

portnox®

WHITE PAPER

The Passwordless Revolution

How Ditching Passwords Can Stop the Next Cyber Attack

Executive Summary

Passwordless security is more than a buzzword; it's a transformative approach that's reshaping the landscape of enterprise cybersecurity. Traditional password-based methods are fraught with pitfalls: complexity, user fatigue, and, most significantly, vulnerability to cyber-attacks. Passwordless security transcends these challenges using alternative authentication mechanisms such as digital certificates, biometrics, hardware tokens, and mobile-based methods. This shift makes both logins and transactions easier and significantly more secure.

For example, the financial services sector is rapidly adopting passwordless technologies to secure user accounts, facilitating both better customer experiences and robust security measures. And the drive for this move is compelling. According to a 2020 survey of IT executives, the majority of respondents (53%) reported that their organizations had suffered data breaches directly related to mismanaged employee credentials. The impact of these breaches was significant: 44% reported financial loss, and nearly half (48%) said their companies endured reputational damage[1]. These alarming statistics illustrate the critical need for enterprises to reconsider their security frameworks.

The passwordless authentication market is surging in line with this need for change. In 2022, the market was valued at an impressive 15.6 billion U.S. dollars, and forecasts predict it will exceed a staggering 53 billion U.S. dollars by 2030[2]. This growth isn't just an indicator of a trend; it's a testament to the urgent, widespread recognition that passwordless security is not the future—it's the present, and organizations must adopt it to protect both their assets and reputations effectively.

Key Benefits

Transitioning to passwordless security offers multiple advantages:

1. **Enhanced Security:** Eliminates the vulnerabilities of password-based systems.
2. **User Convenience:** Streamlines the login experience without compromising security.
3. **Reduced Costs:** Lowers helpdesk expenses tied to password resets.
4. **Future-Proofing:** Prepares organizations for the security demands of tomorrow.

[1] *Report: Passwordless – the Future of Authentication, IDG*
[2] *Passwordless authentication global market size, 2021-2030, Statista*

Introduction

Background on the Evolution of Cybersecurity Challenges

The Early Years: Physical Security Measures

In the 1960s and 1970s, the infancy of the computing age, cybersecurity was virtually synonymous with physical security. The central challenge was to lock up computer rooms and secure them from unauthorized personnel. The threat landscape was limited at this time, primarily focused on insider sabotage or data theft.

The Advent of Malware: 1980s and 1990s

The late 1980s and 1990s marked a seismic shift in cybersecurity challenges. The era saw the emergence of the first computer viruses and worms, such as the infamous Morris Worm. This worm alone wreaked havoc on more than 6,000 computers, leading to estimated damages of $100,000. These new forms of cyber threats necessitated the development of antivirus software and the establishment of foundational network security measures like firewalls and intrusion detection systems.

Complexity and Sophistication: The 2000s

The new millennium brought even more nuanced and targeted cyber-attacks. In response, the cybersecurity industry developed advanced measures like encryption, multi-factor authentication, and virtual private networks (VPNs). Meanwhile, the ascent of cloud computing and the widespread adoption of mobile devices unleashed a fresh set of challenges. Solutions such as mobile device management (MDM) and cloud access security brokers (CASBs) emerged to mitigate these newfound risks.

The Present-Day Quandary: Advanced and Pervasive Threats

Today, cybersecurity isn't just a requirement—it's a critical lifeline for businesses and institutions globally. Cyber-attacks have become more frequent and sophisticated, employing cutting-edge technologies like artificial intelligence and machine learning. These advancements in the cybersecurity space have spawned solutions capable of detecting and responding to threats in real-time. However, the advent of the Internet of Things (IoT) has expanded the attack surface exponentially as more and more devices get connected to the internet.

The continued reliance on traditional passwords is a glaring weak link in contemporary cybersecurity strategies. As cyber-attacks become more refined and targeted, passwords are increasingly vulnerable. Even complex passwords are susceptible to phishing, social engineering, and advanced brute-force attacks. This vulnerability highlights the urgent need for alternative authentication methods that meet the sophisticated threat landscape.

