atsign

WHITE PAPER

Revolutionizing Network Security with Atsign's Zero Trust Approach

Author: Atsign, Inc.

Date: November 2024

Dear Reader,

In today's digital world, the challenges of securing networks and communication have become more critical than ever. At Atsign, we recognized that existing approaches to network security often add layers of complexity without adequately addressing the root problems. This white paper represents our effort to share a fundamentally different approach to these issues—one that addresses security at the lowest possible level while enabling scalability, simplicity, and resilience.

NoPorts uses our core technology, the atPlatform, to eliminate the need for open network ports, the entry point for cyberattacks. By fundamentally rethinking network communication, we've created a zero trust, privacy-first environment that empowers organizations to embrace digital transformation without compromising security.

Sincerely,

Colin Constable
Co-Founder & CTO, Atsign, Inc.

Executive Summary

Traditional network security solutions, including VPNs, firewalls, and today's "zero trust" models, often introduce complexity and overhead while failing to address a major root problem: open network ports that expose systems with unencrypted or private data to anyone or anything on the Internet (or any IP network). Atsign's innovative approach leverages a global namespace, secure communication protocols, and a robust zero trust framework to:

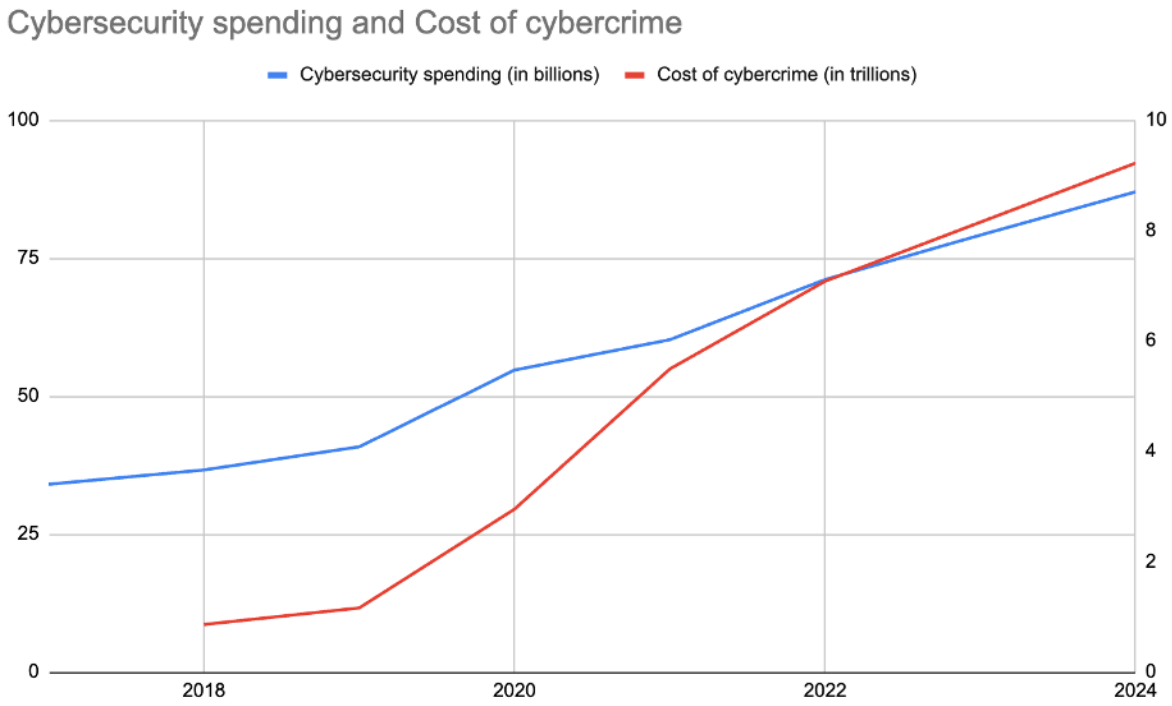
- **Eliminate Open Ports** - Reduce the attack surface significantly.
- **Enhance Security** - Employ end-to-end encryption, ephemeral keys, and customer-generated cryptographic keys.
- **Simplify Network Management** - Streamline operations, simplify firewall rules, and reduce costs.
- **Prioritize Privacy** - Protect sensitive data and privacy.

