



From VPN to ZTNA: Securing Your Business for the Future

**Leveraging ZTNA for a Zero Trust
Security Model**

The Challenge of Modern Cybersecurity

Data Breaches: A Growing Global Concern

The scale of cybersecurity threats is staggering. In France alone, businesses lost **€120 billion in 2024*** to data theft, industrial espionage, and sabotage. Malware, such as ransomware, is particularly on the rise, with threat actors targeting sensitive data and demanding ransom for its release.

In 2024, the number of **breached records** in France reached an all-time high, surpassing **17 million***, a clear indication that current security measures are failing to keep up with the evolving threat landscape.

In response, the **CNIL**, the French data protection regulator, carried out strict regulatory measures, resulting in a total of 331 actions** among other:

87
sanctions

€55,212,400
in cumulative fines

180
compliance orders

64
reprimands

This highlights the severe financial and reputational risks posed by data breaches, which are not isolated to France but are a global concern for all businesses.

Is Your Organisation at Risk?

The truth is, no organisation is immune to cyberattacks. The question is no longer if a breach will happen, but when.

To mitigate risks, businesses need to rethink their security frameworks.

*<https://www.statista.com/topics/7002/cyber-crime-at-companies-in-france/#topicOverview>

**<https://www.cnil.fr/en/sanctions-and-corrective-measures-cnils-actions-2024>

The Limitations of VPNs in a Modern Workforce

Why VPNs Are No Longer Enough

VPNs (Virtual Private Networks) have been a staple in corporate security for years, particularly in the era of remote and hybrid work. They offer a layer of security by encrypting connections and providing a "safe tunnel" for employees to access company resources from anywhere.

But, as cyber threats evolve, **VPNs** fall short in several key areas:

- **Single Point of Failure:**

VPNs operate like a tunnel, once an attacker breaches one end, they can gain direct access to the entire network.

- **Limited Security and Scalability:**

VPNs grant users extensive access to the network, increasing risk. They also struggle to scale with the dynamic, cloud-based environments of modern businesses.

- **Reduced Performance:**

VPNs can slow down internet speeds and create access limitations, leading to poor user experience.

- **Lack of Contextual Awareness:**

VPNs don't adjust based on real-time factors like user behaviour, device health, or location.

The **VPN** model assumes a "trusted" internal network, which is increasingly becoming an outdated and vulnerable way to protect data.