Growing Inadequacies of Traditional Password-Based Authentication

The Limits of Password Complexity

The security limitations of passwords are becoming alarmingly clear as cyber threats continue to evolve. On one end of the spectrum are weak passwords—easy to remember but equally easy for attackers to guess or crack using automated tools. According to Nordpass, an astonishing 73% of the world's most popular passwords can be cracked in less than a second using brute-force attacks. The five most common passwords, analyzed by CyberNews researchers from a data set of 15.2 billion, include startlingly simplistic combinations like '123456,' '123456789,' 'qwerty,' 'password,' and '12345.[3]

20 Most Common Passwords

The Reader´s Digest Version

If yours are on this list, it's time to change.

1.	123456
2.	123456789
3.	Qwerty
4.	Password
5.	12345
6.	12345678
7.	111111
8.	1234567
9.	123123
10.	Qwerty123

11.	1q2w3e
12.	1234567890
13.	DEFAULT
14.	0
15.	Abc123
16.	654321
17.	123321
18.	Qwertyuiop
19.	Iloveyou
20.	666666

On the opposite end are complex passwords, which bring their own set of problems. While harder for machines to crack, these passwords are often so convoluted that users resort to writing them down on physical notes—a practice that carries its own security risks. For instance, storing sensitive passwords under a keyboard is an open invitation for internal threats.

[3] *The password hassle: a strong one is no longer enough, Cybernews*

The Pitfalls of Password Reuse

Another widespread issue is password reuse. Remembering a single strong password may seem efficient. Still, the risks multiply when that password is used across multiple platforms—from social media and banks to news sites and streaming services. A single breach can compromise the user's entire digital identity.

The Persistent Threat of Data Breaches

Data breaches have become alarmingly frequent, making headlines with disturbing regularity. Even organizations with advanced security measures are falling victim to these attacks. The impact of these breaches is magnified when stolen passwords are reused across different platforms, providing cybercriminals with a one-stop gateway to infiltrate multiple networks.

Malicious Software and Credential Theft

Traditional passwords offer little defense in a world increasingly plagued by sophisticated malicious software. Malware can log keystrokes or create false interfaces to trick users into divulging their credentials. The rapid rise of such 'man-in-the-middle' attacks shows how even the most security-conscious users can fall prey to clever schemes that steal passwords.

Phishing Attacks and Social Engineering

As cyber attackers become more skilled in psychological manipulation techniques, the susceptibility of passwords to phishing attacks and social engineering tactics has grown significantly. Users are often tricked into revealing passwords through cleverly disguised emails or messages, bypassing even the most robust technical defenses.

The Human Factor

Human errors, such as inadvertently sending passwords through insecure communication channels or failing to update passwords regularly, further undermine the efficacy of password-based systems. These are not merely theoretical vulnerabilities; they are real-world chinks in the armor that attackers exploit daily.

Passwordless Security as an Innovative Solution

Passwordless security represents a groundbreaking shift in authentication methods, offering a more secure and user-friendly alternative to traditional passwords. By leveraging advanced technologies like biometrics, hardware tokens, and mobile authentication, passwordless systems eliminate the common vulnerabilities associated with password-based authentication.

A standout feature in this landscape is the use of digital certificates. These certificates serve as cryptographic proof of a user's identity, offering a highly secure yet simple way to access services. Unlike passwords, which can be easily compromised, digital certificates provide a robust layer of security that is inherently resistant to phishing attacks, data breaches, and other common threats.

