portnox®

The Building Blocks of Zero Trust Security

www.portnox.com

Table of Contents

What it Really Takes to Achieve a Zero Trust Security Posture

As the cost and frequency of data breaches continue to rise, zero trust has become a priority on the top of every organization's must-do list. In fact, most organizations plan to enable zero trust within the next six months if they haven't already [1]. But with so many zero trust products and strategies on the market, how do you cut through the noise and Get to the core of Zero Trust's principles. Let's get into it.

A Brief History of Zero Trust

Before we can dive into the granular details of zero trust in the modern world, we first need to have a solid understanding of what zero trust is and how it came to be.

Zero trust is a strategic approach to cybersecurity based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter.

The Timeline of Zero Trust

Pre-2004: Cracks begin showing in perimeter-based security

At this time, perimeter-based security was the dominant approach to network defense and had been for decades. Traditional perimeter-based security encloses and monitors a network behind an established perimeter that only authorized users and traffic can access and leave.

However, with cloud services emerging, many network engineers were starting to realize it was no longer safe to assume that organizational data is secure simply because a user's profile is verified. The idea that a trusted internal perimeter puts the company at risk if that perimeter is compromised or an insider turns hostile was starting to take hold.

[1] *https://www.zerotrustedge.com/wp-content/uploads/2021/09/2021-Zero-Trust-Market-Dynamics-Survey-Results-9_10_2021.4-WS-1.pdf*

2004:
Zero Trust is born, but the term not yet coined

The quiet concerns surrounding perimeter-based security were becoming much louder. In a 2004 presentation, Jericho Forum member Paul Simmonds argued that organizations should move toward 'deperimetization' and deploy multiple security controls, including data-level authentication and encryption.

2009:
The term "Zero Trust" is coined

The term "Zero Trust" was coined by Forrester Research analyst John Kindervag in 2009 to represent the sentiment "never trust, always verify."

2011:
Zero Trust gains boost in recognition

Google's BeyondCorp launched an internal initiative to enable employees to work remotely without a VPN. This move garnered widespread attention.

2018:
Forrester and NIST lay some groundwork

Researchers continued to advance zero trust concepts. Forrester launched the Zero Trust eXtended Ecosystem, along with seven core pillars of zero trust. In addition, NIST released SP 800-207, Zero Trust Architecture.

2019:
ZTNA appears

Gartner introduced the terms zero-trust network access (ZTNA) and Secure Access Service Edge (SASE), adding to the available defense layers in the zero trust framework.

2021:
Zero Trust takes off

Microsoft's Zero Trust Adoption Report finds 96% of security decision-makers said zero trust is critical to their organizations' success. The White House also releases a Zero Trust strategy calling for the federal government to advance Zero Trust architecture. In addition, the Cybersecurity and Infrastructure Security Agency (CISA) also releases its Zero Trust Maturity Model.

Challenges and Market Confusion Surrounding Zero Trust

As you can see the bulk of advancements in zero trust happened between 2018 and 2021. This is good news for the security industry as a whole - rapid strengthening of the concepts and subsequent products helps us stay ahead of our adversaries. However, such accelerated change has left many organizations needing clarification about what to buy. Simply put, with everything changing so quickly, there's a worry you might invest in something that will be obsolete in a few years.

Paramount to any successful Zero Trust implementation are these common questions:

- How do we realize Zero Trust collaboration?
- How do we implement Zero Trust across the IT ecosystem?
- How do we integrate Zero Trust into DevSecOps?
- Can we use our current tools to achieve off-network Zero Trust?
- How do we build Zero Trust architecture?

Part of the confusion surrounding zero trust is in its perception. Zero trust isn't a single-packaged solution; it's a paradigm shift. A new way of looking at security through the lens of recent trends including cloud, mobile devices, and remote work. An acceptance that the enterprise perimeter is disappearing. It's a framework, not a product.

[2] *https://www.microsoft.com/en-us/security/blog/2021/07/28/zero-trust-adoption-report-how-does-your-organization-compare/*
[3] *https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf*
[4] *https://www.cisa.gov/zero-trust-maturity-model*

And there are other zero trust misconceptions, further adding to buyer confusion. For example, many people understand zero trust to mean that users aren't trusted and that the organization views them as untrustworthy. This misconception can give rise to push back from users, slowing down the zero trust rollout.

