The IT Admin's Guide to Evaluating Network Security Solutions

How SMBs can cut through the marketing jargon to get what they need

Introduction

There's a lot of noise surrounding cybersecurity (and network security) solutions – some helpful, some harmful. And often, this noise centers around large enterprise businesses, leaving small and midsize businesses out of the conversation completely.

Unfortunately, **cybercriminals and bad actors know better than to spare SMBs from their plans**, targeting businesses with fewer than 500 employees constantly. In fact, **61% of SMBs reported being hit by a successful cyberattack in 2023**.

Meanwhile, the cybersecurity industry is continually consolidating through acquisitions. These deals have led to a boom in "end-to-end" platforms bundling security solutions across a broad range of functions. All the while security leaders are stretched thin and looking for both simplicity and scalability without needing to spend a lot of time on implementation, administration, and the purchasing process. No wonder the great CISO resignation is a real thing!

With constant vendor consolidation in cybersecurity, changes to security requirements, ever-evolving frameworks, and continually emerging threats, **how can you protect your business without adding extra stress – or cost? That is what we hope to help you accomplish in this book.**

In this book, we will discuss:

- The current threat and cybersecurity landscapes.
- What consolidation of vendors means for SMBs.
- Why (and how) to choose between point and platform solutions.
- How to vet potential vendors and find best of breed solutions within your budget.
- Questions to ask before you start shopping for vendors.
- How to make sure point vendors will work well with your current tech stack.
- A checklist to use for note-taking while comparing vendors.

It's important to remember that not every solution is right for every single business. However, there is value in seeking tools tailor made for small and midsize businesses, and that's what we hope to help you accomplish.

Now, let's cut through the chaos of cybersecurity and get started.

There's a lot of noise surrounding cybersecurity

"The business VPN is dead!"

"ZTNA is what you need!"

"ZTNA won't protect you, you need SASE!"

"SSE is way better than SASE!"

"Are you even considering SDP?"

"Anything but another point solution, please!"

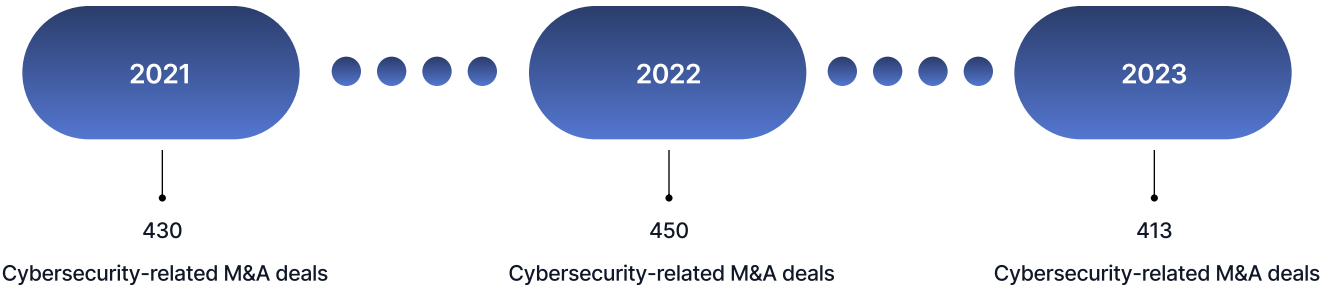
"Point solutions are way better than platforms."

"Why would I need to think about network security, isn't that part of my company's package from that big platform provider?"

Contents

The IT Admin's Guide to Evaluating Network Security Solutions

Part I: To platform or to point – that is the question.



To point, or to platform?

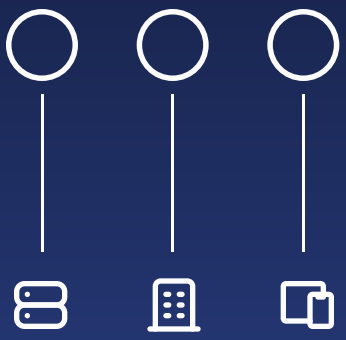
Continual consolidation in the cybersecurity industry means there are now fewer unbundled solutions. Through these mergers, many of these companies lean into the promise of so-called "all-in-one platforms," creating a simplified security strategy for their customers. **(Spoiler alert: simplified is not always the case.)**

These evolutions have different implications for your business. When you look at any solution, you'll need to ask yourself:

- Does it make sense to go with a vendor proclaiming "all-in-one," or are there very real benefits to using best-of-breed point solutions?
- Is convenience worth sacrificing other elements?
- If so, what are the elements you'd be sacrificing?

Defining a point solution vs. all-in-one platform

Point Solution



Point solutions refers to software or application that was created to solve a specific set of use cases or pain points in a specific area of business. But don't let the name fool you – just because a point solution was created with an intended use case doesn't mean it is tied solely to that use case or unable to move beyond the traditional bounds of that use.

For example, while OpenVPN can be applied to several use cases, the main objective is to provide secure remote access for businesses with a hybrid workforce.

VS

Platform Solution

An all-in-one platform refers to a platform that provides multiple solutions housed in one place, sometimes managed by a singular company or contract, and sometimes built or connected through acquisition.

You may see these solutions use the marketing term "end-to-end solution" or "consolidated vendor" to describe their services.

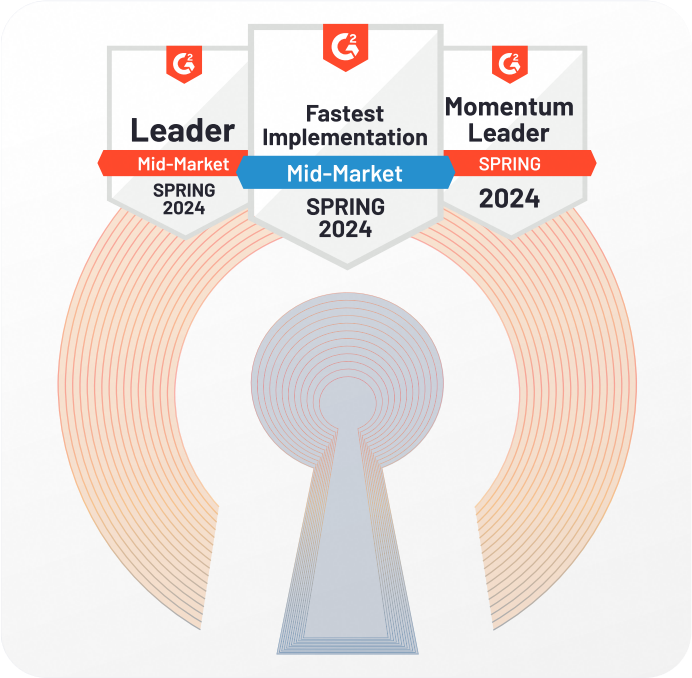
For example, if a vendor offers a "next gen firewall" (one component) that offers firewall, VPN, and malware protection all in one system, managed and configured as one, is a platform.

