A CISO's PLAYBOOK

How to Conquer THE TOP 4 Network Security Challenges with Universal ZTNA

appgate

EXECUTIVE SUMMARY

Advanced digital landscapes and morphing cyberthreats present unprecedented challenges for CISOs and their teams. As security objectives often clash with business goals, the constant pressure to hit an "easy button" versus finding the right balance can be a Herculean task.

Undoubtedly, CISOs have been thrust into strategic business leadership, entrusted with safeguarding intricate hybrid networks and core resources without hampering innovation and digital transformation. This shift is happening because that mitigating risk is no longer just about securing data and systems but is about protecting an organization's brand, financial stability and market position.

With many business aspects out of a CISO's control, influence is key. It is critical to forge relationships with key stakeholders to incorporate cybersecurity plans into the business story. As a CISO, consider these questions: What is known? What do you want to know? What don't you understand? Minimizing risks and gaps with security strategies that enable business agility is essential to build trust and effect impactful change.

CISOs know there are no quick fixes to balancing security objectives with enterprise aspirations. So, if it's never going to be easy, can it at least be easier?

Many CISOs are answering that question in the affirmative with a Zero Trust security framework, using Universal Zero Trust Network Access (ZTNA) as a cornerstone. This approach eliminates overprivileged user access, minimizes attack surfaces, cloaks networks and prioritizes end-to-end monitoring and visibility across hybrid environments. And the right ZTNA solution can yield significant operational benefits and OpEx savings. After all, mastering cyber complexity while enabling the business and contributing to the bottom line are the new hallmarks of CISO success in today's digital world.

TABLE OF CONTENTS

THE CISO AS A BUSINESS ENABLER: *AUTHORITY, OWNERSHIP AND ACCOUNTABILITY*

In recent years, the role of a CISO has evolved from a cost center manager to a strategic partner instrumental in driving business growth. This shift underscores the fact that cybersecurity is not merely a defensive measure, but a critical enabler of innovation, agility and competitive advantage.

However, CISOs often still face budget and authority constraints, which is why building trust and influence with C-suite peers and their Boards is important. Knowing how to balance operational needs, innovation, time constraints and other business priorities are powerful negotiation tactics.

The authority of a CISO varies by organization. Typically, a CISO can evaluate and accept cybersecurity risks up to a certain threshold, set and enforce security policies, allocate resources and align the cybersecurity budget with priorities. They lead risk assessments, frame threat mitigation strategies and establish security expectations and training for employees. And CISOs are tasked with identifying and addressing gaps to prevent security incidents. In the event of a breach, they lead incident response and recovery efforts, building resilience.

As a CISO's influence and authority grows, so does accountability to the business. This requires understanding IT and cybersecurity markets, regulatory landscapes and competitive pressures. CISOs must establish key performance indicators to measure security effectiveness and business impact. And it's also important to be able to communicate the ROI of cybersecurity investments, highlighting how they support business enablement and can reduce operational expenses.

Aligning cyber initiatives with broader business goals is critical. CISOs must transcend risk mitigation and actively contribute to strategic objectives by understanding the needs of the business and harnessing security strategies that drive overall success and minimize impact should a breach occur.

Universal ZTNA emerges as a powerful framework for managing risk, reducing complexity, addressing compliance and proving ROI to the business. By adopting a Zero Trust approach, CISOs eliminate implicit trust, ensuring continuous authentication and authorization for every user, device and application across their organization. This granular control significantly reduces the risk of unauthorized access and lateral movement, thereby enhancing the overall security posture for both enterprises and federal agencies.

And a best-of-breed Universal ZTNA can minimize costly rip-and-replace scenarios with API-rich functionality that consolidates an alphabet soup of disparate solutions like IAM, AV, SIEM, SOAR, EDR, XDR, SWG, CASB, DLP and more into a unified platform. This streamlined approach reduces complexity, improves visibility and enables more effective threat identification and response. Additionally, ZTNA's granular access controls and detailed audit trails help organizations meet stringent compliance requirements.

CISOS MUST ESTABLISH KEY INDICATORS TO MEASURE SECURITY EFFECTIVENESS AND BUSINESS IMPACT

THE TOP FOUR *NETWORK SECURITY CHALLENGES*

#1 THE CHALLENGE OF COMPLEXITY

Modern networks are sprawling ecosystems with resources scattered from the cloud to the edge and everywhere in between. This complexity presents a significant challenge for CISOs and security teams, creating blind spots and vulnerabilities across intricate network topologies. Endpoint proliferation, cloud adoption and the need to integrate lagging legacy have expanded attack surfaces, making it increasingly difficult to harden security postures. And changes such as reorganizations, employee turnover, mergers acquisitions, and digital transformation initiatives all add to that complexity.