Equally concerning is the misconception that zero trust isn't user-friendly. This leads to the idea that companies must choose between user-friendliness and security. But this is false. Zero trust can enhance user-friendliness by baking usability into offerings as a vital security component – as user-friendly tools are less likely to spark workarounds that drive vulnerabilities.

And perhaps the most worrying misconception is that zero trust is too complex to bother with, an idea often perpetuated by vendors offering a myriad of different solutions. But the truth is, zero trust can be simple. At its core, zero trust is based on a simple concept.

Top Challenges to Zero Trust Adoption

Leadership buy-in and analysis paralysis: Zero trust enables a more agile, productive, frictionless, and secure business environment. However, decision-makers have to understand its value to achieve these goals. At the same time, zero trust is so all-encompassing and broad that many companies suffer from analysis paralysis. They don't know where to begin or how to plan a successful zero trust project.

Industry: Some industries have been quicker on the uptake than others. For example, the finance sector has largely embraced zero trust and is many years into maturity. The White House Zero Trust [5] memorandum requires agencies to achieve specific zero trust security goals by the end of 2024. However, companies in other sectors may believe zero trust is unnecessary or do not understand how Zero Trust implementation works in their industry.

Not all tools are created equal: Cutting through the noise of zero trust products can be challenging. It's essential that companies deeply evaluate the vendor's overall perspective on Zero Trust as well as their ability to provide a platform solution that includes layered, cloud-smart, and data-centric features.

Legacy systems: Legacy systems were built during the time of castle-and-moat perimeter security and may cause friction to effective zero trust adoption.

[5] *https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf*

How Siloed Approaches Fall Short

Faced with disappearing perimeters, many organizations implemented siloed, disparate network security tools to safeguard their systems in a modern cyber landscape. Much of the focus here was on technologies in the Zero Trust Network Access (ZTNA), Network Access Control (NAC), and Identity and Access Management (IAM) spaces. Let's look at each of these more closely.

Identity and Access Management (IAM) is a set of policies, processes, and technologies that help companies manage individuals and devices, authenticate access to data or other resources, as well as monitor who has accessed what. Core features of IAM tools include managing user identities, provisioning and de-provisioning users, authenticating users, authorizing users, reporting, and Single Sign-On (SSO).

IAM projects have been blooming since the 2000s, but many companies today are finding their IAM solutions outdated and inflexible in today's perimeter-less landscape. At the same time, IAM controls without a zero trust approach can spell disaster. Zero trust requires continuous authentication, which is not a core function of most traditional IAM solutions.

Network Access Control (NAC) refers to technologies that enable organizations to implement policies for controlling access to corporate infrastructure. These policies may be based on authentication, users' identity or role, or endpoint configuration. You may be thinking, "why use NAC when you have IAM?". The answer is both simple and complex. Essentially, NAC puts the teeth into IAM - it acts as a crucial control point at the network's edge. It can quarantine devices, kick them off, integrate with unified threat management, connect with other systems to apply access control lists, and more.

Coined by Gartner, ZTNA refers to technologies that support secure remote access to applications and services based on pre-defined access control policies. ZTNA arose as a way to replace VPN-based access, which was too inflexible, lacked granular control, and offered only limited visibility of what remote users were doing on the network. We'll dive more into ZTNA in the next section.

These approaches to network security undeniably played an important role in defending corporate systems. However, relying on disparate tools also leaves worrying security gaps. For example, one study found that nearly six out of 10 businesses report that cybersecurity and identity decisions are separate in their organization [6]. This often leads to sluggish remediation when a data breach occurs. And just how many separate tools are we talking? Well, recent research found that 67% of security professionals work with more than ten different security tools [7].

[6] *https://www.globenewswire.com/en/news-release/2018/08/01/1545340/0/en/Most-Organizations-Risk-Breaches-Due-to-Gap-Between-Identity-and-Cybersecurity-Silos.html*
[7] *https://www.commsbusiness.co.uk/content/news/siloed-cybersecurity-needs-new-approach-says-trellix*

Here's the bottom line. Siloed approaches to network security fall short in the modern day. Today, the average organization uses around 110 SaaS applications, up from a measly eight in 2015 [8]. That's an eye-watering 1,275% increase. These applications, along with APIs, have massively expanded the attack surface and exacerbated security concerns. At the same time, siloed security tools often don't play well together. They may struggle to share information, be based on different cybersecurity best practices, or introduce duplicate features that add confusion. These gaps and complexities make organizations more vulnerable to attack.