It's important to note that when we talk about a consolidated vendor, we are not talking about a managed service provider, or MSP, like the ones in our Partner Network.

The benefits of a point solution in a platform world

1. Point solutions can harness "Best-of-Breed" technology

One of the benefits of an all-in-one platform is that you don't have to think about your choices – because **with a consolidated platform, you don't actually have them**. And it is that lack of choice that can hold you back from accessing cutting-edge innovations and best-of-breed technology that can level up your security (and do so at a competitive price).



Companies with a hyper-focused approach to network security for their customers' specific pain points can often put **more time and resources into creating a top-of-the-line solution** that caters to your business size. A best-of-breed solution may have more robust features and more detailed reporting than a feature set that's part of a more extensive suite of products.

Because many unbundled solutions (like OpenVPN) are independently operated, there is a greater drive — and investment — to create a product that goes beyond something that is simply "good enough" or a part of a collection of "good enough" solutions. Additionally, the team building the product is more likely to be experts in the specific technology they are building, offering an edge that helps get the product right — and gets it in the hands of the right people.

When you have a consolidated platform, you're limited to the vendor's product roadmap which may not provide resources or investment into the necessary measures to make it best of the best. The pervasive "if you build it, they will come" mentality of larger consolidated enterprise platforms may mean you are buying capabilities you don't actually need, sacrificing speed and security for these "features" with a lack of investment in cutting-edge technology.

The benefits of a point solution in a platform world

Real World Scenario

You purchase a bundled platform that started as primarily a threat intelligence company. Through a series of acquisitions, that platform now offers breach response, firewall, VPN, and supposed ZTNA solutions. The company's primary investment is still in threat intelligence, with fewer resources dedicated to the rest of the suite. As a result, you get bare-bones capabilities for your breach response, firewall, VPN, and ZTNA efforts. **You aren't getting best-of-breed software, and you're paying more for mediocrity.**

Let's say when you initially signed up for the threat intelligence vendor, you only needed a great threat intelligence tool. But, through the mergers and as their business grew, you're a prime target for upselling. As more mediocre solutions in their platform are piled on, you begin to lose trust in their original software, which was working well until their resources became stretched too thin. Not to mention you're then dealing with a sales push to rip-and-replace your existing stack that has also been working well.

You might also find that these platform companies move more slowly to make significant changes to their UI or functionality. So, while you are bundling and getting the bare minimum, you are also unlikely to see those necessary changes that you could expect from a more agile point solution.

In short, it's a recipe for frustration.

The benefits of a point solution in a platform world

2. Better scalability: pay only for what you need without vendor lock-in

"As many as 90% of companies are overpaying for their SaaS products by 20%-30%."

- TechCrunch

Let's talk turkey: **Point solutions give you the freedom to pay for what you actually need**, with the ability to scale up or down as your business grows and evolves – ultimately optimizing your network security budget.

When you choose a point solution,you pay for only what you actually need and are less likely to overpay for features that don't serve your goals. These savings can mean the difference between having all of the software you need to protect your business or having to choose between which capability is most important (leaving you vulnerable to cyber attacks).

At the same time, you'll save money on deployment because you will only need to configure features you will actually use rather than spending hours on a complex deployment for features you don't actually need.

In short: With a point solution, **you'll find more of the "Goldilocks" solutions you need** — *within* your budget — than you ever would with a more expensive bundled platform targeting much larger enterprises.

Food for Thought

Point solutions prevent potentially costly vendor lock-in, which can leave you in a more vulnerable position financially if your singular provider of all security implements a rate hike.

Ultimately, when you have the freedom and flexibility to choose individual solutions, you can take advantage of a more competitive market.

The benefits of a point solution in a platform world

3. Shrink your attack surface

$10.5 trillion

Predicted annual cost of damage from cyberattacks by 2025, according to McKinsey

+300%

Predicted increase in annual damage from cyberattacks between 2015 and 2025

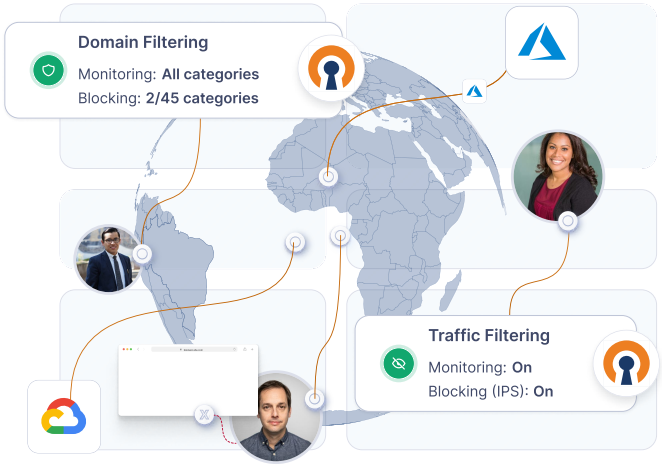
62%

Number of organizations that report their attack surface has grown from 2021-2023

One of the greatest advantages of point software is often the most underestimated: Platform solutions create a larger attack surface while **point solutions allow you to create a smaller, more segmented attack surface.**

Larger, consolidated vendors often have bigger targets on their backs. After all, if they are the primary — or in some cases *only* — IT software vendor for a company, one attack represents a large-scale risk for their customers. For example, they may be more prone to distributed denial-of-service (DDoS) attacks or targeted botnet attacks that allow bad actors to infect other parts of the business. However, a more segmented attack surface will work to prevent the DDoS attack and ultimately quarantine the botnet attack, preventing lateral movement.

You can start reducing your attack surface by simply creating multiple points where a breach can be detected and stopped. For example, you can look for specialized solutions with frequent internal security audits, like secure remote access, to block threat actors as much as possible. Not only does this create fewer points of entry into your secure systems, but it also prevents lateral movement within potentially connected systems.



Source: Enterprise Strategy Group Research Report: Security Hygiene and Posture Management Remains Decentralized and Complex Jul 21, 2023

The IT Admin's Guide to Evaluating Network Security Solutions

The benefits of a point solution in a platform world

Real World Example(s)

Cyberattacks and attack surface risk aren't just hypothetical.

Take, for example, the 2024 Ivanti VPN vulnerabilities that allowed bad actors to access other areas of their platform, creating a major risk for users of the Ivanti platform.

In January, Ivanti uncovered two zero-day vulnerabilities that allowed an authenticated administrator to send crafted requests to execute code on affected appliances, bypassing authentication. Mere weeks later, two more zero-day vulnerabilities were uncovered. These included a privilege escalation vulnerability and a server-side request forgery in the SAML component. These allowed attackers to access certain restricted resources without authentication.

