DON'T RISK IT!

NAC's Critical Role in Mitigating Network Risk

www.portnox.com

Introduction

In today's increasingly connected world, the challenges of cybersecurity have grown exponentially, keeping companies, both big and small, on their toes. Cyber threats are evolving at an unprecedented pace, with the proliferation of connected devices within companies adding a new layer of complexity. Organizations are struggling to identify and mitigate risks to their networks, and this is where Network Access Control (NAC) has emerged as a crucial tool in their cybersecurity arsenal.

This white paper delves into the evolving cyber threat landscape, the proliferation of connected devices, the challenges companies face in securing their networks, and how NAC plays a pivotal role in addressing and mitigating network risks. Furthermore, we explore the future of NAC and its evolving role in tackling emerging security challenges.

The Threat Landscape is Growing (Too) Fast

The digital age has ushered in a new era of cyber threats. Hackers and malicious actors have become more complex and innovative, constantly adapting to exploit vulnerabilities. The following factors exemplify the evolving nature of cyber threats:

Increased Sophistication: Cybercriminals have evolved from script kiddies to highly sophisticated entities. They employ advanced techniques like social engineering, exploit zero-day vulnerabilities, and develop advanced malware to breach corporate networks.

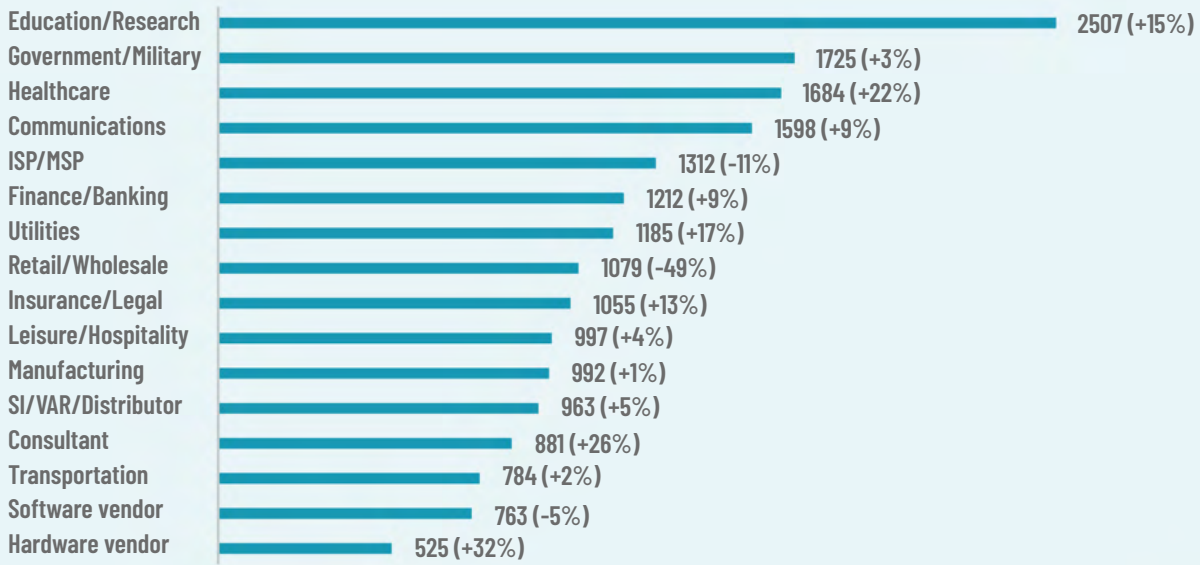
Ransomware Surge: Ransomware attacks have skyrocketed, causing massive financial losses and data breaches. Attackers often demand hefty ransoms in cryptocurrencies, making it challenging for organizations and law enforcement agencies to trace the money.

Supply Chain Attacks: Attackers have expanded their focus beyond individual organizations to their supply chains. A breach in a supplier's network can lead to a cascade of compromises affecting multiple organizations downstream.

Nation-State Actors: Nation-state-sponsored cyberattacks have become more common. These attacks can have serious geopolitical implications and aim to steal intellectual property, conduct espionage, or disrupt critical infrastructure.

IoT Vulnerabilities: The proliferation of Internet of Things (IoT) devices has created numerous new entry points for attackers. Weak security on these devices makes them attractive targets.

Global Average Weekly Cyber Attacks Per Industry
(2022 Q1 Compared to 2023 Q1)



Source: Healthcare cyber attacks are on the rise, World Economic Forum

There Are So Many Connected Devices, We've Lost Count

As organizations embrace digital transformation, the number of connected devices within their networks has grown exponentially. This proliferation includes not only traditional devices like laptops and smartphones but also a wide range of IoT devices, such as smart thermostats, security cameras, and industrial control systems. The increasing number of connected devices brings both opportunities and challenges:

Productivity and Efficiency: Connected devices enhance productivity and efficiency in various industries, including manufacturing, healthcare, and logistics.