#2 THE CHALLENGE OF INSECURE VPNs

Traditional security solutions like internet-facing VPNs are a popular threat actor target due to insecure open ports. So, what happens when security appliances ARE the attack vector? Cybersecurity 101: CISOs must make sure they are not the path for exploitation.

Publicly disclosed CVEs and VPN zero-day exploits often lead cyber industry headlines, most recently driven by months-long reporting on multiple Ivanti security flaws. These CVEs serve as a stark reminder of VPN weaknesses and the dangers of exposed infrastructure.

But the answer isn't to wait for an exploit to be discovered so a VPN vendor can issue a patch. Persistent VPN exploits are a clarion call that highlights a trend … advanced persistent threat tactics used by adversaries have shifted from targeting endpoints to targeting exposed infrastructure. CISOs need a sense of urgency when it comes to protecting their enterprise house because most organizations will never be as fast as the adversary, especially state-sponsored efforts that employ vast resources.

#3 THE CHALLENGE OF SECURING LEGACY SYSTEMS

Tech innovations are made in response to demand, whether from customers, regulation, employees, partners or competition. Back-office functions, network infrastructure, databases and other capabilities that are less dynamic or aren't user-facing, tend to lag in modernization until it becomes an imperative.

Security gaps created by the legacy system tech debt is an ongoing concern for CISOs. Network devices are particularly attractive targets because they are the path into infrastructure and all the crown jewels. These easily exploitable internet-facing resources keep security teams busy with the burden of remediating, patching and updating. Not to mention that each patch and update requires extensive testing to make sure systems continue to work properly

#4 THE CHALLENGE OF SHIFTING ATTACK TACTICS TOWARD EXPOSED INFRASTRUCTURE COMPONENTS

Undoubtedly a CISO priority is to stay ahead of cyberattack trends and quickly identify possible defense vulnerabilities. A quick scan of cyber news shows hackers are shifting from targeting endpoints to exposed infrastructure components. This shift is driven by several factors:

Expanding attack surfaces: Internet-facing infrastructure components present a vast, rapidly growing attack surface because organizations don't always retire or update old tech before adding new. And adoption of leased capabilities (e.g.,SaaS) also changes the attack surface and takes it out of an organization's control.

Exposed vulnerabilities: Each Patch Tuesday, each major update, every CISA advisory adds to a CISO's "to do" list. Patching servers and other non-end user devices often lags because it's hard and time-consuming. This leaves an organization's critical back-end business systems attractive, susceptible targets.

Efficiency and cost-effectiveness: Adversaries target infrastructure because it's a faster, easier way in than phishing. All the vulnerabilities in internet-facing systems make an easy path to follow, and attackers can efficiently and cost-effectively bypass user and email defenses to move straight to data compromise.

A UNIVERSAL ZTNA CASE STUDY: *PROTECTING LEGACY NETWORK DEVICES*

Universal ZTNA changes the network security focus from static perimeters to "segments of one" to protect each user-to-resource and resource-to-resource connection. This takes the issue of protecting access to legacy network devices off the table. Case in point?

One of Appgate's Fortune 50 customers uses Appgate SDP to cloak 99% of its 18,000-plus servers equaling roughly 1.2 billion ports. The remaining <1% are aggressively defended with instant alerts to port status changes via a protocol that ensures shifts aren't lost in the noise.

Appgate SDP also is used to block approximately 202 million SMB ports and control access to file servers, printers and systems with no reported user disruptions. These SMB ports are invisible, eliminating a threat actor's ability to seek out attractive network targets. And, over the course of a year, this global behemoth used Appgate SDP to block traffic to high-risk ports ~75 million times. This kind of service denial is core to keeping an organization safe from unknown sources and malicious actors seeking to steal data and infect the network.

CONQUERING THE CHALLENGES WITH UNIVERSAL ZTNA

Let's face it, securing access to a diverse network environment can feel like walking a tightrope for most CISOs. Cloud deployments, legacy systems, data center and on-premises infrastructure must co-exist. Attack surfaces and blind spots multiply. Disparate secure access solutions make policy management a logistical nightmare. And workforces located anywhere that need access to enterprise resources housed everywhere introduce more network security complexity.