In other words, **these vulnerabilities were the equivalent of hackers walking in through an unlocked front door** and putting entire businesses at risk.

The benefits of a point solution in a platform world

4. Eliminate a single-point-of-failure

$7.75 million

Median cost of IT outages with high business impact

$100,000 per hour

Cost of IT outages to organizations reported by 3 in 5 technologists

$500,000 per hour

Cost of IT outages to organizations reported by 1 in 5 of technologists

$1 million per hour

Cost of IT outages to organizations reported by 1 in 5 of technologists

System outages are not cheap

For the same reason that using multiple specialized solutions reduces your risk of cyber attack, it also **reduces your risk of a major system failure, outage, or widespread scheduled maintenance that hinders your teams' productivity.**

Especially in network security, avoiding a single point-of-failure is not only important for productivity, but for protecting your business from a breach.

Let's say that you use an all-in-one vendor for your IT infrastructure. When that vendor has a system flaw that causes an outage or widespread latency, your entire team could be stuck waiting for a solution - costing thousands of dollars in time - while bad actors are able to target your business.

Essentially, if that happens, you're a sitting duck. But with an unbundled solution, you can work around the point-of-failure (and reach the support team more easily) until it is resolved more easily.

Benefits of bundled platforms

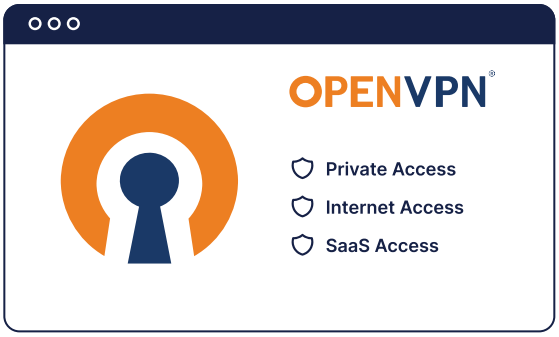
Convenience	Simpler Training and Implementation
In the Gartner® Top Trends of 2023 Report, analysts stated, "Organizations desire less complexity, simplify operations and make their staff more efficient. Vendors are consolidating into platforms around one or more major cybersecurity domains." This doesn't always amount to better productivity. Rather, it amounts to fewer things to manage – fewer contracts to keep track of, a one-stop-shop for product support, and perhaps a more seamless integration process since much of your existing tech stack will be eliminated.	When you use a larger, consolidated enterprise software, there's a good chance that you'll be able to train your team all at once on that suite of software. You may be sold on a simpler implementation process as well, as software and processes may be deployed all at once. However, that doesn't necessarily mean you'll gain speed on the implementation or training process with an all-in-one vendor. In fact, you may find quite the opposite. When migrating large amounts of data from one software to another, there is a risk of broken or missing data hindering the process.

The IT Admin's Guide to Evaluating Network Security Solutions

Part II: What the... acronym? How to understand popular network security frameworks and discover what's right for your SMB.

The growth of cloud services makes it easier than ever for small and mid-size businesses to create information technology (IT) infrastructure without breaking their budgets. But like all businesses, SMBs face an increasing number of threats.

But it's not all doom and gloom. Operating an SMB is a labor of love, albeit one that often doesn't afford the luxury of a full IT team that enterprises may enjoy. Knowing which threats you're facing — and the best technologies and strategies to thwart those threats — can help.



43% of cyberattackers

Targeted small businesses in 2019*

60% of SMBs

Were victimized by a cyberattack in 2021*

61% of SMBs

Reported being hit by a successful cyberattack in 2023**

58% of of SMBs attacked

Experienced significant downtime in 2023**

39% of SMBs attacked

Lost customer data in 2023**

*According to Security Intelligence
**According to a survey conducted by BlackFog.

Most common cyber threats in the U.S.

The U.S. Small Business Administration (SBA) reports that the following are the most common cyber threats for small businesses:

Phishing:

This popular social engineering method tricks recipients into clicking malicious links, thereby providing hackers access to their networks, or divulging Personally Identifiable Information (PII) or sensitive company data like credentials or financial information. Phishing attacks exploit human error by preying on human emotions and negligence rather than system vulnerabilities.

Learn More

Malware:

Malware, or malicious software, is any computer software with malicious intent. A malware attack often stems from a phishing email. Once a malicious actor has access to your network, you'll need to contain the threat and prevent lateral movement. Failure to do so can lead to a ransomware situation.

Learn More

Ransomware

Ransomware is a malicious program that encrypts data on your device and typically demands a payoff in return for the decryption key. An epidemic of ransomware attacks has gotten so serious that Biden administration officials deemed it a national security threat. The key to stopping ransomware is to get better at identifying and isolating threats earlier on in the cyber kill chain. This can be done with:

- Email security to detect malicious payloads.
- Improved staff training to help spot phishing emails.
- A risk-based patching program to remediate vulnerabilities before they can be exploited.
- Detection and response tools at the endpoint, and across the IT environment, to spot suspicious behavior before malware or ransomware is installed.

Learn More

Spyware:

A type of malware, spyware infects a user's device and gathers info, including usernames and passwords. If an employee's device is infected, a bad actor can use stolen login credentials to access your company network. Endpoint protection can help detect spyware in its most common form, adware, but employee education is your best bet to prevent spyware in the first place.

Learn More

Choosing a cybersecurity solution for SMBs

NIST Cybersecurity Framework

Before you choose any cybersecurity solution, take time to review the NIST Cybersecurity Framework. This risk management methodology focuses on five functions — Identify, Protect, Detect, Respond, Recover — that will help you get a high-level understanding of your cyber risk and the security solution your business needs.

According to NIST, the five Framework Core Functions (outlined below) "... can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk."

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

In light of the NIST Cybersecurity Framework Core Functions — and the fact that business networks face the biggest threats — **the most popular security solutions are VPN, ZTNA, SASE, SSE, and SDP.**

The IT Admin's Guide to Evaluating Network Security Solutions

Virtual Private Network (VPN)

A Virtual Private Network (VPN) gives your business a securely encrypted connection to your private network over the public internet. VPN protection is an important piece of a layered security protocol that protects both company data and personal employee data in motion. Using a VPN service gives you the ability to remotely access important network resources and connect your company's branches and locations worldwide. A VPN can be used for site-to-site networking and/or secure remote access. Additionally, a VPN can provide split-tunneling to help protect your team without slowing down their network speed.