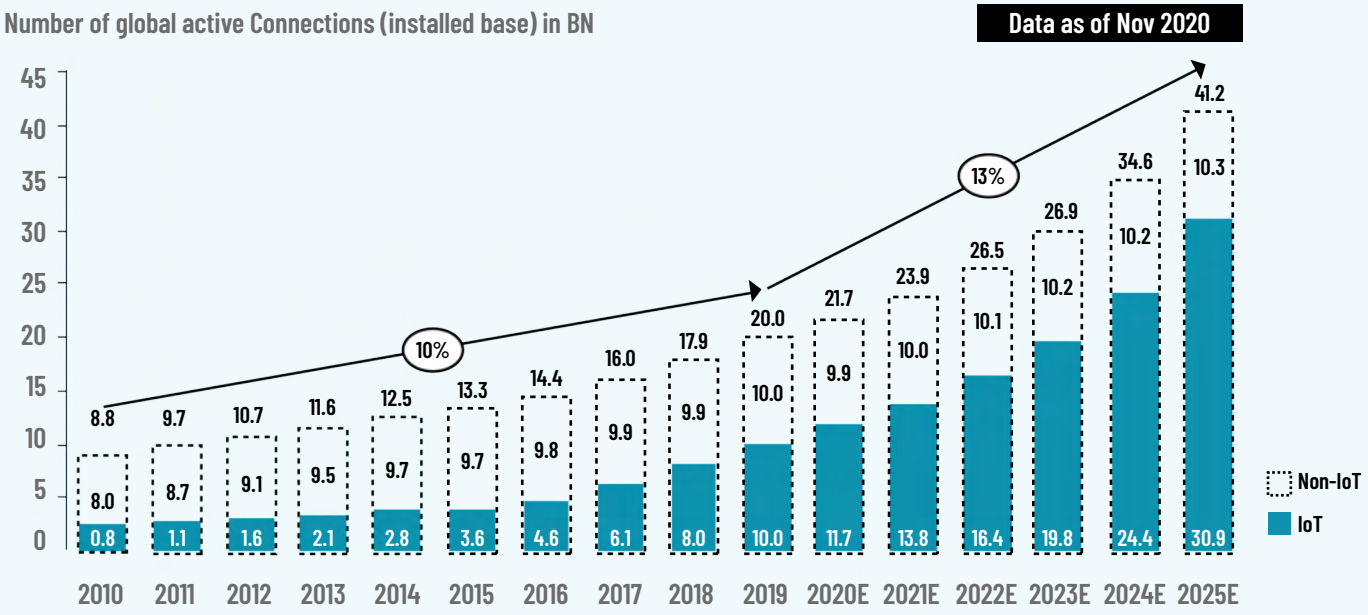
Complexity and Vulnerabilities: Each new device presents a potential vulnerability. Poorly configured IoT devices, weak passwords, and unpatched firmware can all create entry points for cybercriminals.

Shadow IT: Employees often bring their own devices to work, adding to the complexity. The use of personal devices for business purposes can introduce unmanaged endpoints into the corporate network.

Third-Party Risks: As companies collaborate with third-party vendors and service providers, these external entities may introduce additional vulnerabilities into the network.

Total number of device connections (incl. Non-IoT)