NoPorts makes network infrastructure and devices invisible, creating a formidable defense against cyber threats. You can't attack what you can't find.

The Challenge of Traditional Network Security

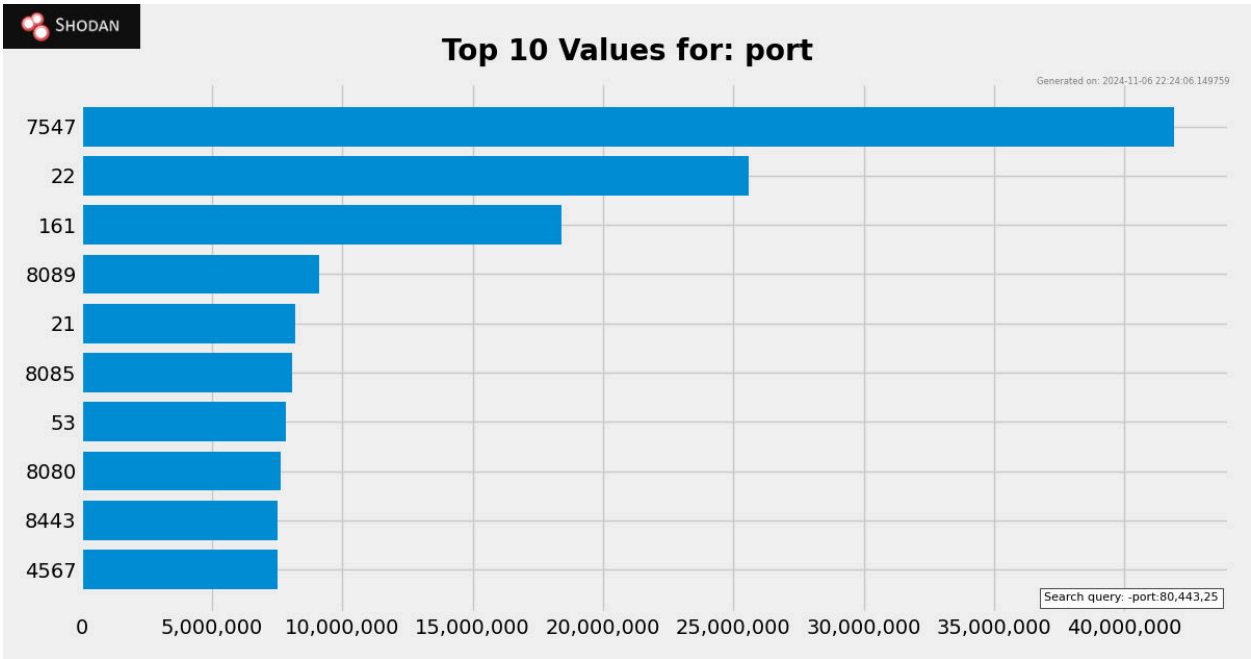
Modern networks are increasingly complex, with a proliferation of IoT devices, cloud services, and remote access needs. Traditional security measures, such as firewalls and VPNs, add more complexity and often fall short, leaving organizations vulnerable to attacks. Even solutions like Zero Trust Network Access (ZTNA), Secure Access Service Edge (SASE), Security Service Edge (SSE), and Cloud-Based Security Deployment (CBSD) are incomplete solutions as they too leave network ports open.

Despite a surge in spending on traditional cybersecurity methods, with Statista reporting a 78% increase from 2018 to 2023, the financial impact of cybercrime continues to skyrocket, highlighting the limitations of traditional defensive methods.



Source: Statista.com Worldwide Cybersecurity Spending and Cost of Cybercrime

The sheer number of open ports worldwide underscores the vulnerability of traditional network security approaches. According to Shodan, there are over 703 million open ports, excluding common ports like 80, 443, and 25. This vast attack surface presents a prime opportunity for cybercriminals.