Zero Trust Network Access (ZTNA)

ZTNA is a strategy that creates identity- and context-based access boundaries, hides apps, and restricts access to only those who need it for their essential job functions. Doing this hides the apps from discovery and restricts access using a trust broker and a set of named entities. The broker verifies users based on identity, context, and policies — and stops lateral movement in the network. Because application assets are removed from public visibility, the potential attack surface is reduced.

However, it's crucial to note that ZTNA is not any one singular product or service, rather it is a collection of services and solutions that work together to accomplish the principles of zero trust and least privilege.

Instead of enforcing a physical network perimeter, ZTNA enforces a perimeter that extends to user endpoints.

There are three basic principles of ZTNA:

- **Explicit verification** — Each user and machine log-in must be verified using two-factor authentication (2FA) or multi-factor authentication (MFA). No access is permitted until requests are fully authenticated.
- **Use of least privilege access** — No single user or account has access to all data. Not even high-level employees, management, or executives. Each user is assigned the permissions required to fulfill their tasks — nothing more.
- **Assume data breach attacks are underway** — Network administrators and IT teams operate as if each connection is a potential threat. No user is trusted unless authenticated, as possible injections and other attacks could be hiding on the network and have yet to be discovered.

> *There is a harsh reality beneath the glossy sheen of this buzzword: No single ZTNA technology can deliver a zero trust framework. Zero trust is a comprehensive mindset that challenges the very foundations of traditional security models, one which takes time, patience, and dedication to properly build up.*
>
> - Francis Dinha
> CEO, OpenVPN

The IT Admin's Guide to Evaluating Network Security Solutions

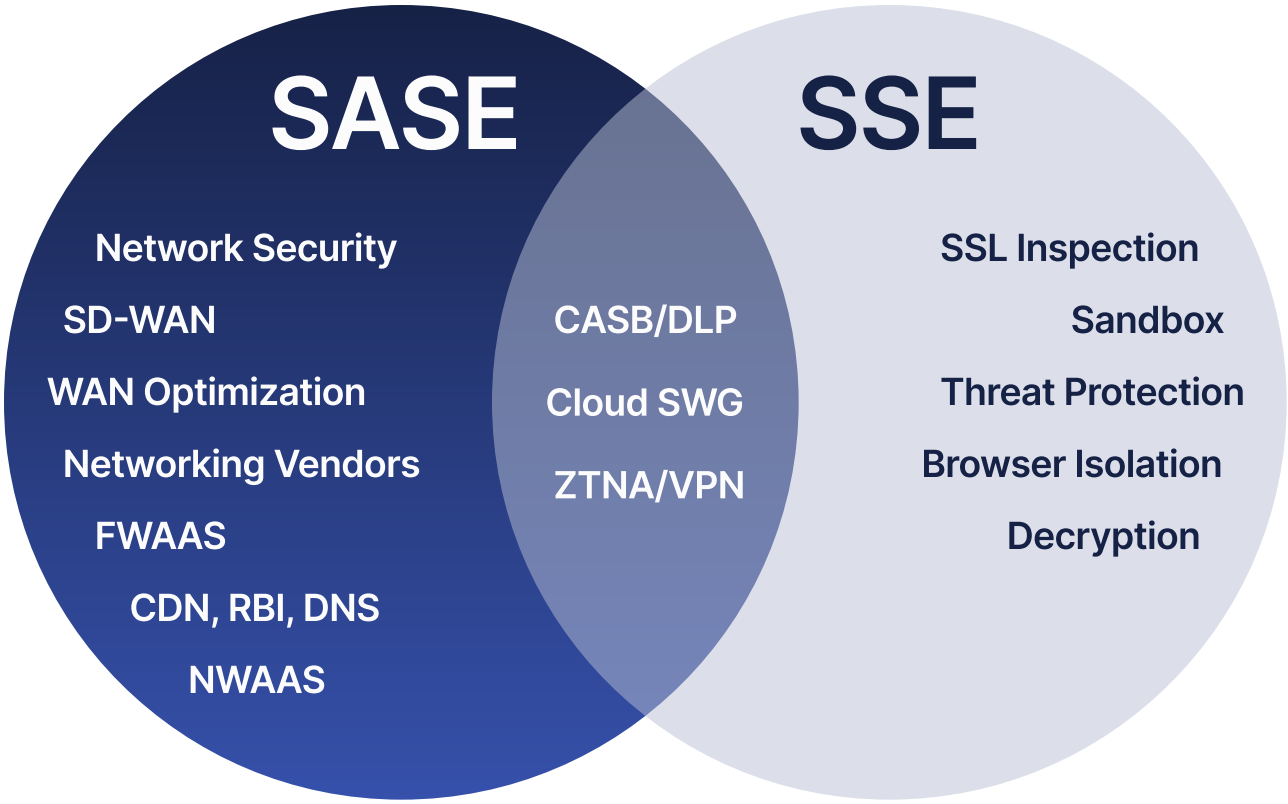
Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE)

The Secure Access Service Edge (SASE) model combines network security functions – such as SWG, CASB, FWaaS, and ZTNA – with WAN capabilities (i.e., SDWAN) to support the dynamic secure access needs of organizations. These security capabilities are delivered primarily as a service (aaS) and based on the identity of the entity, real-time context, and security/compliance policies.

SASE solutions move cybersecurity from data centers to the network infrastructure to create a converged security model. The individual security services that create a SASE platform are:

- **Software-defined Wide Area Network (SD-WAN):** Applies software-defined networking (SDN) to large-scale WAN for improved agility and app performance as well as easier management.
- **Cloud Access Security Broker (CASB):** Software (on-prem or cloud-based) between cloud users and cloud apps that monitors activity and enforces security policies.
- **Next-Generation Firewall (NGFW) and Firewall-as-a-Service (FWaaS):** This goes beyond protecting against threats by completely blocking malware before it gets into your network.
- **Zero Trust Network Access (ZTNA):** Creates a concealing, secure perimeter around application(s) with identity- and context-based access to reduce the potential attack surface.
- **Secure Web Gateways (SWG):** Detect and prevent threats, unauthorized access, and malware using a digital barrier and filter between a website and end-point device. This blocks access to potentially harmful sites in addition to cyberattacks.



Security Service Edge (SSE)

SASE originated with Gartner in 2019, but there aren't many full SASE vendors. That's why, in 2021, Gartner introduced a new term: SSE (Security Service Edge).

This subset of SASE services focuses mainly on the security access of SASE, dropping the WAN networking components. SSE comprises security services — SWG, CASB, ZTNA — but excludes SD-WAN, QoS (Quality of Service), and WAN optimization. SSE's inability to provide SD-WAN on its own is the critical difference. SSE-related network capabilities include ZTNA, and because near-term cost is lower, SSE's focus on security may win out over a SASE solution.