The simple truth is that functioning independently, IAM, NAC, ZTNA, and related security controls like Identity and Access Governance (IAG) and Privileged Access Management (PAM) are not enough in a world where a cyber-attack happens every 39 seconds [9].

The Push to Universal Zero Trust, Security's White Whale

Aside from being another term for a Beluga, a white whale is something you obsess over and relentlessly pursue but is difficult to achieve. Universal zero trust is security's white whale. It's the thing security thought leaders doggedly pursue because the benefits are extremely rewarding.

So, what, then, exactly is universal Zero Trust? Simply put, it's a full realization of Zero Trust principles across the IT estate. It's all the benefits of the siloed security tools but with added features and no gaps. It's iron-tight security where automation, continuous authentication, and granular access control reign supreme. But how do organizations achieve this? It's no easy feat, but it is possible and certainly encouraged.

A fully realized zero trust posture will unify security tools like IAM, ZTNA, NAC, PAM, IAG, Network intrusion detection tools, encryption tools, continuous authentication tools (including biometric authentication), firewall tools, and more. It's about centralizing and unifying the security of networks, applications, infrastructure, users, and devices. This kind of unified security improves visibility and allows knowledge sharing across traditionally siloed security layers. By doing this, organizations can achieve boosted security posture, reduce time to detection and remediation, and realize true zero trust.

But zero trust is also about more than just finding the best tools and plugging the gaps. This is where the Zero Trust Maturity Model comes in. This model, developed by CISA, aims to help organizations mature in their zero trust journeys by offering guidelines on what traditional, advanced, and optimal zero trust looks like. You can gauge which part of the journey your organization is in by answering these questions:

[8]the average organization uses around 110 SaaS applications, up from a measly eight in 2015.
[9]https://aag-it.com/how-often-do-cyber-attacks-occur/

Traditional

- Are you using robust authentication methods like multifactor authentication (MFA) and
- Single-sign-on (SSO) to reduce password risks?
- Do you have visibility into device compliance, cloud environments, and logins to detect anomalous activity?
- Have you segmented your networks to prevent lateral movement?

Advanced

- Are you leveraging real-time risk analytics to assess user behavior and devices to make better decisions?
- Can you integrate with multiple tools to correlate security signals across architecture components to detect advanced threats and take fast action?
- Are you proactively searching for and fixing vulnerabilities?

Optimal

- Are you using automated threat detection and response across architecture components?
- Are you actively enforcing dynamic policies after access has been granted?
- Are you analyzing productivity and security signals to find actionable insights and improve the user experience?

Other industry leaders use a five-phase approach to Zero Trust Maturity. These are some of the activities associated with each phase:

1. **Traditional:** Deploying MFA for employees and connecting employee directories to business-critical cloud apps.
2. **Emerging:** Implementing MFA for external users like contractors and business partners. In addition, implementing SSO, enabling self-service for password resets, and automated provisioning and de-provisioning of applications.
3. **Maturing:** Activities in this phase include extending SSO to all authorized external users, building policy requirements around SSO support, enabling privileged access management to cloud infrastructure, and integrating endpoint and cloud application threat feeds into security information and event management (SIEM) tools.
4. **Elevated:** Organizations in this phase will leverage different authentication factors across user groups based on risk, add APIs, implement context-based policies, and deploy tools to modernize legacy technologies.
5. **Evolved:** Implementing secure passwordless access across the IT landscape and making access decisions at the data layer.

Crucially, when organizations reach the evolved stage, they have the basics of identity-first zero trust in order and can focus on further refinements of the security architecture on an ongoing basis.