Source: Shodan.com on November 6, 2024

Atsign's NoPorts Approach

Instead of securing networks by adding layers of complexity, Atsign built a new protocol, the atProtocol, that works on existing TCP/IP networks, and fundamentally changes network communication and security.

NoPorts was designed on Atsign's atPlatform, which consists of three key pillars:

- **Global Namespace** - Every person, device, and entity is assigned a unique, globally addressable identity (an atSign), enabling direct communication without relying on IP addresses or complex network configurations.
- **Secure Communication** - The atProtocol ensures secure, end-to-end encrypted communication between devices, eliminating the need for open ports.
- **Zero Trust Framework** - Atsign's zero trust model enforces strict access controls, ensuring that only authorized entities can communicate.

How it Works

1. **Software Installation** - NoPorts operates using a lightweight software binary that is installed in the user space on devices, whether it's a client, server, or IoT device.
2. **Key Generation and Management** - Devices generate cryptographic keys locally or on the edge, minimizing the risk of compromise.
3. **Identity Verification** - All connection requests are authenticated using public-key cryptography. Once trust is established, NoPorts uses a peer-to-peer connection.
4. **Directory Lookup** - Devices use the directory service to discover other devices based on their atSigns, a unique, human-readable character string that is used as an address and provides a unique, consistent identity across the network.
5. **Secure Connection** - The relay service establishes secure, encrypted connections between devices using ephemeral keys.
6. **Access Control** - The policy engine enforces granular access controls based on identity and context.

Benefits of NoPorts

- **Enhanced Security** - Reduced attack surface, strong encryption, and zero trust architecture.
- **Simplified Network Management** - Eliminates the need for complex network configurations (ex: firewalls only need one rule, reject all inbound traffic) reducing operational overhead.
- **Increased Scalability** - Easily accommodates growing numbers of devices and users.
- **Improved Privacy** - Protects privacy and sensitive data while in transit or at rest.

NoPorts: A New Era of Network Security

NoPorts offers a compelling solution to the challenges faced by organizations today. By adopting a zero trust, privacy-first model and eliminating open ports, NoPorts empowers organizations to build more secure, efficient, and scalable networks.

Both the atPlatform and NoPorts follow the architectural rule of never having ports open where there is anything of value, ports are only open where data is either public or where data is encrypted with keys that infrastructure never has.

Use Cases

Securing Sensitive Data in the Cloud

A leading cloud provider is working with Atsign technology to address the challenges faced by government agencies, particularly the Department of Defense and Intelligence Community, when securely sharing sensitive data. This collaboration focuses on solutions for:

- **Reduced Visibility** - Making remote government assets invisible on the internet, minimizing potential attack surfaces.
- **Enhanced Data Security** - Enabling secure data transfer without exposing data or opening ports on the network.

This approach significantly reduces both operational complexity and security vulnerabilities.

Here's how NoPorts works in this context:

- **atSign Identity** - Cloud services authenticate with a unique identifier, ensuring only authorized users or services can communicate.
- **Relay Service** - This acts as a broker, facilitating communication between services without relying on traditional methods like VPNs.
- **Policy Engine** - This enforces access control rules, ensuring only authorized data exchanges occur.

By combining these elements with a zero trust framework, NoPorts allows seamless and secure communication across diverse environments while minimizing the risks associated with open network ports.

Securing Remote Access for Private 5G Networks

Managing private 5G networks often involves scattered transmitters that require secure remote access for troubleshooting and updates. Traditionally, "backdoor" access points are created, leaving networks vulnerable to breaches. Atsign's NoPorts offers a secure solution. By installing NoPorts software on each Radio Access Network, technicians can access them remotely with zero exposed ports and strong cryptographic authentication. This ensures only authorized devices can connect, maintaining the privacy and security of the entire private 5G network.