Software-Defined Perimeter (SDP)

A software-defined perimeter (SDP) conceals Internet-connected infrastructure, hosted either on-premise or in the cloud, so it's invisible to unwelcome outsiders. Authorized users, though, can still access the hardware and software that enable network connectivity and communication between users, devices, apps, and the internet.

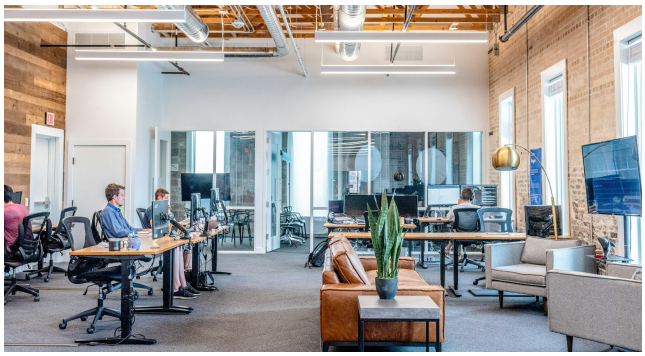
Part III: Guidelines for vetting vendors

Questions to ask yourself before you move into vendor evaluation

Now that you've decided between platforms and point solutions and what types of security solutions you may need, you may be asking yourself where to begin with evaluating different network security vendors.

Note: this guide and checklist can be used to evaluate vendors beyond network security.

To help narrow the field, begin by addressing the following questions within your organization. Answering these questions internally will help gauge your organization's needs, maturity, and security posture — and will help you hone in on the solutions that may be able to meet your needs. You may not have the answer to some of these questions, and that's okay too. However, these can serve as a baseline as you move through the buying process with a point solution of your choosing.



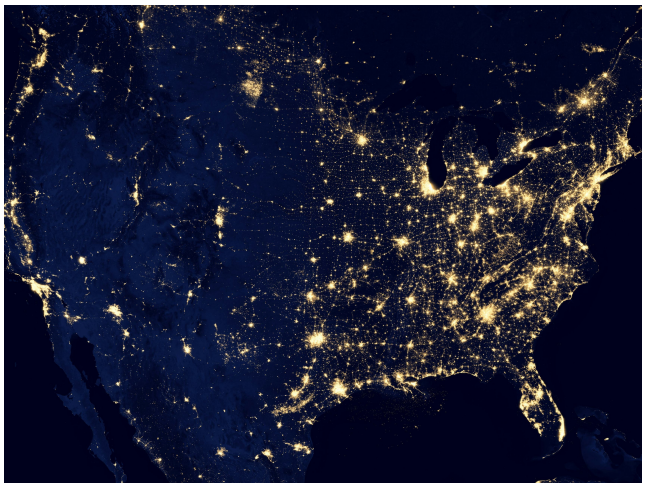
Questions to Ask

1. What is your budget? Will your business be looking for ways to save on costs in the future?
2. Does your business have a current secure remote access tool? If so, what purpose does your current service serve today, and what are you looking to accomplish?
3. What types of assets are you looking to protect? Are the majority of your assets or applications in a SaaS or cloud environment?
4. What is your overall work environment like – is the majority of your team fully remote, hybrid, or fully in-office? Will you need a remote access VPN? Does your team routinely use public wi-fi or private routers?
5. Depending on the prior answer, do you see a need for a VPN tunnel from the employee or remote user workstation to your cloud/datacenter, or is routing your primary concern?
6. Are your workstations domain-joined, or are they part of a workgroup? If so, do they talk to something like Azure or an on-prem active directory? Do you have a firewall in place?
7. Do you believe that you will need more (or fewer) connections in the future?
8. Does your security planning now, or will it in the future, require Zero Trust Network Access (ZTNA) tenets?
9. Do you have any other cybersecurity tools that require an integration with your VPN or secure remote access tool?

Cut through marketing jargon: What you should look for in a network security vendor

Now that you've asked yourself the questions on the previous page, what do you do with that information? For example, you know you need a VPN or ZTNA solution, but what else should you consider?

Before you begin perusing the websites of your potential vendors, **we have compiled a list to help you cut through the marketing speak. Let us help you find the solution that works with, not against, your goals** while avoiding expensive shelfware.



1. Flexible pricing

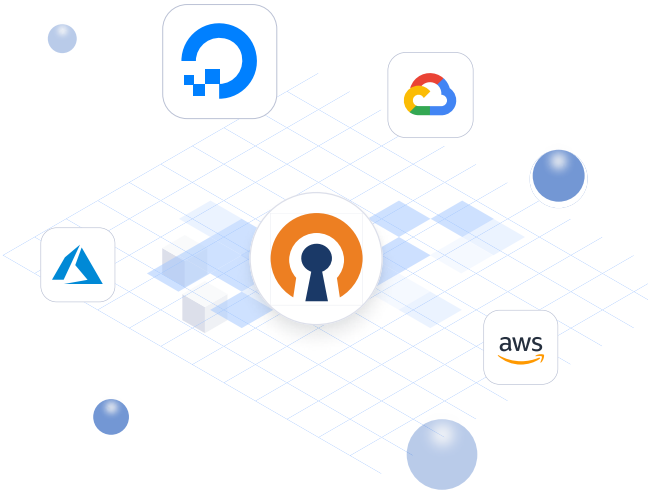
In many platform and point solutions alike, small and midsize businesses pay the same as, or in some cases more than, a much larger enterprise. Sticker shock, especially after you've been able to trial a point software, can be frustrating to say the least.

As you evaluate point solutions, it's important to consider:

- Is the vendor up-front with their pricing?
- Does the vendor offer usage-based pricing?
- Will your business be expected to pay for unused seats or licenses?
- Will you be able to scale up or down as needed and on demand?
- Is there an added charge or cost associated with onboarding, troubleshooting help, or customer support?
- Does standard pricing include features like byte counts for individual traffic flows, Internet Assigned Numbers Authority (IANA) protocol names by numbers for easier review and analysis of traffic flows, log streaming, access from multiple operating systems, etc.?

2. Simplified deployment

Simplified deployment sounds like an oxymoron – show me an engineer who has never had a demanding deployment, and I'll show you a liar (or someone who just started their first day on the job). However, lengthy deployment processes can cost more than just time and money; they can erode trust between decision makers and their teams.



A few considerations should include:

- The average amount of time used for setup and configuration.
- Whether you can sign up and test the solution without speaking with a sales person first.
- Whether you can deploy the solution directly from an IaaS marketplace, like AWS or another preferred marketplace.
- If the solution is self-hosted or has an option for a managed (SaaS) version.
- The level of difficulty to deploy network controls to block potentially malicious or unauthorized websites. For example, is it as easy as a toggle switch? Or typing in a domain name to block a site?
- The level of difficulty to add or remove users or to scale up or down.
- The look and feel of the interface for both admins and users. Is it easy to deploy for Admins but very complicated for the average User on their company-issued laptop?
- Can someone with minimal experience learn how to set up and deploy the solution without needing hours of training and set up time?
- Do you need a specific operating system for deployment? For example do you need Linux?

