WHITE PAPER

Securing Digital Innovation Demands Zero-trust Access

CIOs Face New Cyber Risks as the Attack Surface Expands

Executive Summary

To accelerate business and remain competitive, CIOs are rapidly adopting digital innovation initiatives within their organizations. Business applications and data are dispersed far and wide away from the corporate premises, so now workers have access to more corporate assets from many locations. Because of these changes, the traditional network perimeter is dissolving, which increases the attack surface. In response to these threats, organizations need to take a "trust no one, trust nothing" approach to security. Specifically, CIOs need to protect the network with a zero-trust network access policy that supports "work from anywhere." All users, all devices, and every web application from the cloud must be trusted and authenticated, and only given the right amount of access. Network and security support needs to be provided no matter where users, devices, applications, or resources may be located.

70% of breaches were caused by outsiders, 45% involved hacking, 86% were financially motivated, 17% involved some form of malware, and 22% featured phishing or social engineering.[1]

The Evolution of the Network Edge

For CIOs, digital innovation initiatives are critical for business growth. One aspect of this growth is the proliferation of new network edges, which include private and public cloud infrastructures, Internet of Things (IoT) and mobile devices, and software-defined (SD) branches. All of these edges generate an exponentially growing volume of data, applications, and workflows. To manage user access and interconnect an array of devices from different locations both on and off the network, organizations are increasing the number of devices deployed at the edges of these networks. And in today's work-from-anywhere world, CISOs need to find ways to give users secure access to the network and applications so they can do their jobs without compromising security. But strengthening security also can't result in slowing down users and processes to a crawl.

Because of the explosion of network edges, the traditional network perimeter is dissolving, which creates an open environment that is ripe for attack. Cyber threats are growing more prolific and continuously adapting. In the past, perimeter security was based on a "trust but verify" approach. But with so many users, devices, and applications on the network, it is hard to know which ones to trust.

Exploits like credential theft and malware enable bad actors to gain access to legitimate accounts. And once in, they easily identify ways to maneuver laterally, spreading very quickly to take advantage of the flat and trusted internal network. Once they gain access to an edge device, infiltrators can launch attacks that can cause operational downtime, data theft, financial loss, and reputational damage.

For CIOs and security leaders, it is incredibly difficult to keep up with the growing number of attacks. These changes have led to a philosophical shift from trusting everything on the network to not trusting anything, or *zero trust*. The zero-trust model moves security away from implied trust that is based on network location. Instead, it focuses on evaluating trust on a per-transaction basis. Zero-trust access (ZTA) operates on the assumption that threats both outside and inside the network are an ever-present reality and that potentially every user and device has already been compromised. It also treats every attempt to access the network or an application as a threat. Supporting rigorous, trustless security measures with ZTA requires:

- Ongoing verification of users and devices
- Segmentation of the network to create small zones of control, which helps limit the impact of a breach and establishes more control points
- Least access privilege for users and devices, so only the access they need to perform their role is granted, which helps to limit the impact of a compromised identity or device

ZTA focuses on specific vulnerable areas of the network edge that can be considered untrustworthy: users, devices, and assets both on and off the network.

Knowing Who Is Connected to the Network

Security leaders need to know who is on the network at all times. However, organizations are at an increased risk when it comes to workers that use weak passwords to connect to the network. Because so many accounts now require credentials, many passwords are overly simplistic and easy to compromise through exploits like phishing attacks. It's critical for organizations to know every user and what role they play in the company. Only with that knowledge can they securely grant access to those resources necessary for each role or job, while providing additional access to others on a case-by-case basis.

Another challenge facing organizations is the geographically dispersed workforce, where employees perform their jobs from various locations—such as the headquarters, branch campuses, and even home offices. To respond to shifts in how employees work and the ongoing shift to the cloud, organizations need a new way to securely connect employees to applications. Solutions need to reflect the fact that both the employees and the applications could be located anywhere.

The average time to identify and contain a data breach is 280 days; 207 days to identify the breach and 73 days to contain it.[2]

With so many users gaining access to the network remotely, there are many more opportunities for the attack surface to grow. For example, workers often connect using hotspots or public Wi-Fi networks in coffee shops, airports, automobiles, or on public transportation. This kind of connectivity poses significant security risks. Third parties can eavesdrop on all information that passes between the user and the corporate network. Attackers can exploit unpatched software vulnerabilities to inject malware into the endpoint device, to not only access local information but also gain access to the corporate network via the endpoint device.

Zero-trust access is critical because today's networks are dynamic; devices are constantly going on and off the network. Security leaders need to know which users are on the network and that they have the right level of access. As roles change, such as an employee move from sales to operations, that user might not need access to the same areas that were required for their previous role.

Knowing What Is Connected to the Network

In addition to knowing who is on the network, CIOs and security leaders need to know what devices are on the network at all times. The proliferation of mobile devices and IoT products have dissolved the traditional network perimeter into many microperimeters, which results in a much larger attack surface for the organization. Because each microperimeter is associated with each user device, endpoints become prime targets for malware infections and sophisticated exploits.