Securing AI at the Edge

Deploying AI models across multiple edge devices for real-time video analysis often involves complex network configurations, VPNs, and open ports to securely transmit data to a central server. NoPorts simplifies this process by allowing AI-enabled edge devices to communicate directly with a host server using the atProtocol, eliminating the need for open ports. NoPorts' zero trust model ensures data encryption and contextual access control, significantly enhancing security and privacy. This streamlined approach reduces deployment complexity while maintaining robust security measures.

Secure Data Sharing and APIs

A healthcare data sharing platform provides a secure and efficient way for hospitals, care providers, and insurers to seamlessly share data. Atsign's atPlatform provides the foundation for this platform, ensuring best-in-class privacy and security, but more importantly, easy integration. IT hospital staff understand the importance of securing data. This can significantly slow down data sharing with other healthcare organizations because it often requires network changes and configuration. With the atPlatform, hospitals can be exchanging data with other verified healthcare providers within a matter of minutes, with no IT burden or intervention.

Appendix - More Technical Detail

Atsign Architecture and Components

NoPorts is built upon the atPlatform which consists of the following components:

- atProtocol® - The foundation of Atsign's architecture, enabling the secure, end-to-end encrypted exchange of data without open ports or static IP requirements. It facilitates secure, peer-to-peer communication with minimal configuration.
- **atServer** - The atServer is responsible for managing identity and maintaining the key-value data store for each atSign (Atsign address). It performs cryptographic identity validation to ensure that each entity is who they claim to be, supporting secure interactions. It serves as a secure repository and only holds data that is either public or data that is encrypted with keys it never has.
- **atDirectory** - The atDirectory service helps in locating atServers across the network. It functions like a distributed phonebook, providing the necessary information to facilitate communication to atServers (DNS address and port number).

Additional NoPorts Components

- **Relay** - Provides a TCP session rendezvous point over which encrypted traffic can flow between two endpoints.
- **Policy Engine** - The policy engine governs access decisions based on identity, context, and pre-defined rules. It ensures that all communication abides by zero trust principles, meaning that no entity is inherently trusted, and all access is explicitly granted based on policy rules. This granular control ensures that client/server communication remains secure and is only accessible to authorized entities.

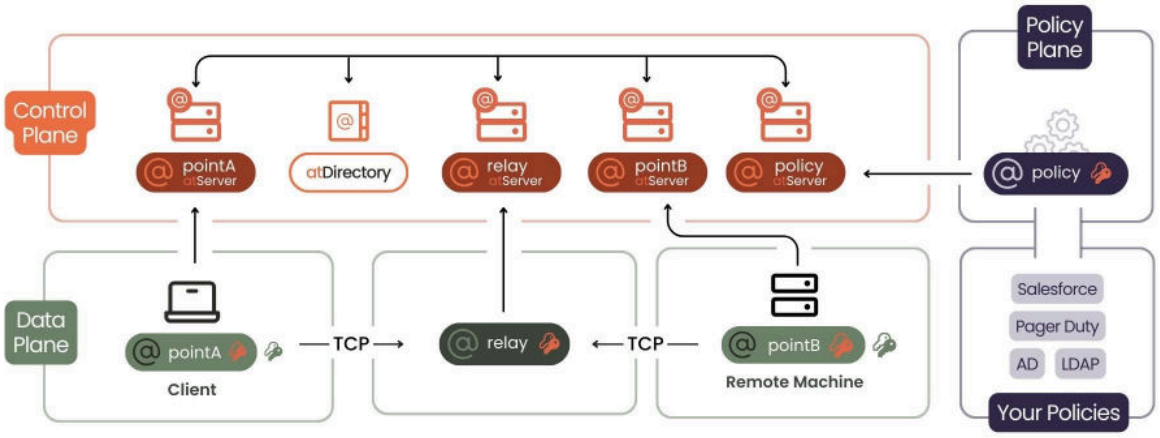
By integrating these components, Atsign provides a control mechanism that keeps all devices invisible to attackers. The use of asymmetric encryption, dynamic session management, and identity-based directory services ensures that devices can communicate without exposing their network details. This approach minimizes attack surfaces and mitigates risks associated with open ports and static IP addresses.