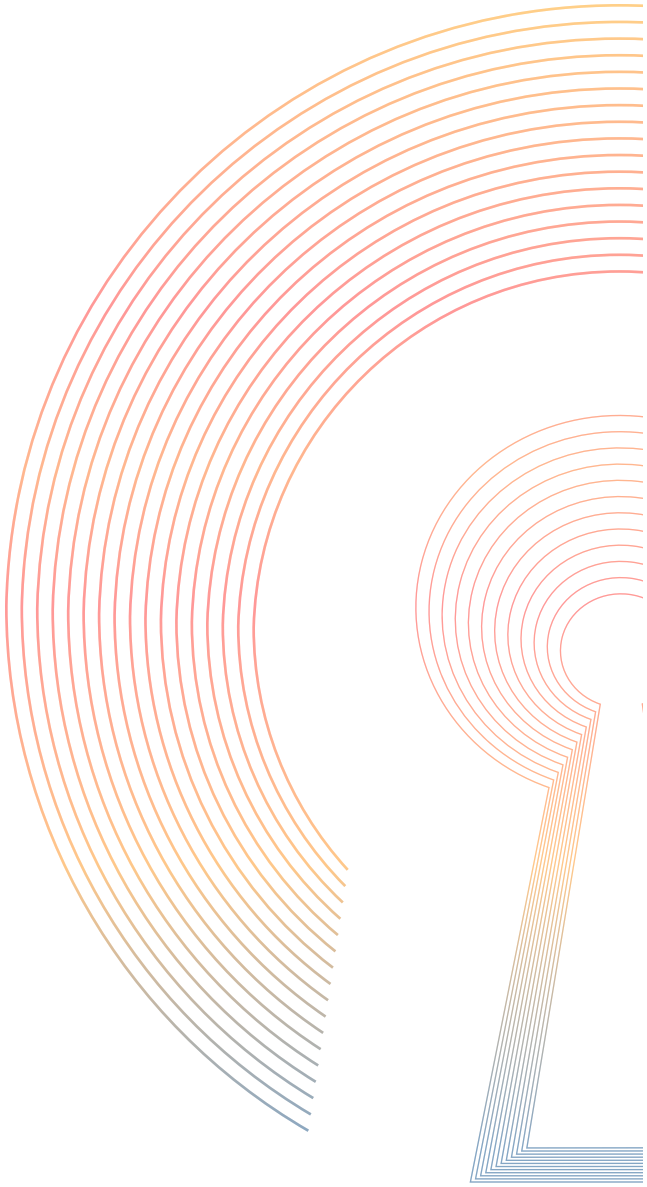
3. Asset, app, and workspace environments that work with your current and future strategy

Depending on the type of business and the number of years you have been in business, you could have a myriad of application types in your IT environment. These could range from legacy mainframe applications to the latest Web3 applications — and everything in between. Ask whether the solution you're considering can handle all the application types, including those you eventually plan to transition to the Zero Trust framework.

You'll also need to **choose solutions that allow connectivity at the IP, TCP, and UDP (network-level) instead of solutions that work just for web apps** (HTTPS application protocol) or specific application protocols.

Depending on your specific needs and current environment in these areas, you may also need to consider the following:

- Employee bandwidth for remote and hybrid workers who may benefit from split-tunneling technology, especially for those using public internet or an unsecured internet connection.
- Whether you have multiple internal web applications that need to be hidden from discovery to enhance protection and comply with ZTNA standards.
- Whether the solution you are considering has features like DNS-based content filtering to monitor and block threat actors.
- If the tool can secure IoT devices and communication.
- If you are able to specify traffic that travels over the VPN by website domain names — similar to per-app VPN policies, while other traffic routes outside the encrypted tunnel.
- If the tool can enforce SaaS access to only allow logins coming through the secure VPN.
- If you'll be able to interconnect your private networks across multiple sites and public clouds.
- If you can use both site-to-site networking and secure remote access.
- How many points of presence (PoPs) the vendor has across the globe and whether that is enough to support your global workforce.
- Potential impacts on network speed and performance — and ways to increase network speed should a lag occur.
- Will your users need to connect via iOS or Android?



4. Security compliance and prioritization of safety

We talk a lot about security compliance for your secure remote access tools — be they point or platform — because it can make or break a successful cyber attack. Increasingly, for small businesses, the reality is, it is not a matter of if you and your SaaS vendors are attacked — it's a matter of when.

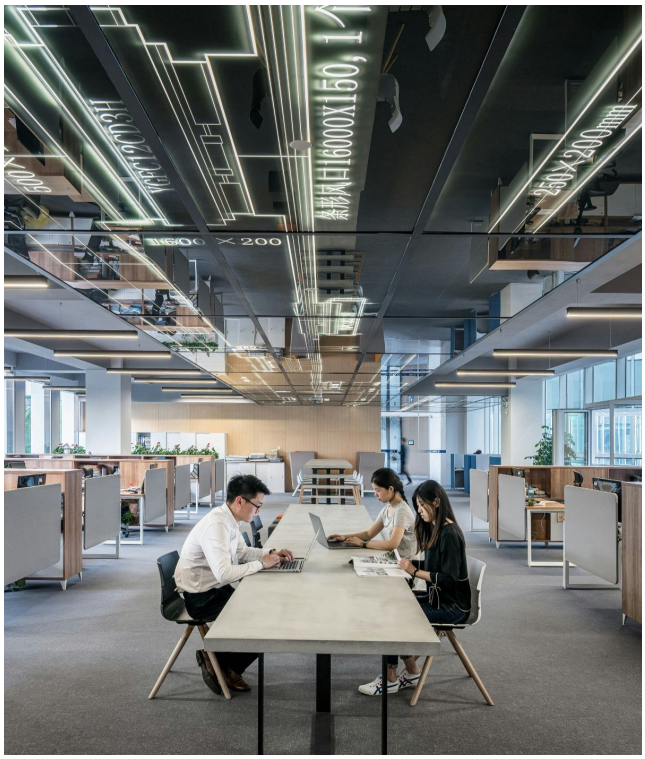
In fact, according to Enterprise Strategy Group, **"three-quarters of organizations report experiencing an attempted ransomware attack within the past 12 months, with 27% indicating that attacks happened on a weekly basis or even more frequently."**

However, that doesn't necessarily mean that SMBs are not taking necessary steps to protect themselves.