Understanding Passwordless Security

Explanation of Passwordless Authentication via Digital Certificates

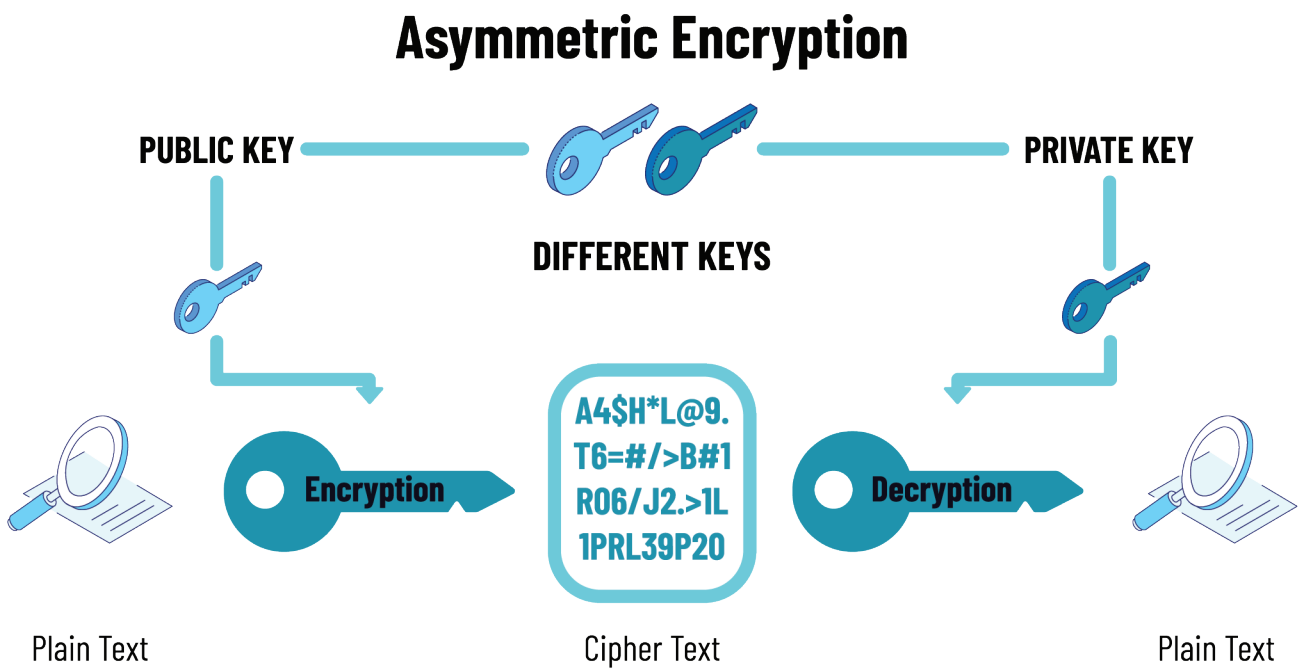
Passwordless security is a revolutionary departure from traditional authentication methods that depend on something the user knows (a password) to something the user has or is (a device, a biometric trait). One of the most secure forms of passwordless authentication involves using digital certificates, cryptographic credentials stored on a user's device, or a secure hardware token.

Digital Certificates: How They Work

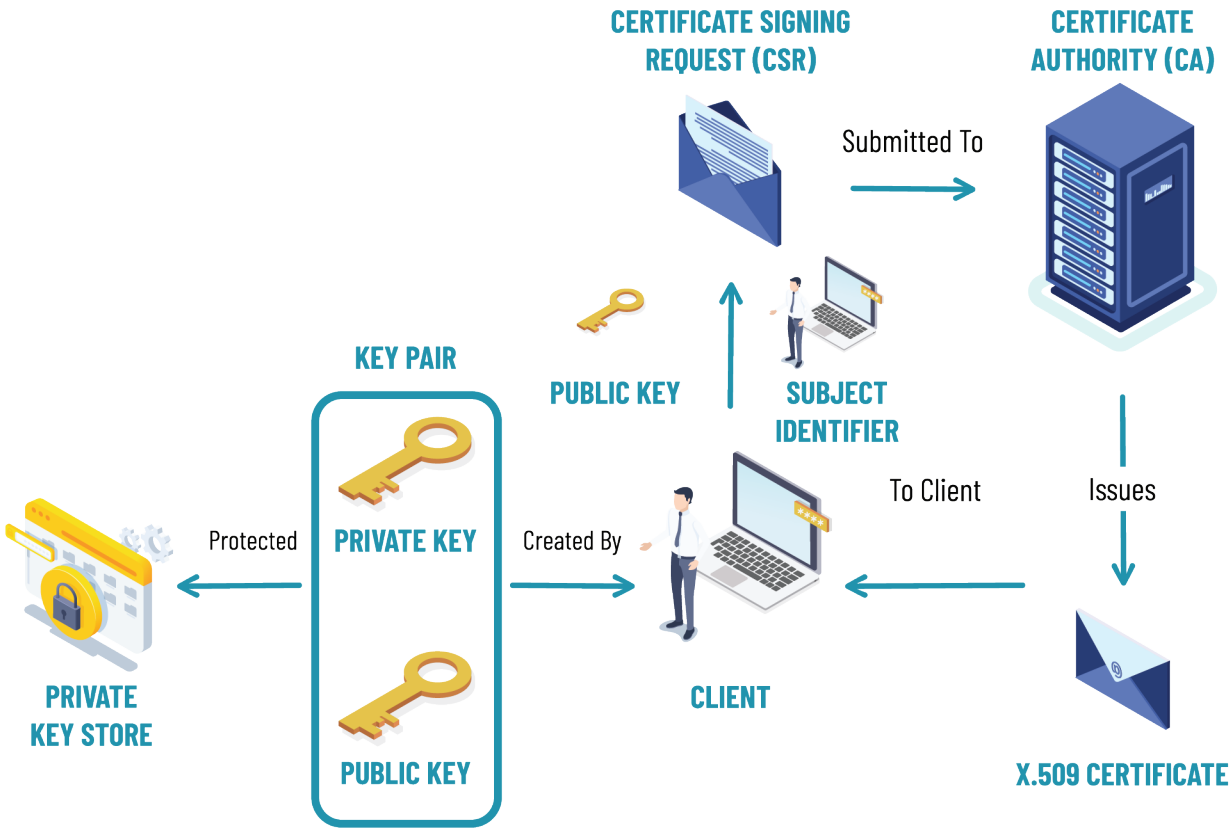
To understand how digital certificates work, you must start with the PKI (Public Key Infrastructure.) The PKI is comprised of all hardware, software, procedures, and anything else required to manage the creation, distribution, revocation, usage, and storage of digital certificates and public key encryption.