Introducing ZTNA: A New Paradigm for Security

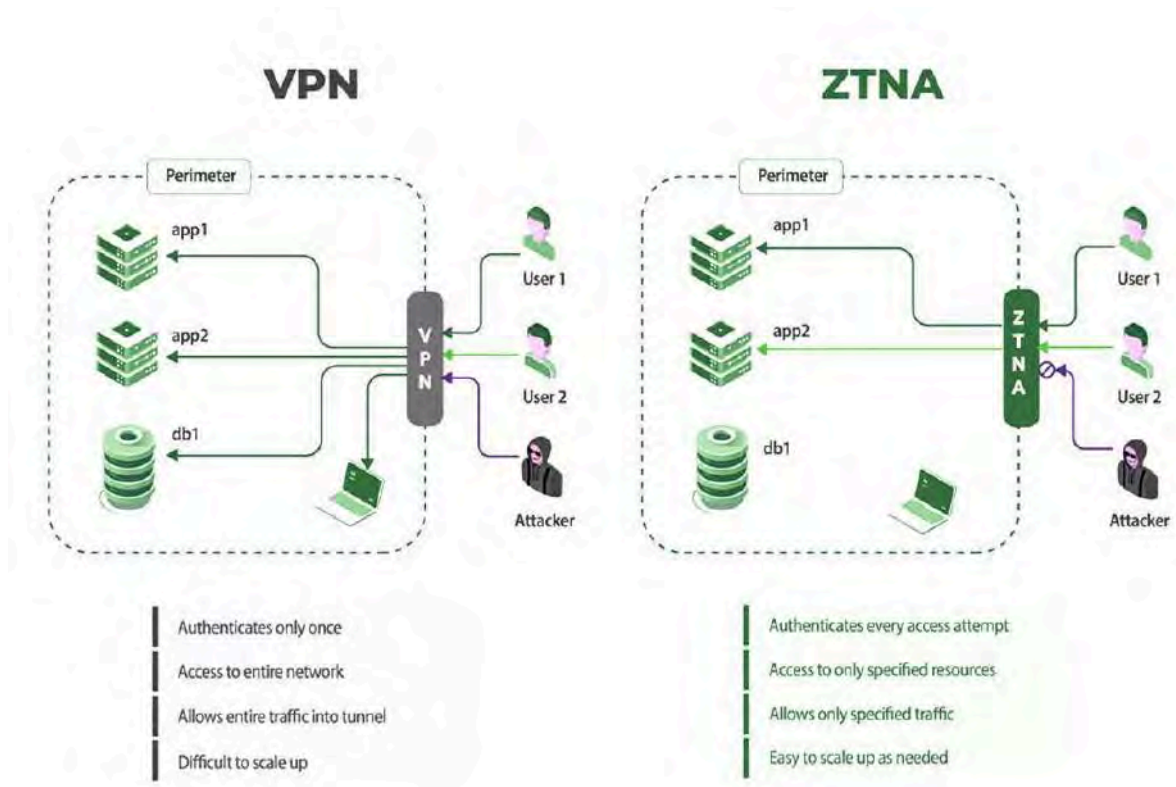
ZTNA stands for Zero Trust Network Access. In today's rapidly evolving threat landscape, a **modern, comprehensive security approach** is essential, and that's where **Zero Trust Network Access (ZTNA)** comes in. Built on the principle of **"never trust, always verify"**, ZTNA ensures that every access request is continuously validated, regardless of the user's location.

ZTNA grants access to specific applications and services based on a variety of dynamic factors, including **user identity, device health, and contextual information**. This approach allows for more **granular, secure access**, ensuring that only authorised users can connect to the resources they need.

ZTNA also minimises the risk of lateral movement within your network, providing a more secure, flexible solution for today's distributed work environments.

VPN vs. ZTNA: Why the Old Perimeter No Longer Works

As workforces become more distributed and cloud adoption accelerates, traditional VPNs are struggling to keep up. Zero Trust Network Access (ZTNA) offers a smarter, more secure way to connect users to the applications and data they need, without exposing your entire network.



Here's how they compare:

Category	VPN (Legacy Model)	ZTNA (Modern Approach)
Trust Model	Trust is granted broadly after login. Once authenticated, users often have wide access across the network.	Trust is never assumed. Every access request is continuously verified, regardless of user location or device.
Access Control	Users typically gain broad access to network segments, increasing risk in the event of a breach.	Access is granted on a per-application basis with least privilege by default , limiting potential damage.
Context Awareness	Static rules based on fixed parameters like IP address. Doesn't account for device health or user behaviour.	Dynamic access policies adapt to context , such as location, device type, time of day, or activity patterns.
Security Response	Manual and reactive. Threats often go undetected until damage is done.	Automated threat detection and real-time response using AI and machine learning.
Segmentation	Basic segmentation. Once inside, users can move laterally across the network.	Microsegmentation isolates applications and limits attacker movement inside the network.
Scalability & Management	Complex to manage and scale. VPNs often require additional hardware and configuration.	Cloud-native, with centralised policy control and easy scalability across users, apps, and environments.

The Business Value of ZTNA

Shifting to Zero Trust Network Access (ZTNA) is more than a security upgrade, it's a strategic move toward **smarter operations, stronger protection, and a more productive digital workplace.**

Strengthened Security Posture, Smaller Attack Surface

ZTNA minimises cyber risk by continuously verifying identities, enforcing least privilege access, and eliminating broad network exposure. Apps are hidden from public view, reducing the attack surface and removing the need for firewalls, VPNs, and their public IPs.

Prevents Lateral Movement and Limits Breach Impact

Unlike VPNs, which provide broad network access, ZTNA connects users **directly to the applications they need, nothing more.** This microsegmentation approach halts lateral movement and limits the scope of any breach.