Technical Considerations of Zero Trust

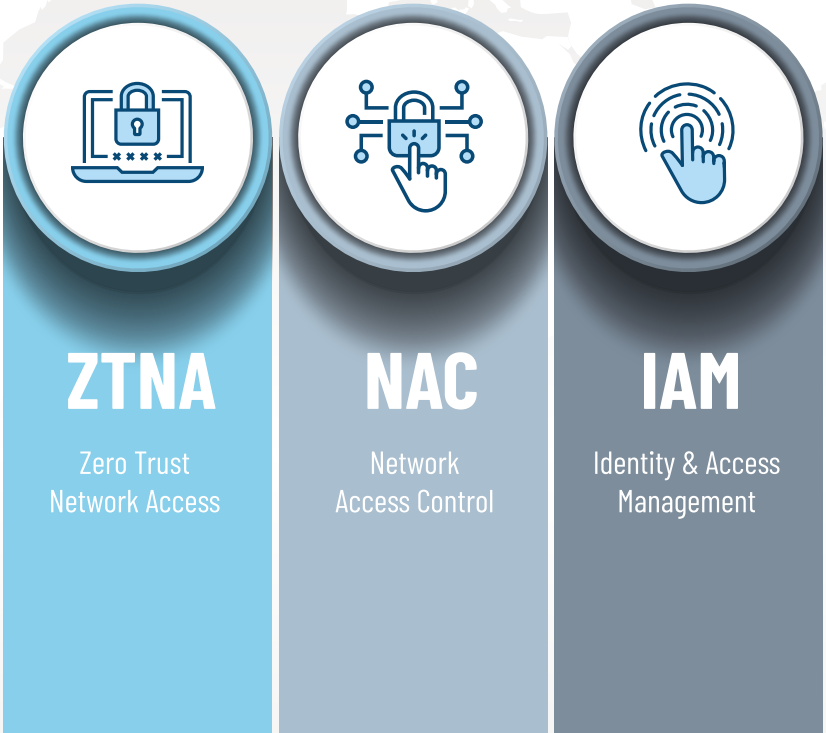
Unified

When an organization begins crafting a comprehensive security policy, it's key to look for a solution that casts a wide net across the key pillars of zero trust. Creating a piecemeal solution adds unnecessary complexity to deployments and risks creating gaps in security policy with disparate tools.

If a tool cannot handle IoT fingerprinting, your risk posture could be expanded by unknown devices on your network. If your network is covered, what about your infrastructure?

Securing a facility is one thing, but addressing BYOD and remote workers adds another level of difficulty. A unified solution that covers all the zero trust bases saves time and frustration with deployment, saves cost with a less complex implementation, and saves frustration on the part of IT staff tasked with walking the fine line between secure and accessible.

The 3 Key Areas of Technologies Needed for Effective Zero Trust



Cloud-Native

Cloud-native has become a popular buzzword in recent years, but it can mean different things depending on who you ask. Here, the term refers to building and running applications to leverage the benefits of distributed computing offered by the cloud delivery model. The move to cloud-native in recent years has dramatically altered software development and allowed organizations to exploit the resiliency, scale, elasticity, and flexibility that cloud delivery models offer.

Fundamental principles of cloud-native architecture include microservices, containerization, continuous integration, DevOps, and agile methodologies. But how do we approach zero trust in a cloud-native world? First, cloud-native architecture is compatible with unified zero trust.

For example, cloud-native zero trust solutions don't rely on any particular traditional network connections. Instead, they keep track of the activities specific users, applications, devices, and services should be able to do when interacting with any endpoint. It achieves this by fingerprinting applications and users.

Cloud-native zero trust also leverages machine learning (ML) and automation to reinvent network micro-segmentation. Simply put, it's no longer feasible to manually (or even programmatically) handle micro-segmentation policies in a cloud-native world. Instead, these emerging solutions leverage ML with zero trust principles to continually create and modify colossal numbers of individual policies to effectively verify the identity of each user, device, and application in the network.

Cloud-native technologies are preferred for many reasons, one of them being the vastly reduced maintenance burden on security teams and end users. And a fully actualized zero trust model only furthers this by leveraging automation in all the right places.

Friction-Less

Another consideration when embarking on your zero trust journey and considering various products is how well those products will play with your existing architecture. You should opt for solutions that work with your existing infrastructure without requiring significant changes.

Many legacy zero trust solutions are locked into a specific vendor, solution, or protocol that is not necessarily universal. The reality is most organizations have an existing infrastructure that is made up of multiple vendors; even if you build your network with the intent to stick with one specific solution, a buyout or an acquisition may result in a sudden expansion of vendors and equipment.

Therefore, it's important to look for a solution that relies on tried-and-true standards like RADIUS and 802.1x; you would be hard-pressed to find a device that did not offer support for these two gold-standard protocols. This will make deployment and scaling infinitely easier, since there will be no danger of having to wait for complex workarounds or spend hours on the phone with support trying to make a solution work for a broader range of devices than it was designed for.

What's Next For Zero Trust?

Zero Trust is a dynamic model that will continue to evolve as time goes on. The zero trust of today will look different from the zero trust five years in the future, just like today's zero trust looks different from 2018's. But what changes can we expect to see?