When considering any point solution, look for:

- SOC® II compliance.
- Third-party security audits and validation.
- A list of vulnerabilities and exploits associated with the technology.
- Security features within the solution, such as content filtering.

As a general rule, software that has an open source foundation is often safer and more frequently tested and validated than privately developed software. This is crucial, because open source is used across many private products. For example, OpenVPN's VPN protocols are not only tried and tested; they are a foundational piece of many VPN providers' foundations.



A February 2024 survey from ESG found that:

60%

of SMBs had plans to invest in better cybersecurity initiatives overall in 2024

45%

of SMBs reported that cybersecurity has become significantly more important to their organization's future over the last 2 years

30%

of SMBs will use third-party cybersecurity vendors in 2024

*The missing factor is recognizing which of your SaaS vendors may pose an additional risk, and understanding how those vendors mitigate risks on your behalf.

5. Integrations, APIs, updates, and the impact on your existing tech stack

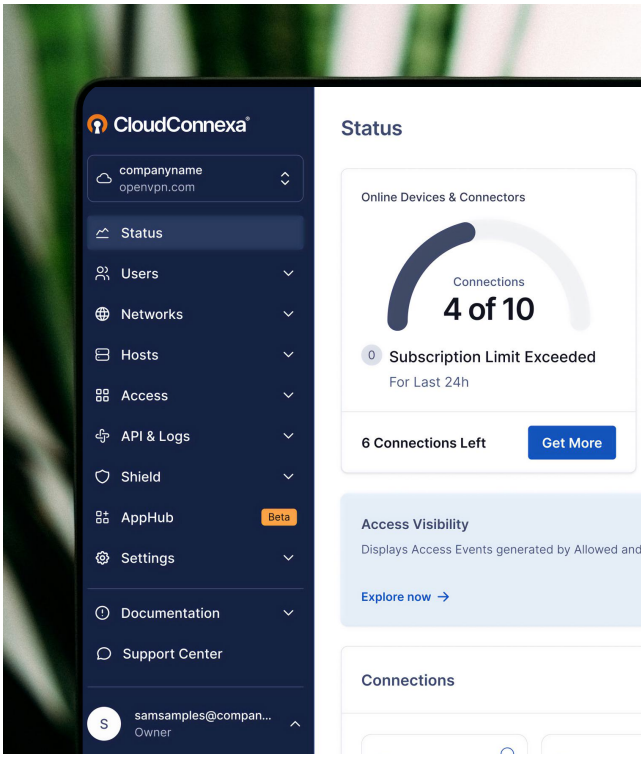
When you opt to use point solutions, make sure they integrate not only with your current strategy but also with your current tech stack and user authentication tools. This is key.

You'll need a few things in your solution, including:

- APIs that allow you to programmatically configure and manage them.
- Webhooks that allow you to send or react to external events from other systems.
- Software that allows the use of IaC (infrastructure as code) to create the same configuration in different cloud environments.
- Software that allows log collection for SIEM systems.

Additionally, you should look for:

- Integrations that are compatible with a self-hosted solution.
- Available integrations with a managed solution (SaaS).
- Whether there is easily-accessible documentation to set up the integrations.
- Automation in the integration. Will you have to manually update any of the tools in the tech stack to keep them synced?
- Layers of protection in the integration and whether the integration is fully secure.
- Whether the point solution you're considering will threaten the speed or connectivity of existing integrations.
- Compatibility or integrations with multi-factor authentication (MFA) tools that you already use.
- Whether the vendor's product roadmap reflects future integrations or updates that will help you meet your goals.



6. Tenets of Zero Trust

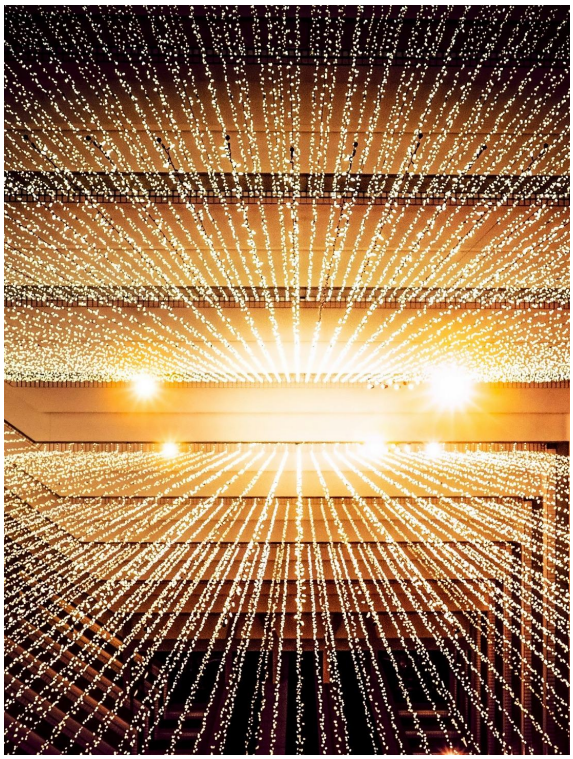
We've said it before, and we will say it again: **Zero Trust is not one singular tool or solution.** If your team has current plans — or is currently looking — to deploy Zero Trust across your organization, there are multiple ways to achieve your goals.

If we deconstruct the main functionality of ZTNA solutions into two main components, they would be: 1) applying the zero-trust security principles to ensure that there is no lateral movement and that permissions to applications are based on identity and context and 2) providing a means to get network access to those applications.

The ZTNA solutions in the market differ based on the technologies they use to accomplish the zero trust and network access functionality. The choice of technologies can give some products an edge over others or suit a particular market need better.

A few examples of ZTNA capabilities to consider include:

- Whether it provides connectivity at the IP layer and therefore supports all internet application protocols. Using an approach other than IP layer connectivity implies that it will support only a limited set of applications (most likely web-based) and will try to convert other popular application protocols like RDP and SSH into HTTPS with limitations.
- Does the tunneling protocol provide access to the network and grant access to only those applications that are authorized based on authenticated identity and context?



41%

of businesses of all sizes have plans to increase in ZTNA investments in 2024*

44%

of SMBs adopt zero trust to reduce the number of security incidents in 2024*

50%

of SMBs adopt zero trust as a method to modernize cybersecurity programs in 2024*

69%

of businesses of all sizes have implemented or have begun to implement zero trust across their organizations as of Q1 2024***

*ESG

7. Positive customer reviews & input

Let's face it: there is nothing quite as valuable in helping you find the right tool as talking to a company's existing customers. They don't hold back.