20.0B in 2019 - expected to grow 13% to 41.2B in 2025



Source: IoT connections market update—May 2023, IoT Analytics

Risk Blindness is Real, Ask Anyone in IT Security

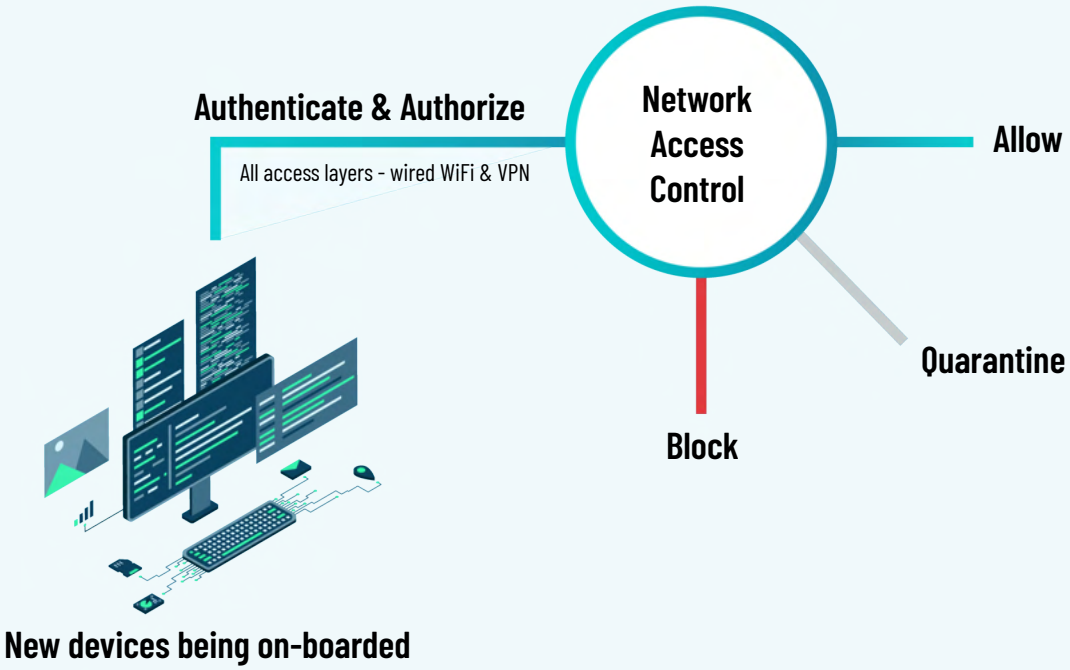
Identifying and securing network risks in this dynamic environment is a formidable challenge for organizations. The following factors contribute to the difficulties faced by companies in safeguarding their networks:

- **Visibility:** The sheer volume and diversity of devices make it difficult for organizations to have full visibility into their network. Knowing what devices are connected and what they are doing is a fundamental requirement for security.
- **Compliance and Enforcement:** Ensuring that devices comply with security policies and enforcing these policies consistently across the network can be a daunting task.
- **Zero Trust Security:** The traditional perimeter-based security model is no longer effective. Zero Trust Security, which assumes that no device or user should be trusted by default, is gaining prominence. Implementing this model requires a significant shift in mindset and technology.
- **Security Patch Management:** Keeping devices up to date with the latest security patches is a constant battle. Legacy systems, IoT devices, and the need for thorough testing before deployment often slow down the patch management process.
- **User Awareness:** Employees and users can inadvertently introduce risks through actions like clicking on phishing emails or downloading malicious software. Educating and raising awareness among employees is a continuous effort.

Network Access Control (NAC): Your New (Old) Friend

In the face of evolving threats and the challenges associated with the proliferation of connected devices, Network Access Control (NAC) has emerged as a key tool in the cybersecurity arsenal of organizations. NAC solutions help mitigate network risks by addressing the aforementioned challenges:

- **Visibility and Control:** NAC solutions provide organizations with comprehensive visibility into the devices on their network, allowing them to enforce security policies consistently. This extends to both managed and unmanaged devices, improving control.
- **Compliance and Enforcement:** NAC solutions ensure that devices adhere to security policies, such as up-to-date antivirus software, strong passwords, and system updates. Non-compliant devices can be quarantined or granted limited access until they meet requirements.
- **Network Segmentation:** NAC enables organizations to segment their networks, separating critical assets from potentially vulnerable devices. Segmentation helps contain breaches and limit lateral movement by attackers.
- **Guest Network Security:** NAC facilitates secure guest access to company networks. It ensures that guests are isolated from internal resources and can only access the internet, safeguarding sensitive data.
- **Integration with Other Security Tools:** NAC solutions often integrate with other security tools, enhancing their effectiveness. This includes Security Information and Event Management (SIEM) systems, firewalls, and endpoint protection platforms.
- **Continuous Monitoring:** NAC systems monitor device behavior continuously, allowing for real-time threat detection and response. Any anomalous activity can trigger alerts and automated actions.



Control Access, Control Risk

Network Access Control addresses and mitigates network risks in the following ways:

- **Enforcing Security Policies:** NAC ensures that all devices meet security requirements before they are granted access to the network. This reduces the risk of vulnerabilities being exploited by attackers.
- **Thwarting Unauthorized Access:** NAC identifies and prevents unauthorized devices from gaining entry into the network. This is critical in preventing both external and internal threats.
- **IoT Device Management:** NAC can secure IoT devices and separate them from other critical assets to prevent them from becoming an entry point.
- **Granular Access Control:** NAC offers granular control over user and device access. This minimizes the risk of lateral movement within the network by attackers who have breached the perimeter.
- **Reducing Attack Surface:** By segmenting networks and isolating devices, NAC helps reduce the overall attack surface. Even if one segment is compromised, the rest of the network remains secure.