Public Key encryption, also known as asymmetric encryption, is what makes digital certificates secure. In symmetric encryption, the same key is used to decrypt and encrypt messages. In order to decrpyt a message there must be a way of securely transmitting the key, which quickly presents issues of scale, both in the number of keys and the number of secure channels available to transmit the keys.

Asymmetric encryption features a public key that is available to anyone, and a private key that is kept closely guarded. Anything encrypted using one key can only be decrypted with the corresponding key. This system is much more efficient, but requires an element of trust that the person who owns the corresponding key is who they say they are.



Enter the Certificate Authority, a key feature of the PKI. The CA issues a digital certificate that binds the public key to an individual, device, or service. So a digital certificate is, in essence, a key that is signed by a CA that promises the identity of this key holder is legitimate.



So when used for passwordless authentication, the digital certificate is created and signed by the Certificate Authority, and then distributed to the user's devices. When authentication is needed, the server sends a cryptographic challenge to the client.
The client signs the challenge using their private key (which does not require them to actually transmit the key).
The server validates the signature using the client's public key, which is stored in the digital certificate, and if that's successful, the server grants access.

Comparison with Traditional Password-Based Systems

Traditional password-based authentication systems rely on static, shared secrets that are prone to various types of attacks, including brute force, phishing, and social engineering. In contrast, digital certificates employ asymmetric cryptography, where a private key is kept confidential on the user's device, while the corresponding public key is freely accessible via the certificate. This eliminates the need for shared secrets and significantly reduces the attack surface.

Security Advantages

Digital certificates offer multiple layers of security benefits:

1. **Non-Repudiation:** Since the certificate is tied to a unique entity, actions taken using it are verifiable and indisputable.
2. **Data Integrity:** Cryptographic algorithms ensure that the data exchanged between parties remains unchanged.
3. **Resistance to Phishing:** Even if a malicious actor tries to impersonate the server or client, the absence of a shared secret makes it almost impossible to succeed.
4. **Elimination of Password Breaches:** Without a password database to target, attackers lose one of their most fertile grounds for compromise.

User Experience Improvements

1. **Simplified Access:** Users no longer need to remember complex passwords.
2. **Quick Authentication:** Automatic certificate-based methods can be faster than manual password entry.
3. **Universal Compatibility:** Digital certificates can be used across multiple platforms and services, simplifying the user experience.

Reduced Reliance on Memorization

The transition from password-based to certificate-based systems eliminates the cognitive burden of memorizing complex passwords. Users are free from the recurring cycles of password changes and the challenges associated with forgetting passwords.

The Business Case for Passwordless

Enhanced Security

1. **Eliminating Password-Related Vulnerabilities:** Adopting a passwordless approach eradicates all categories of cybersecurity threats. For instance, phishing campaigns that aim to capture passwords become ineffective because there are simply no passwords to be stolen. This is not just theoretical; companies that have transitioned to passwordless systems report substantially fewer incidents related to credential theft.
2. **Reduction of Successful Cyberattacks:** Using digital certificates adds a strong layer of security that significantly minimizes unauthorized access. Unlike passwords, which can be guessed or cracked using brute-force methods, digital certificates utilize cryptographic keys that are nearly impossible to replicate.