Zero trust's focus will continue to shift from securing individual security pillars to policy unification across pillars. Moreover, threat intelligence and automated responses will empower security teams with the knowledge and time they need to detect, deter, and defeat critical attacks.

And as we progress further into a cloud-native future, software and DevOps processes will be tightly informed by zero trust principles. For example, developer access to code and development tools will use just-enough-access and just-in-time features to minimize exposure of sensitive information and resources. At the same time, native integrations, built-in connections, and configurable APIs will empower organizations to realize zero trust without needing to retrofit applications.

Zero trust is paramount for security teams and the wider business, and reaching zero trust maturity should be a top priority for any security-conscious organization in today's hostile threat landscape.

Portnox & Zero Trust

Finding a comprehensive zero trust solution may seem like a herculean undertaking, especially as vendors scramble to encompass to reposition their solutions as part of the zero trust equation - sometimes trying to force a square peg into a round hole. Portnox's cloud-native zero trust access offering has emerged as a leader that encompasses all the key elements of zero trust with all the advantages of a cloud-native platform.

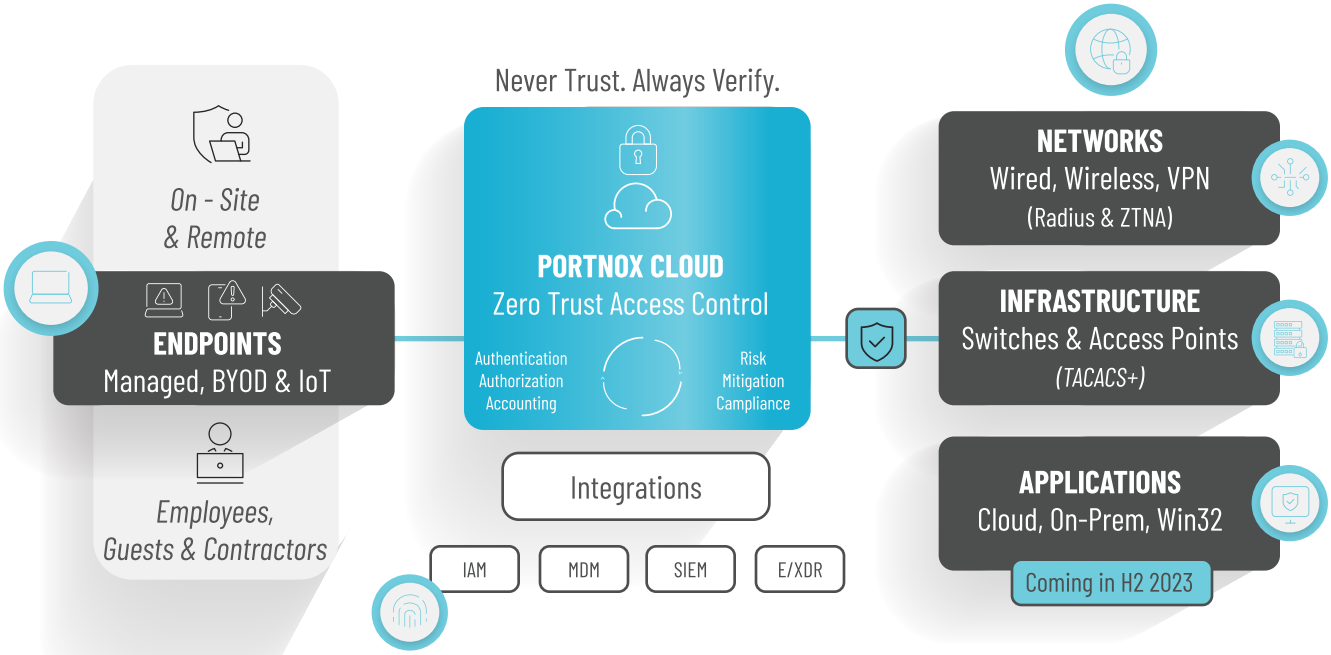
Key zero trust features of Portnox:

- Integration with Identity Providers - Portnox works with existing Identity providers such as Google, Azure, Okta, and more. It's well known that having multiple, complex password requirements often results in users' partaking in unsafe behaviors like saving them in an unencrypted text file or writing them on white boards in public conference rooms. Identity Provider integration means simplicity for both users and IT teams in managing network access.