NAC, Risk & Zero Trust

The Zero Trust security model offers a groundbreaking approach that assumes no trust within or outside the network. At the core of this model is Network Access Control (NAC), which plays a pivotal role in enforcing the principles of Zero Trust. In this article, we will delve into the world of Zero Trust and explore how NAC fits seamlessly into this innovative security paradigm.

Understanding Zero Trust

Zero Trust is a security philosophy that stems from the realization that perimeter-based security, where trust is placed in users or devices solely based on their location within the network, is no longer effective in today's complex and dynamic threat landscape. Zero Trust proposes a fundamental shift in mindset: "Never trust, always verify." This means that trust is not granted by default to any user, device, or application, regardless of where they are located.

Zero Trust relies on the principle of continuous verification, ensuring that every element attempting to access network resources is authenticated and authorized, even after gaining initial access. Trust is no longer based on network location but on a combination of user and device attributes, the current state of the network, and other context-aware factors.

Key Principles of Zero Trust

• **Identity-Centric:** Zero Trust centers around the concept of identity. Users, devices, and applications must be uniquely identified and authenticated before gaining access to resources. Multi-factor authentication (MFA) is a common component of identity verification.

• **Least Privilege Access:** Zero Trust minimizes access privileges to the absolute minimum necessary for a user or device to perform its tasks. This reduces the potential for lateral movement in the event of a breach.

• **Continuous Monitoring**: Network activity is continuously monitored to detect any anomalies or suspicious behavior.
Even after initial access, users and devices are scrutinized to maintain trust.

• **Micro-Segmentation:** The network is divided into micro-segments, with granular access controls applied to each segment. This reduces the attack surface and limits lateral movement for attackers.

• **Encryption:** Data in transit and at rest is encrypted to ensure its confidentiality and integrity.

The Role of NAC in Zero Trust

Network Access Control (NAC) is a critical component of the Zero Trust security model, as it provides the mechanisms to enforce the core principles of Zero Trust.

• **Authentication and Authorization:** NAC solutions ensure that every user, device, or application is authenticated and authorized before they can access network resources. This identity-centric approach aligns with the Zero Trust principle of never trusting by default.

• **Device Assessment:** NAC solutions assess the security posture of connecting devices. They check for up-to-date operating systems, security patches, antivirus software, and other security essentials. If a device does not meet the defined security criteria, it can be isolated or denied access until the issues are resolved.

• **Continuous Monitoring**: NAC solutions continuously monitor network traffic, user activity, and device behavior.
They detect unusual patterns or suspicious activities, helping to maintain the trustworthiness of the network.

• **Least Privilege Access:** NAC enforces the principle of least privilege access by ensuring that users and devices only gain access to the resources required for their specific tasks. Access policies are dynamic and can be adjusted in real-time based on changing context.

• **Micro-Segmentation:** NAC enables the creation of network micro-segments, each with its specific access policies.
This segmentation minimizes lateral movement opportunities for potential attackers and limits the impact of a security breach.

3 Benefits of Microsegmentation

Reduce the Impact of an attack

Improve Breach Containment

Strengthen Compliance

• **Compliance Enforcement:** NAC solutions enforce compliance with security policies and regulations. They ensure that users and devices adhere to security best practices and policies defined by the organization.

• **Encryption:** NAC can facilitate and ensure the encryption of network traffic, especially in sensitive environments. This aligns with the Zero Trust principle of securing data in transit and at rest.

Challenges and Considerations

While Network Access Control is a critical component of Zero Trust, implementing it effectively can be a complex endeavor. Organizations must consider several challenges and best practices:

• **Scalability:** Organizations should choose NAC solutions that can scale to accommodate the growing number of devices and users while maintaining optimal performance.

• **Integration:** NAC must be integrated with other security technologies, such as identity and access management (IAM), firewall rules, and intrusion detection systems, to enforce Zero Trust policies consistently.

• **User Experience:** Implementing strict access controls can sometimes lead to a friction-filled user experience. Striking a balance between security and usability is crucial.

• **Visibility:** Zero Trust relies on continuous monitoring and visibility. NAC solutions should provide detailed insights into network activity, device posture, and user behavior.