Improved User Experience

1. **Simplified Authentication Processes:** One of the most immediate benefits of passwordless systems is streamlining the authentication process. Rather than having to remember and input complex passwords, users can authenticate themselves using biometric data like fingerprint scans or facial recognition. Alternatively, they can use hardware tokens that generate time-based codes. In healthcare settings, for example, this simplification can be invaluable, allowing medical professionals quick and secure access to vital patient information, thereby speeding up care delivery.

2. **Convenience and User Satisfaction:** Users often struggle with password fatigue, having to remember multiple sets of complex passwords for different systems and services. Passwordless authentication eliminates this cognitive burden and substantially improves user satisfaction. In fact, more than 50% of organizations transitioning to passwordless saw a significant positive impact to risk reduction and improved user experience[4].

Regulatory Compliance

Transitioning to passwordless systems proactively aligns with the increasingly stringent data protection standards mandated by regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. These legal frameworks have a global impact, affecting companies that deal with the personal data of EU citizens or California residents, regardless of where the companies are based. GDPR and CCPA are explicit about the necessity for robust data protection measures, including employing strong authentication protocols to safeguard user data.

And it doesn't stop there. Organizations must also consider other standards like the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and Singapore's Personal Data Protection Act (PDPA). Each framework emphasizes the importance of robust authentication measures to safeguard sensitive data.

By leveraging digital certificates in passwordless authentication, organizations can meet these robust security standards and shield themselves from potential legal liabilities, including steep fines reaching up to 4% of annual global turnover under GDPR.

Demonstrating Compliance During Audits

Demonstrating compliance is an integral part of the regulatory landscape. Traditional password-based systems often make this task cumbersome, requiring meticulous audits of security protocols, configurations, and user behavior logs. Passwordless authentication systems streamline this by maintaining secure and immutable logs of authentication events, all tied to cryptographic proofs of identity. These logs can be easily retrieved and presented during an audit to demonstrate consistent use of robust and compliant authentication across the organization.

Cost Savings

One of the most compelling arguments for transitioning to passwordless security is its significant cost savings. Traditional password-based systems often require substantial resources for password resets, account lockouts, and customer support. According to industry reports, password resets can cost companies upwards of $70 per incident[5]. Passwordless systems substantially reduce or even eliminate these support-related costs by eliminating the need for passwords.

Moreover, the financial impact of a data breach can be devastating. In 2022, the global average data breach cost reached a staggering $4.35 million. And the number is more than double in the U.S., averaging $9.44 million[6].

[4] *Why 2023 is the year of passwordless authentication, Tech Target*
[5] *How Much Does a Password Reset Cost Your Company?, JumpCloud*
[6] *The Devastating Business Impacts of a Cyber Breach, Harvard Business Review*

With conventional authentication, the risk of data breaches stemming from credential theft or phishing attacks is high. Adopting passwordless security considerably lowers these risks, thereby reducing the potential financial liabilities that come with data breaches, which often include immediate monetary loss and long-term reputational damage.

Implementation Considerations

Implementing new technology is always a tricky process, but the more prepared you are, the less likely you will encounter problems.

Assessing Organizational Readiness

Organizations must assess their readiness for this shift before embarking on a journey toward passwordless authentication. This involves a thorough evaluation of the existing infrastructure, which includes evaluating the compatibility of current systems with digital certificates. Organizations must also identify potential challenges, such as legacy systems that may not support newer authentication methods or hardware constraints that could hinder a seamless transition.

Evaluating Existing Infrastructure

A detailed audit of existing network architecture, servers, and endpoint devices is essential. This will help you understand what upgrades or modifications are necessary to support digital certificate authentication. For instance, you might need to update your authentication server to support the X.509 standard for digital certificates if it isn't already equipped to do so.

Moving Ahead with Certificate-Based Authentication

For the actual implementation, organizations should consider how digital certificates will integrate with existing systems and applications. Compatibility issues could arise with legacy systems or custom-built applications. Careful planning is needed to ensure the integration is smooth and doesn't compromise security or functionality.