CISOs wrestling with securing diverse environments are increasingly turning to Zero Trust Network Access (ZTNA) for its proven ability to strengthen security posture and adapt to evolving IT landscapes. But not all ZTNA solutions are created equal. And hybrid IT complexities mean CISOs must be discerning when choosing best-of-breed ZTNA that can handle current and future network security needs. When comparing ZTNA solutions, consider the following:

- Can it effectively handle more than remote access connections? The majority of ZTNA solutions are cloud-routed and primarily designed for remote access. Not only do they struggle to integrate with legacy systems and protect on-premises infrastructure they force your traffic through a vendor multi-tenant cloud which adds latency, throughput and scale limitations.
- Does it offer seamless integration and interoperability? It is important to ensure the ZTNA solution that you choose can effectively connect with other security and business tools to avoid creating silos.
- Does it provide comprehensive visibility? Can it deliver provide complete insights into diverse user and device activity, including logging and access information.
- Can it scale and adapt to meet your future needs? It must have strong adaptability and scalability to support overall growth plans and integration with emerging technologies.

THE UNIVERSAL ZTNA ADVANTAGE

Universal Zero Trust Network Access is a paradigm shift in secure access management. With a comprehensive policy framework, organizations can ensure rigorous, consistent application of Zero Trust principles for all users, irrespective of device or location (on-premises or remote). A streamlined approach replaces traditional tech like VPNs, MPLS, and NAC, simplifying secure access management across intricate network topologies. And a Universal ZTNA solution helps CISOs strike a healthy balance between robust network security, user experience and business goals. As a result, security dramatically improves, end users enjoy seamless access, and the business profits from enhanced efficiency and reduced operational and capital costs.

THE DXC TECHNOLOGY STORY

Formed through M&As, Fortune 500 DXC Technology faced a common challenge: a complex array of VPNs, needless overhead, operating obstacles and security gaps. To overcome issues and align to Zero Trust security principles, ***in just 120 days DXC deployed Appgate SDP Universal ZTNA*** *to create a unified platform to protect its vast, converged infrastructure and 130,000-plus users.*

Besides significant reduction in hands-on management time for staff and an improved user experience, DXC cut MPLS connections from over 600 sites to create a café-style Wi-Fi network that capitalizes on Appgate SDP's direct-routed architecture and multi-tunneling functionality. This slashed connectivity costs by 67%, translating to millions of dollars in annual savings. And Appgate SDP addressed DXC's overlapping IP spaces—a frequent hurdle in post-M&A integrations and divestitures.

THE BENEFITS OF UNIVERSAL ZTNA BUILT ON DIRECT-ROUTED ARCHITECTURE

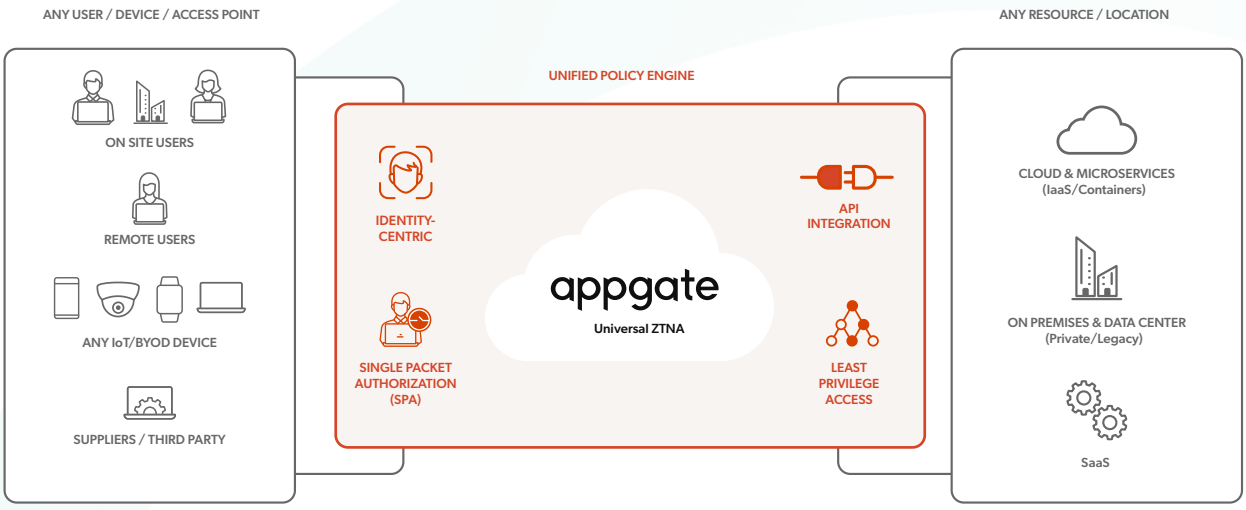
Appgate SDP offers a robust security solution for organizations navigating the complexities of modern IT ecosystems. It is one of the only direct-routed ZTNA solutions on the market. This puts CISOs in control of how data traverses the network and avoids the pitfalls of cloud-routed ZTNA solutions that rely on the implicit trust of multi-tenant clouds. Appgate SDP delivers optimal performance with minimal latency and centralized access controls for all user-to-resource and resource-to-resource connections. This adds the flexibility and control needed to secure diverse environments, encompassing remote and on-premises locations, multi-cloud deployments and legacy infrastructure.