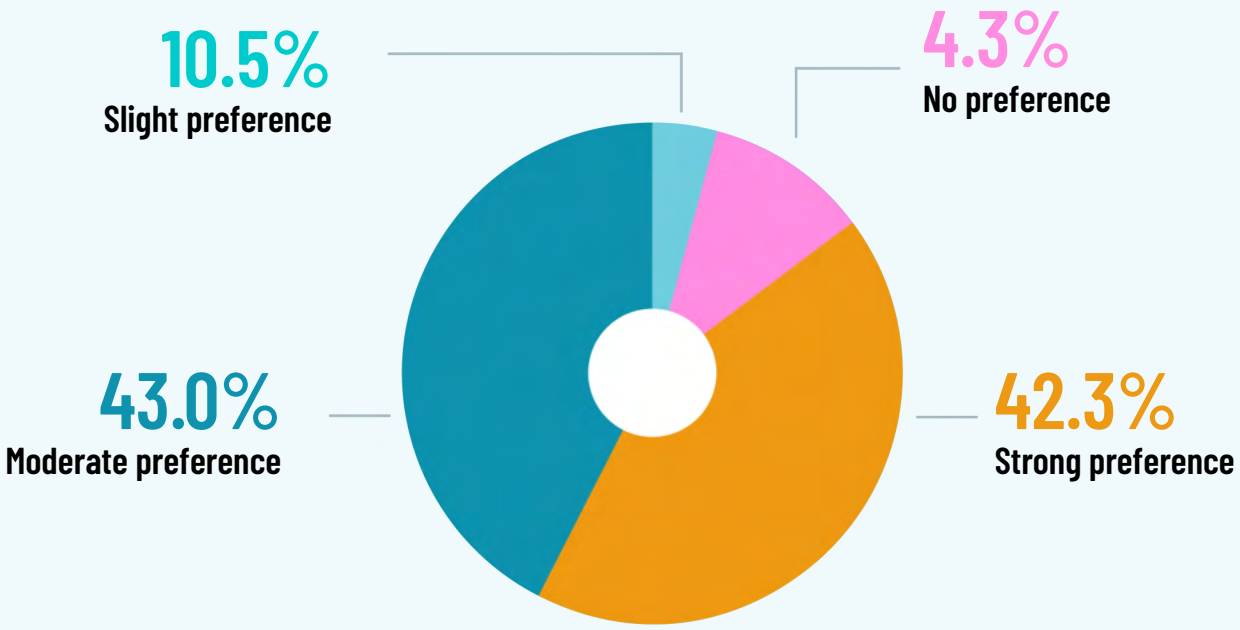
What's in Store for NAC In the Future?

As the cybersecurity landscape continues to evolve, NAC must adapt to meet new security challenges. The following are some directions in which NAC is likely to evolve:

- **Machine Learning and AI Integration:** NAC solutions will incorporate machine learning and artificial intelligence to better detect and respond to threats. These technologies will help NAC systems adapt to emerging attack patterns.
- **Continuous Authentication:** Continuous authentication will become more common, replacing traditional, static password-based access. Behavioral analysis and biometric data will play a significant role in this evolution.
- **IoT Security Integration:** NAC will become even more adept at managing and securing IoT devices. It will adapt to the unique requirements of various IoT deployments, such as industrial automation and healthcare.
- **Improved User Experience:** NAC solutions will focus on providing a seamless user experience while maintaining stringent security. This will involve reducing friction in the authentication process.
- **Compliance and Reporting:** NAC systems will offer more robust compliance monitoring and reporting capabilities, helping organizations meet regulatory requirements and demonstrate their commitment to cybersecurity.

Majority prefers AI, machine learning security

According to survey results, an overwhelming percentage of organizations globally want security products to use machine learning AI.



Source: Unpack the use of AI in cybersecurity, plus pros and cons, TechTarget

Conclusion

In a world characterized by evolving cyber threats and the proliferation of connected devices, organizations must leverage robust cybersecurity measures. Network Access Control (NAC) has proven to be a pivotal tool in addressing and mitigating network risks. With its ability to enforce security policies, control device access, and offer comprehensive visibility, NAC is well-equipped to adapt to the changing landscape of cybersecurity.

As the future unfolds, NAC will continue to evolve to meet new security challenges, ensuring that companies can defend their networks against the ever-adaptive cyber threats of the digital age.

About Portnox

Portnox offers cloud-native zero trust access control and cybersecurity essentials that enable agile, resource-constrained IT teams to proactively address today's most pressing security challenges: the rapid expansion of enterprise networks, the proliferation of connected device types, the increased sophistication of cyberattacks, and the shift to zero trust. Hundreds of companies have leveraged Portnox's award-winning security products to enforce powerful access, endpoint risk monitoring and remediation policies to strengthen their organizational security posture. By eliminating the need for any on-premises footprint common among traditional information security systems, Portnox allows companies – no matter their size, geo-distribution, or architecture – to deploy, scale, enforce and maintain these critical zero trust security policies with unprecedented ease.


portnox®
www.portnox.com