Zero Trust Framework

Atsign's zero trust model encompasses the entire communication flow, ensuring that no device or entity is inherently trusted. Access is granted based on identity verification and contextual access policies.

Atsign's zero trust approach is embedded across the data, control, and policy planes:

- **Data Plane** - All communication and data transfers are end-to-end encrypted, ensuring that data is private and secure at all times.
- **Control Plane** - The control mechanism dynamically manages connectivity without relying on static IP addresses or open ports, utilizing cryptographic techniques such as asymmetric key exchanges.
- **Policy Plane** - Access control is governed by identity and contextual factors, ensuring a granular level of control over who or what can access each resource.



How it Works

Software Installation and Key Management

NoPorts operates using a lightweight software binary or library that is installed in the user space on devices or as a container, whether it's a client, server, or IoT device. Once installed, the first step is generating cryptographic keys—often referred to as "cutting keys." These keys are created directly at the edge, on the device itself, ensuring that private keys never leave the originating device. This significantly enhances security, as

sensitive key material is not transmitted over the network or stored in centralized repositories. This also removes the need for SSL/TLS certificates on edge devices.

Connecting to the atServer

The atServer plays a key role in identity management. When a device or client wants to establish a connection, it authenticates itself using the public and private key pair it generated during the setup. The atServer maintains a secure key-value data store for each identity, holding the public key while the private key remains on the device. This identity verification step ensures that each entity attempting to connect is legitimate and authorized.

Directory Lookup

Once a device has authenticated, it may need to communicate with another device or server. The Directory service assists in locating the atSign identity of the intended target. The Directory functions much like a distributed phonebook that allows devices to discover each other without ever exposing IP addresses or network details of the client, instead delivering the atSigns atServer DNS Address and Port number.

Relay Setup and Secure Connection

The Relay service facilitates the connection between the two atSigns. Upon receiving a request, the relay provides two random ports to the requesting atSign and starts listening on those ports. When the two devices connect to those ports, the Relay authenticates using PKI (public key infrastructure) and connects the two TCP connections. The relay never possesses the ephemeral symmetric key that the client and device use to communicate, which means it can never see the data being exchanged. As the connections are terminated at the relay neither device ever needs open ports.

Access Control via Policy Engine

The Policy Engine is responsible for determining whether a connection should be allowed. When one device attempts to connect to another, the receiving device sends the request to the policy engines atSign.The Policy Engine checks predefined rules based on the identity and contextual information such as location, time, and type of request. The policy engine sends back a binary decision to the device and the connection is made or ignored.

By using a zero trust model, the Policy Engine requires explicit verification for each connection, ensuring that only authorized communications are permitted. This further reduces risk, as every action must be validated.

Keys and Encryption

The keys used for communication in NoPorts include a combination of long-term identity keys (used for authentication) and ephemeral session keys (used for each communication session). The public key is stored at the atServer for identification, while the private key remains on the device. Each session's ephemeral keys ensure that the communication remains secure and that keys are discarded after the session, reducing the potential for compromise.

All data transferred between devices is encrypted end-to-end using AES encryption (AES256 CTR), making it unreadable to anyone who does not possess the correct session keys. The key exchange process itself uses asymmetric encryption (RSA 2048), adding another layer of security to the setup of secure sessions.

The encryption algorithms used can be changed or extended as the whole of the atPlatform uses an abstracted encryption and hashing library. The underlying atProtocol is independent of the encryption layer so is forward compatible with any future encryption algorithm or technology, including quantum and quantum resistant schemes.

Closed Ports and Attack Surface Reduction

NoPorts eliminates the need for open ports like 22 (SSH) or 3389 (RDP), which are entry points for cyberattacks. By removing the requirement for open ports, the attack surface is significantly reduced, as potential attackers cannot scan for or exploit open ports to gain access to devices. All data layer connections are established through relays, with no ports exposed on the client or device to the Internet, thereby massively improving the overall security stance.

Additional Resources:

- NoPorts Documentation
- NoPorts GitHubRepository
- Atsign's OpenSSF Scores (includes atServer & NoPorts reports)
- atProtocol Patent