User Onboarding and Education

Human factors play a critical role in the effectiveness of any security system. For passwordless authentication to succeed, employees must be educated and trained on the new authentication methods. This may involve creating easy-to-follow guides, tutorials, or training sessions to explain how the new system works and what actions they need to take.

Addressing Potential Concerns and Resistance

It's natural for employees to have concerns or resist change. Addressing these concerns proactively is critical. Organizations should prepare FAQs and provide channels for employees to ask questions or report issues. Moreover, demonstrating the benefits—improved security, ease of use, and cost savings—can help overcome resistance.

Overcoming Challenges

Security and Privacy Concerns

One of the primary challenges in implementing passwordless authentication is addressing security and privacy concerns. Organizations must ensure robust data protection and encryption mechanisms are in place to secure digital certificates and the private keys associated with them. Implementing Hardware Security Modules (HSMs) or Trusted Platform Modules (TPMs) can offer an additional layer of security by storing cryptographic keys in a hardware-protected environment.

Ensuring the Resilience of Authentication Methods

Passwords may be a pain to manage, but everyone knows how they work and how to troubleshoot them. Certificates might be new to your IT Team, which means troubleshooting issues might take longer than normal. You also might need a back up plan if a device gets lost or stolen.

Technical Considerations

Integrating passwordless methods often involves dealing with legacy systems not designed for modern authentication mechanisms. In these scenarios, API wrappers or middleware solutions can serve as an interim bridge until the legacy systems are phased out or upgraded. Additionally, planning for authentication failures and recovery options is crucial. Organizations must implement well-defined protocols for re-issuing digital certificates and resetting secure hardware tokens when necessary.

Change Management

Successfully moving to a passwordless system also demands effective change management strategies. Beyond the technical aspects, organizations need to prepare for the human factor. Strategies for managing the transition smoothly include:

- Phased rollouts
- Thorough beta testing with a smaller group before full-scale implementation
- Constant communication with stakeholders to keep them informed and engaged

Gaining Stakeholder Buy-In and Support

Lastly, shifting to a new authentication system requires buy-in from key stakeholders, including executive leadership, IT teams, and end-users. Detailed briefings showcasing the economic and security benefits can be persuasive tools for gaining this essential support.

Going Passwordless with Portnox

A Closer Look at the Portnox Cloud

The Portnox Cloud is the first fully cloud-native zero trust network access control solution that combines the functionality of traditional Network Access Control (NAC) with today's Zero Trust Network Access (ZTNA) solutions.

The importance of zero trust as a philosophy for cybersecurity has come to the forefront in recent years due to the explosion in data breaches. According to IBM, the average cost of a data breach has risen over 15% in the last 3 years to a staggering $4.45 million.[7] Companies can no longer afford to trust that their current security posture is enough; they need to look at a full spectrum of tools to make sure their critical networks and data assets are safe.

The Portnox Cloud is designed with resource-constrained IT teams in mind; thanks to the gold standard 802.1x protocol, it is a truly vendor-agnostic solution that is simple to set up and configure. The benefits of cloud-native architecture mean that there is no constant cycle of after-hours upgrades and patches.

Despite being a simple, set-it-and-forget-it access control solution, the Portnox Cloud boasts a large array of features. Some highlights include:

- Passwordless Authentication
- IoT Fingerprinting & Device Trust
- Secure MAB
- Continuous Risk Policy Evaluation
- Automated Endpoint Remediation
- Guest Access Management
- Integrations with IAM, EDR/XDR, SIEM & more

Leveraging Certificates with Portnox

The three biggest challenges with certificate-based authentication are:

1. **Setting up a PKI (Public Key Infrastructure)**
2. **Deploying certificates to all devices needing access**
3. **Managing the certificate lifecycle.**

Fortunately, the Portnox Cloud is well-positioned to solve these problems and bring the simplicity of setup Portnox is known for – now to certificate-based authentication.