UNIVERSAL ZTNA USE CASES

- Full VPN replacement
- Third-party access
- Transitioning traffic off MPLS to the internet
- Eliminating software-defined wide area network (SD-WAN)
- Network access control (NAC) replacement
- Branch connectivity to corporate resources
- Secure access to legacy infrastructure

To enforce granular, context-aware control, Appgate SDP leverages multi-layered authorization that includes:

- **Single packet authorization (SPA):** This layer cloaks the infrastructure and ensures complete invisibility with no exposed ports, enabling communication channel access only to users that are cryptographically validated with a single packet.
- **Multi-factor authentication (MFA) at sign-in:** Registering a user's device serves as a second authentication factor, enhancing security by blocking unauthorized access attempts with stolen credentials.
- **Authentication:** This layer validates user and device credentials against defined trusted sources such as SAML and OIDC.
- **Authorization:** Policy assignment criteria evaluates user/device attributes, enabling a specific set of entitlements to be assigned to each user/device.
- **Access controls:** This layer compares user traffic to entitlements, enforces access policy, verifies conditions for access and prompts user for action (e.g., MFA) when required. Appgate SDP dynamically manages the access for each user/device based on the host, port and protocol of the protected resource defined in entitlements.
- **Alert actions:** This layer acts as a triggering system that blocks and logs with an alert for high-risk behaviors, such as unauthorized port scans, to proactively address potential threats.



Appgate SDP delivers a unified policy engine to support universal ZTNA for all users, resources including legacy and custom apps, and locations across hybrid IT, multi-cloud, HQ, branch offices and data centers.

SECURING THE FUTURE: WHY CISOS NEED UNIVERSAL ZTNA

Organizations are increasingly managing heterogeneous IT environments, encompassing cloud-based applications, on-premises infrastructure and legacy systems. By their inherent design, these diverse systems will continue to present vulnerabilities that cyber adversaries can exploit. The evolving threat landscape necessitates a sea change in secure access control strategies and Universal ZTNA has emerged as the most compelling solution to mitigate these risks by enforcing granular access controls and eliminating the concept of implicit trust.

Notably, Gartner predicts that through 2026 more than 50% all cyberattacks will be aimed at areas that Zero Trust controls don't cover and can't mitigate. A security approach that extends Universal ZTNA controls across all users and devices, regardless of location, is required to thwart many of these attacks.

ADDITIONAL CISO RESOURCES

Whitepaper: A Return on Investment Analysis of Universal Zero Trust Network Access

Guide: Cloud-Routed vs. Direct-Routed ZTNA: What's the Difference?

eBook: Zero Trust Maturity Model Roadmap

Appgate SDP Universal ZTNA offers a powerful solution for CISOs seeking to secure their organization's expanding digital footprint. Benefits include:

- **Unified access for all users and devices:** Eliminate the friction of managing multiple solutions; achieve consistent and uniform access controls for all users and devices.
- **Adaptive and scalable security:** Dynamically adapt access policies to accommodate diverse users and devices, ensure suitability for a wide range of use cases and security requirements.
- **Increased productivity:** Reduce trouble tickets and expedite access to resources for authorized users for a more agile, productive environment.
- **Simplified compliance:** Apply consistent access controls to reduce the reporting scope and ensure compliance with industry regulations.
- **Cost efficiency and return on investment (ROI):** Enhance operational efficiency and achieve a significant ROI by consolidating multiple access control tools. By consolidating access control and eliminating the need for disparate legacy security solutions, Universal ZTNA empowers organizations to achieve a secure and simplified access environment, optimizing security posture, user experience and operational costs.

appgate

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.

SDP – 1693