FERTINET

Braxton-Grant
TECHNOLOGIES

WHITE PAPER

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 (DI) initiatives within their organizations. This means business applications and data are now dispersed far and wide, away from the corporate premises, giving workers access to more corporate assets from many locations. For this reason, the traditional perimeter is dissolving, which opens the internal network to a growing 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, making sure all users, all devices, and every web application from the cloud is trusted, authenticated, and has the right amount of access.

The Evolution of the Network Edge

For CIOs, DI initiatives are critical for business growth. One aspect of this growth is the proliferation of new network edges—private and public cloud infrastructures, Internet of Things (IoT) and mobile devices, software-defined (SD) branches—all of which 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.

Many of the most damaging and successful attacks experienced by organizations and governments over the past couple of years have been focused on edge networking devices.[2]

In recent years, there's been an explosion of network edges, so much so that the traditional perimeter is dissolving, creating 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.[1]

For CIOs and security leaders, it is incredibly difficult to keep up with the growing number of attacks. That is why there is a shift happening, from trusting everything on the network to not trusting things. With a zero-trust access model, CIOs assume they have already been compromised. In particular, there are three 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. Due to the fact that 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.

While bring your own device (BYOD) may be popular with users and managers alike, CIOs cannot overlook the dangers. The broad attack surface makes it easier for evolving threats to penetrate traditional perimeter defenses and move laterally inside the internal network, which is one of the ways breaches can remain undetected for so long. Some of the most damaging breaches have occurred through unauthorized users gaining access to the network or through inappropriate levels of access given to trusted users. While BYOD is becoming ubiquitous within enterprises, 83% of security leaders say their organizations are at risk from mobile threats.[3]

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. 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.

This is why zero-trust access is so important. Since devices are constantly going on and off the network, it is critical to ensure that security leaders know which users are on the network, and that they have the right level of access. As roles change, such as a move from sales to operations, workers might not need access to the same areas they had in 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. However, the proliferation of mobile devices and IoT products have dissolved the traditional network perimeter into many micro-perimeters, which results in a much larger attack surface for the organization. Since each micro-perimeter 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 BYOD or IoT. In regards to BYOD, mobile devices can put networks at heavy risk. This could be 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.

81% of organizational leaders say employees are now the greatest risk to mobile security.[4]

Many of the most damaging and successful attacks experienced by organizations in recent years have been focused on edge networking devices.[6]

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, as well as many other types of 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. Security leaders must be able to track devices at the edges or the network. However, almost half of cybersecurity professionals say they do not have a plan in place to deal with attacks on IoT devices, even though nine out of ten express concerns over future threats.[5]

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.

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 not logged into the 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.

This comes at a time when companies are unable to keep up with the number of endpoints coming on and off the network. In a recent Ponemon Institute report, 63% of companies are unable to monitor off-network endpoints, and over half can't determine the compliance status of endpoint devices.[7] The sheer number of devices connected to the network obscures visibility across all endpoints. As a result, the ability to manage a significant amount of risk is greatly reduced.

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.

63% of organizations are unable to monitor endpoint devices when they leave the corporate network, and 53% reveal that malware-infected endpoints have increased in the last 12 months.[8]

Conclusion: A Zero-Trust Access Approach is Needed

While CIOs are measured in how they use DI to accelerate the business, DI initiatives also expand and change the enterprise attack surface, opening up new attack vectors for cyber threats to exploit. Bad actors become more sophisticated and advanced, and the traditional perimeter security approach is no longer sufficient. Depending on the nature and sophistication of the threat, there is no single point in an organization's security infrastructure that can see all aspects of the threat. With zero-trust access, CIOs can focus 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.

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. To fully secure all of these endpoint devices, enterprises need a zero-trust access policy across the entire network that provides visibility into where each device is, what it does, and how it connects to other devices across the network, as well as continuous monitoring to detect any behavioral anomalies that could indicate a threat.

As CIOs and security leaders navigate a workforce that is working from a variety of locations and using both personal and business devices to access the network, they need a way to protect all endpoints at the network edge. With a zero-trust access approach, organizations can improve visibility of all devices on and off the network, enable advanced protection, and implement dynamic access control, all while reducing the always-expanding attack surface.

[1] "Cyber Threat Alliance Joint Analysis: Securing Edge Devices," Cyber Threat Alliance, 2019.

[2] Neil Jenkins and Natasha Cohen, "Living on the Edge," Cyber Threat Alliance, April 30, 2019.

[3] "Mobile Security Index 2019," Verizon, 2019.

[4] "Mobile Security Index 2019," Verizon, 2019.

[5] "Only 47% of Cybersecurity Pros are Prepared to Deal with Attacks on their IoT Devices," Help Net Security/Neustar International Security Council Research, November 8 2019.

[6] Neil Jenkins, "Living on the Edge," CyberThreatAlliance, April 30, 2019.

[7] "The Cost of Insecure Endpoints," Ponemon Institute, 2020.

[8] "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.