- Role-Based Access - A key component is making sure that only those who need access to certain resources as part of their job function have access to those resources. Looking at several recent high-profile data breaches (Cisco, Uber), the ability to gain entry and then move laterally through the network played a large factor in the amount of damage that was caused.

• IoT Fingerprinting - Internet of Things devices - from your Fitbit to your Fridge - are growing exponentially in popularity. In fact, by 2030 estimates are that over 24 billion devices will be connecting to the internet - devices that are notoriously difficult to detect. In fact, one study showed 80% of IT departments found IoT devices on their network they were not aware of. Portnox offers a unique fingerprinting method that requires no on-prem installation and recognizes over 260,000 devices across 27,000 brands

Portnox zero trust access control

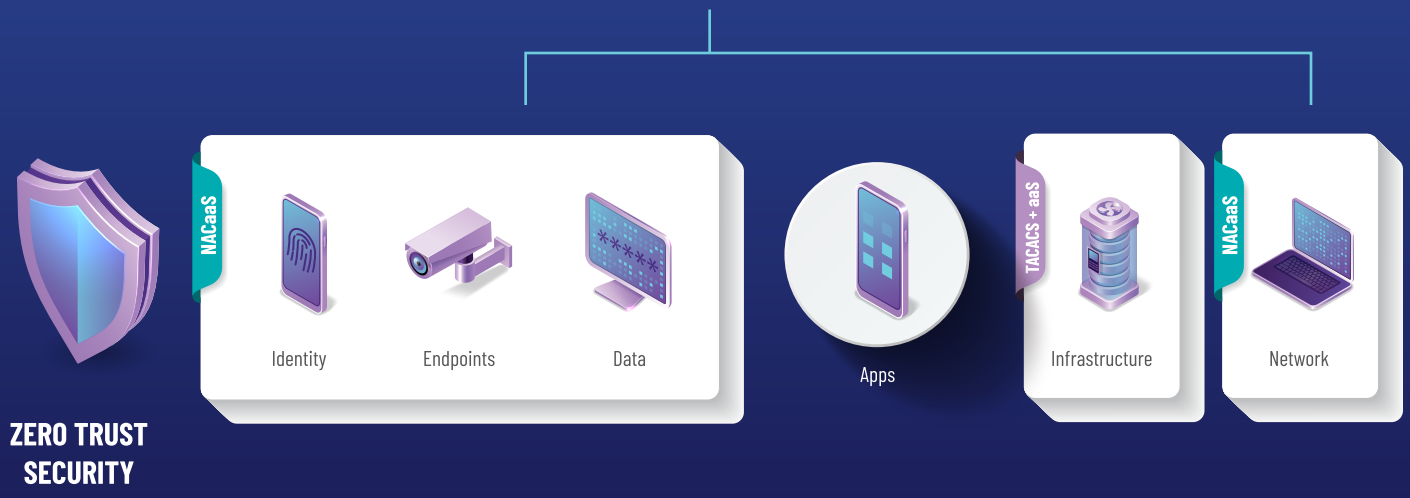


• Risk Assessment - Portnox's policy creation options allow you to set criteria for risk - a phone with no passcode, a laptop with no firewall - and then choose what to do based on the cumulative risk score, from quarantine to outright deny access. Risk scores are regularly calculated - not just when a device connects - so if something changes, you'll know about it via an alert or a nightly report.

• Automated Risk Remediation - Calculating a risk core is valuable, but what do you do with risky devices? Portnox makes it simple through automation beyond just quarantining and denying access - automatically force the device to update the antivirus software, start a firewall, start/stop a service, run a script, and more with automated risk remediation.

• Security Integrations - As we detailed above, it's imperative that your solutions work together vs. operating in a silo. Portnox uses the REST API to connect with tools from Splunk, Sumo Logic, SolarWinds and more.

Portnox covers



Portnox offers all the benefits of a truly cloud-native solution – with no requirement to install on-premise software, the pressure of maintenance and upgrades is removed from IT staff. New features are deployed to immediate benefit without needing to schedule downtime for an upgrade to take advantage of them. Additionally, being vendor agnostic means there is no requirement to change or replace hardware to implement the solution.

There are many more features that make Portnox a winning solution, which can be explored at portnox.com

[10] *https://www.zipitwireless.com/blog/future-of-iot-what-to-expect-in-the-next-5-years*
[11] *https://blogs.infoblox.com/security/what-is-shadow-iot-how-it-teams-can-defend-their-networks/*

portnox®