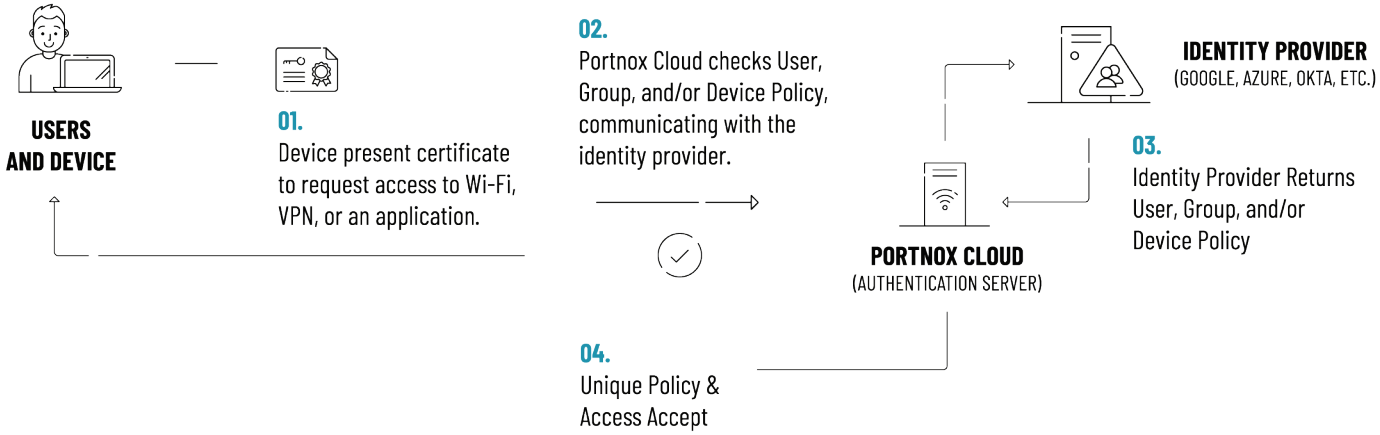
Portnox creates a trusted root certificate for each new organization and acts as the PKI, negating the need for one internally. This also simplifies distribution by giving administrators three easy methods for distributing certificates:

- GPO to distribute AgentP
- Self-service portal
- SCEP (Simple Certificate Enrollment Protocol) server with MDM integration

[7] *Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs, IBM*

One of the great benefits of using the Portnox PKI with AgentP is that it also handles the certificate lifecycle, so when the expiration date is approaching, new certificates will automatically be provisioned and distributed when devices connect.

Organizations that already have their internal PKI set up can still utilize Portnox along with SCEP and MDM to distribute all their certificates by simply uploading their trusted root certificates, although this puts the responsibility of maintaining these certificates on them. However, it is still an easier method of distribution and thus controlling access with a NAC.



Future of Passwordless Security

Emerging Authentication Technologies

As cybersecurity threats evolve, so do the mechanisms designed to thwart them. Two notable emerging technologies in passwordless security are behavioral biometrics and zero-trust architecture.

Behavioral Biometrics: Unlike traditional biometrics, which rely on static characteristics like fingerprints or retina scans, behavioral biometrics analyzes the unique ways in which users interact with devices. This could be the rhythm of their typing, how they move a mouse, or even how they scroll on a touchscreen. Because these behaviors are unique to individuals, they serve as an additional layer of authentication that is difficult to replicate.

Zero-Trust Architecture: This approach operates on the principle of "never trust, always verify." In a zero-trust framework, every request for network access is treated as potentially hostile, whether it originates from inside or outside the network. This adds another layer of protection, requiring robust authentication at every step.

Evolving Threat Landscape & the Need for Continuous Innovation

The nature of cybersecurity threats is constantly evolving, making the need for innovative solutions even more critical. Phishing attacks are growing more sophisticated, malware is becoming harder to detect, and the avenues for attacks are expanding with the rise of IoT and connected devices. This dynamic landscape necessitates continuous innovation in authentication technologies. Traditional password-based systems cannot keep pace with the range and complexity of modern threats, underscoring the urgent need for passwordless solutions.

The future of passwordless security is not static; it will continue to evolve in response to emerging challenges, offering robust, multi-layered solutions for tomorrow's cybersecurity landscape.

Conclusion

Increasingly, passwordless security isn't just an option; it's a necessity. It slashes the risk of phishing, credential theft, and human error. It meets rigorous standards like GDPR and CCPA. Plus, it cuts costs and boosts user satisfaction. This is the robust defense your enterprise needs in a world of escalating cyber threats.

Here's the bottom line. Password-based authentication is fraught with issues, and these issues are only growing as the cyber threat landscape becomes more sophisticated. So get started - explore and adopt passwordless solutions today.

As the cybersecurity landscape continues to evolve, passwordless security promises to be a game-changing force, setting a new standard for protecting networks, applications, infrastructure – and ultimately, people.