation blueprint

The network automation blueprint is made up of four major building blocks (see Figure 2 above). These create a management network design pattern to accommodate Gartner's definition of hyperautomation and allow organizations to stitch together a seamless fabric of various cybersecurity solutions. The blueprint's building blocks are:

IT/OT production infrastructure: This includes discrete servers, switches, routers, NGFWs, and common production equipment. To prevent device proliferation, it's recommended to use the open cybersecurity platform approach. This platform enables a single piece of hardware to host multiple security and network functions (NGFWs, SD-WAN, user experience monitoring), which can be automated in a zero-touch fashion from a centralized cloud orchestrator.

Automation infrastructure: This layer is key to reducing anxiety around automation. This is a truly independent infrastructure that is connected to the production infrastructure in an out-of-band fashion. Customers call this the double-ring network (see Figure 3 below). This layer often uses a combination of serial console and Ethernet connections, along with staging jump boxes, local storage, TFTP source of truth, and version control systems. This layer is critical to automating diverse security products to work together, as it provides a safety net for teams to roll back to golden configurations in case of mistakes. In simple words, this automation infrastructure layer is able to destroy and rebuild the production network safely, so teams don't have to worry about breaking any systems. It's similar to having an IT person troubleshoot a locked-up device by typing commands in the console port to rebuild the device, but without any human interaction.

Orchestration and automation systems: This is where the desired outcome and playbooks are sourced from. The key is that the orchestration reaches the production systems through the independent out-of-band network to achieve the desired outcome.

AI Ops infrastructure: This layer receives rich information from observability platforms to make reactive and predictive decisions at scale. Using machine learning and artificial intelligence, this layer learns the network's normal behaviors and pushes changes through the orchestration and automation layer.

This blueprint is the reference architecture validated to successfully implement hyperautomation, as well as meet the Open Networking User Group (ONUG) Orchestration and Automation recommendations. This blueprint gives you the necessary layers to confidently implement a holistic cybersecurity approach and outlines the practical steps required to overcome the gaps described above.

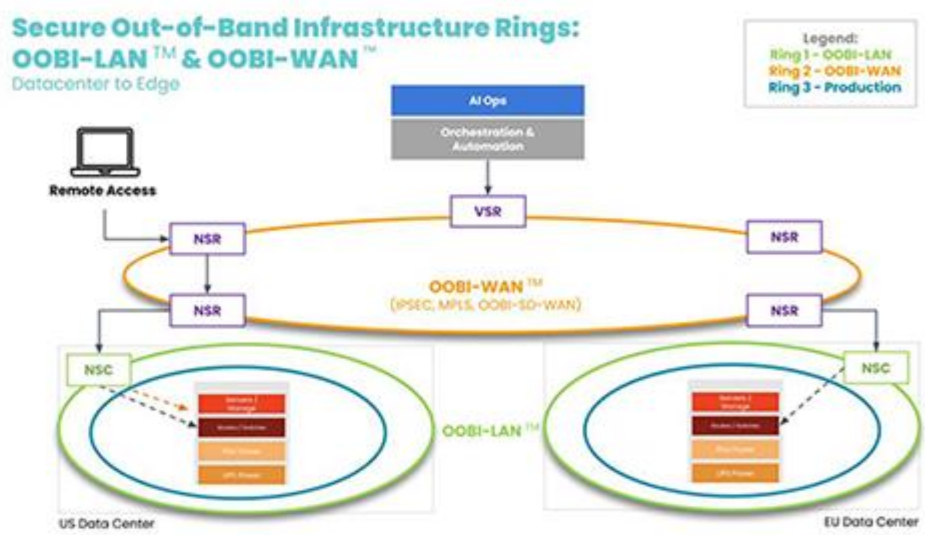

Figure 3: Dedicated automation network best practice known as double-ring architecture
click to enlarge

Fight ransomware with the network automation blueprint, open cybersecurity platform, and OOBI-WAN™

A single-vendor cybersecurity strategy is no longer adequate to combat increasing cyber threats and ransomware. Organizations must reduce the attack surface and close gaps using a diverse fabric of security solutions. This requires an automation infrastructure to remove the anxiety from pushing upgrades and patches. A vendor-neutral, open cybersecurity platform also allows the best picks of security products to be positioned where needed. When automation infrastructure is independent of production infrastructure (out-of-band), IT teams can safely recover from errors, much like having a network-wide 'undo' button. This unique combination of automation infrastructure, open cybersecurity platform, and secure out-of-band enables teams to:

- Quickly patch infrastructure without fear of causing breakages and unscheduled downtime, using CI/CD pipelines to rebuild production at any time regardless of human resources (see this auto-upgrade/downgrade example of Fortinet firewalls here)

- Simplify the deployment of the necessary, multi-vendor security stack from datacenter to edge, by easily deploying vulnerability scanning from Vendor A, NGFWs from Vendor B, and experience monitoring from Vendor C

- Protect management portals and reduce the attack surface, by restricting interfaces and remote desktops to a private and secure out-of-band infrastructure (OOBI-WAN™) network

The network automation blueprint helps organizations close these gaps and achieve holistic cybersecurity, by explaining these techniques in detail. Download the complete blueprint from ZPE Systems.