As you peruse your shortlist of vendors' websites, try to locate:

- Recent reviews and customer success stories on the business page.
- Social media comments or threads relative to the product and your specific use case.
- Reviews on G2, Capterra, or another trusted review site.
- A way to request customer recommendations or references.
- The number of current customers on the company roster. For example, OpenVPN's CloudConnexa has over 2,400+ small and medium business customers from organizations of all industries.
- A customer Net Promoter Score (NPS) or customer satisfaction rate. For example, CloudConnexa boasts a 93.5% customer satisfaction rate.
- How the company uses customer feedback in their future product roadmap.

Vendor checklist

Save this checklist for easy reference as you evaluate vendors and make notes on each vendor you're evaluating. Although each vendor may not check every box, you can use this sheet to prioritize your SMB's needs and compare vendors easily.

Note: this guide and checklist can be used to evaluate any security vendor and is not limited to network security providers.

- ☐ Pricing sheet available? _____
- ☐ Free trial or connections? _____
- ☐ List of recent security vulnerabilities / security compliance _____
- ☐ Integrations with current tech stack _____
- ☐ Existing customer reviews or references available _____
- ☐ Free technical support _____
- ☐ Scalability: Adding concurrent connections or future users _____
- ☐ Deployment: On-prem or cloud? _____
- ☐ Technology: Does the company roadmap reflect our future goals? How are the vendor's updates prioritized and implemented? _____
- ☐ Technical notes _____
- ☐ Additional Notes _____

_____

_____

_____

_____

Let's get technical

There are a few more elements to consider when you purchase a network security solution, specifically if you are looking for use cases wherein a VPN can be used to accomplish the inclusion of secure remote access or ZTNA basics. The following features should be considered by SMBs:

Cloud vs. self-hosted

- Ability to self-host through private servers or AWS if preferred.
- Options for a fully-managed and hosted service.
- Point-and-click centralized management and configuration.
- Fast, easy creation and management of multiple wide-area private clouds (WPCs) from a single Owner account.

Networking

- Support for Site-to-Site and Remote Access.
- Full-mesh connectivity without complex configuration.
- Unique local address range available for customer use.
- Support for peer-to-peer communication.

Security

- Enhanced security as only outgoing connections are made.
- Firewalls don't need to be opened to allow incoming traffic from the internet.
- DNS-based content filtering.
- Device Identity Verification & Enforcement (DIVE) to make it easy for admins to verify device identities before granting network access.

IPv4 and IPv6

- Full RFC 1918 IPv4 private address range and IPv6 RFC 4193.
- IPv6 and IPv4 support.
- Virtual, worldwide, private, secure networking.
- IPv4 and IPv6 space for each Tenant/Customer.
- There should not be a limit to the list of protocols or service support.

Routing

- Improve network performance with smart routing.
- Increase redundancy with multiple network connections.
- IP-layer networking allows access to all IP-based services.
- Flexible routing of Internet traffic.
- Access private services by connecting to any of the worldwide regions.
- Customers can use their private DNS servers.
- Routing via domain names is an option, even if there are multiple networks with overlapping IP address ranges.
- Similar to per-app VPN policies, traffic can be steered into the VPN tunnel on a per-domain basis.

Take the next step with OpenVPN

Now, the sales pitch. We know, we know, nobody wants to hear a sales pitch. But **if you've read this far, it's clear you need your Goldilocks solution, and we can help.**

OpenVPN's secure networking solutions, self-hosted Access Server and cloud-hosted CloudConnexa, combine the most essential elements of network security into a single cost-effective, easy-to-use package.

Access Server offers a full-control option for users who are comfortable using and maintaining their own servers, with data communications remaining under your control without passing through OpenVPN infrastructure. Access Server simplifies the rapid deployment of a secure remote access and site-to-site solution with a web-based administration interface and built-in OpenVPN Connect app distribution with bundled connection profiles.

We built Access Server using the OpenVPN open source core and additional open source software like OpenSSL. OpenVPN Access Server maintains compatibility with the open source project, making the deployed VPN immediately usable with OpenVPN protocol-compatible software on various routers and operating systems, and Linux. The official OpenVPN Inc.-developed client, OpenVPN Connect, is available for Windows, macOS, and both Android and iOS environments.

For those who prefer a cloud-hosted environment, **CloudConnexa takes the cost and complexity out of secure networking to keep your business operating safely and efficiently.** CloudConnexa reliably identifies and routes trusted apps and traffic using an integrated multi-tenant virtual network with built-in critical security functions.

No matter which option you choose, our subscriptions are based on "concurrent connections," not users, so you pay for what you actually use. Concurrent connections means that you will only pay for the number of users connected at any given time. So if you have users who will only log in at night and some who log in during the day, you won't pay extra. You can even get started with free connections, no credit card required, and scale to a paid subscription when you're ready.

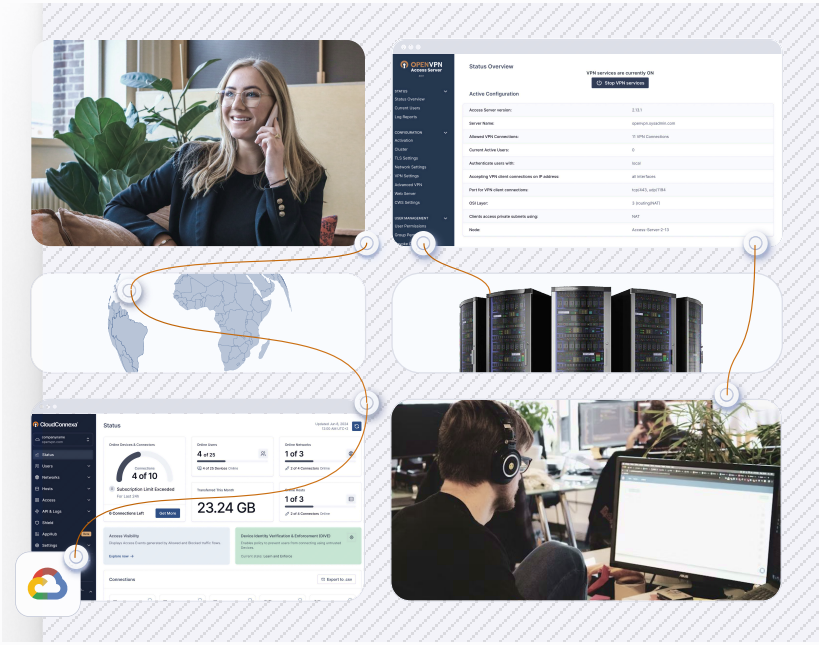
Take the next step with OpenVPN

Join 20,000+ commercial customers that choose OpenVPN

- Connect up to three devices free
- Scale as your business grows
- Support, upgrades and Connect Client included

Learn more

Get Started for Free



Have any questions? Feel free to contact our sales and support team.