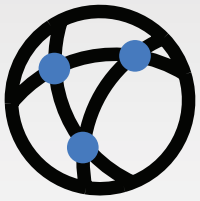
As a result of this explosion of endpoints and expanding attack surface, many organizations are fundamentally losing control of the network in the sense that they are no longer sure what devices are connecting to it. In fact, there is virtually no device configuration standardization for bring your own device (BYOD) or IoT. BYOD mobile devices can put networks at risk through data leakage, unsecured Wi-Fi, network spoofing, phishing, spyware, broken cryptography, or improper session handling.

However, the greatest area of growth in the endpoint attack surface is from the IoT device explosion. Cyberattacks on IoT devices are booming as organizations connect more and more "smart" devices. Bad actors are exploiting these devices to conduct distributed denial-of-service (DDoS) attacks and other malicious actions.

To fully secure BYOD and IoT endpoints, enterprises must have visibility into where each device is, what it does, and how it connects to other devices across the network topology. Lack of visibility leaves an organization vulnerable to unseen risks, and many organizations do not have a plan in place to deal with attacks on IoT devices. Security leaders must be able to track devices at the edges of the network.

Traditional network segmentation is used by some organizations, but it is difficult to define secure network-based segments that can be simultaneously accessible to all authorized users and applications and completely inaccessible to all others. Even best-effort segmentation leaves gaps in network defenses—access scenarios that network architects did not envision—which malicious actors can exploit.

In addition, organizations remain under attack if access permissions are based on assumed trust of vetted devices. Numerous organizations have been surprised by attacks from previously trusted employees and contractors. A lost or stolen device can reveal passwords that enable future attacks on the network. This is why a zero-trust approach is so critical. As cyber criminals focus on compromising the broad array of network devices, CIOs and security leaders need better visibility and detection of every specific device connecting to the network.



IDC predicts that by 2025 there will be 55.7 billion connected devices worldwide, 75% of which will be connected to an IoT platform.[3]

Protecting Assets On and Off the Network

Another significant problem for security leaders is the increasing use of mobile devices offline or on other networks, which presents security threats such as malware or botnets when those devices log back onto the network. For example, many workers use their BYOD devices to bridge their personal and business lives. They use them to browse the internet, interact with others on social media, and even receive personal emails when they're not logged into the corporate network. But when they rejoin the network after being online, workers can inadvertently expose their devices, and company resources, to a variety of threats such as viruses, malware, and other exploits.

By transitioning to a zero-trust network access framework that identifies, segments, and continuously monitors all devices, organizations can replace their high-risk, flat networks to ensure that internal resources remain secured, and that data, applications, and intellectual property remain protected. This strategy not only reduces the risks associated with perimeter-centric security strategy but also increases the visibility and control of off-network devices, while simplifying overall network and security management.

Setting up ZTA includes establishing pervasive application access controls, strong authentication capabilities, and powerful network access control technologies. Using the zero-trust model for application access or zero-trust network access (ZTNA) makes it possible for organizations to shift away from only relying on traditional virtual private network (VPN) tunnels to secure assets being accessed remotely. A VPN often provides unrestricted access to the network, which can allow compromised users or malware to move laterally across the network seeking resources to exploit.

With ZTNA, access is only granted to applications on a policy-based, per-session basis to individuals and applications after devices and users have been authenticated and verified. The system applies this policy equally whether users are on or off the network. So you have the same zero-trust protections no matter where a user may be connecting.

Conclusion: A Zero-trust Access Approach Is Needed

Digital initiatives expand and change the enterprise attack surface, which opens up new attack vectors that can be exploited. As attacks become more sophisticated and advanced, the traditional perimeter security approach is no longer sufficient. Depending on the nature and sophistication of the threat, no single point in an organization's security infrastructure has visibility into all aspects of the threat. Zero-trust access focuses on the users and devices that are connecting to the network, confirming their identity and making sure they have just the right amount of access and trust.

Secure authentication plays a pivotal role in the implementation of an effective ZTA security policy. Adopting the ZTA practice of applying "least access" privileges as part of access management means that if a user account is compromised, cyber adversaries only have access to a restricted subset of corporate assets.

One of the main reasons for the growing attack surface is due to the proliferation of IoT and smart devices that are coming onto the network. CIOs and security leaders often lack the visibility into the flood of devices accessing the network. A zero-trust approach empowers organizations to identify and secure unknown IoT endpoints and devices that enter the network. Integrated endpoint visibility, granular control, advanced protection, and policy- and context-based endpoint assessment work together to ensure organizations are protected against compromised devices.

Today's workforce accesses networks from a variety of locations and uses both personal and business devices, so CIOs need a way to protect all endpoints at the network edge. Cyber criminals have been quick to respond to the fact that the network perimeter has expanded so rapidly and dramatically, so CISOs can no longer ignore the benefits of the zero-trust model for network security. With a zero-trust access approach, organizations can improve visibility of all devices on and off the network, enable advanced protection, provide secure access to applications, and implement dynamic access control, all while reducing the attack surface.

[1] "2021 Data Breach Investigations Report," Verizon, May 2021.

[2] "2020 Cost of a Data Breach Report," IBM Security, July 2020.

[3] "IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC," IDC, July 27, 2020.

July 15, 2021 11:26 AM

696181-C-0-EN