Simplified Management and Reduced Complexity

ZTNA replaces a patchwork of point products with a unified platform. It streamlines operations through centralised policy enforcement and simplifies connectivity with a direct-to-app model, cutting IT complexity and cost.

Built for Agility and Growth

ZTNA adapts effortlessly to your evolving environment, whether you're onboarding remote teams, rolling out new apps, or expanding globally. With cloud-native scalability and centralised control, you can move fast without compromising security.

Real-Time Threat Detection and Scalable Protection

ZTNA inspects all user traffic, including encrypted traffic, through a cloud-native security layer that scales on demand. Threats are detected and policies enforced in real time, ensuring fast, automated protection without compromising performance.

Data Loss Prevention Across All Channels

ZTNA prevents both accidental and malicious data loss by applying consistent security controls across endpoints, encrypted traffic, cloud apps, and web access, securing sensitive information wherever it flows.

Seamless Access, Better User Experience

By eliminating the latency of traditional VPNs and routing traffic through the shortest path, ZTNA improves application performance. Users enjoy frictionless, secure access, backed by transparent authentication and MFA that doesn't disrupt productivity.

Choosing the Right Partner for ZTNA

Why Partnering with the Right Provider Matters

Implementing **Zero Trust Network Access (ZTNA)** isn't just about adopting a new security framework, it's about ensuring that your organisation is equipped with a robust, scalable, and future-proof security model. To fully leverage the benefits of ZTNA, it's crucial to partner with a provider that can guide you through this complex transformation.

The right partner will not only help you implement ZTNA effectively but will also provide ongoing support to adapt your security posture as your business evolves and threats become more sophisticated.

Key Considerations When Choosing a ZTNA Partner

- **Experience and Expertise:** ZTNA is a specialised solution, and deploying it requires deep technical expertise. A trusted partner should have a proven track record in **Zero Trust** implementation and security architecture.
- **Customisation:** Every business has unique needs. A good partner will tailor the ZTNA solution to match your **existing infrastructure**, security requirements, and growth objectives, ensuring that it integrates seamlessly into your broader IT strategy.
- **Scalability and Flexibility:** As your business grows and changes, so should your security solutions. The right partner will ensure that the ZTNA solution is not only scalable but also adaptable to support **cloud adoption**, remote work policies, and emerging threats.
- **Compliance Assurance:** Ensuring compliance with industry regulations and standards is crucial for any business. A trusted ZTNA partner should help you align your security framework with **data protection laws, GDPR** (General Data Protection Regulation), and other **industry-specific compliance requirements**. Your partner should have a clear understanding of how to implement **ZTNA in a compliant manner**, safeguarding sensitive data while meeting regulatory demands.
- **Ongoing Support and Maintenance:** ZTNA is not a one-time implementation. Ongoing monitoring, management, and optimisation are key to ensuring the security solution remains effective as new challenges arise. Choose a partner who offers long-term support and continuous improvement.
- **End-User Experience:** Security should never come at the cost of user productivity. A trusted partner will ensure that ZTNA is deployed in a way that enhances user experience, providing **seamless, direct-to-application** access while maintaining strong security controls.

The Role of a Trusted Partner in Your ZTNA Journey

Successfully adopting ZTNA involves more than just technology, it's about transforming your entire security mindset. Your partner should act as an **extension of your team**, helping you navigate the complexities of Zero Trust while focusing on your business outcomes.

From initial assessment to full-scale deployment and ongoing management, the right partner will ensure that your ZTNA solution delivers the protection, scalability, compliance, and efficiency your business needs.

Getronics' Approach to Zero Trust Network Access (ZTNA)

In today's dynamic threat landscape, traditional perimeter-based security models are no longer sufficient. Getronics delivers a modern, robust approach to network security through Zero Trust Network Access (ZTNA), a key pillar of our cybersecurity portfolio.

Getronics supports the full lifecycle of ZTNA adoption, from initial assessment and solution design, to deployment and 24/7 operational support. Our cybersecurity teams work closely with clients to integrate ZTNA into complex, hybrid IT landscapes, ensuring minimal disruption and maximum security value. Whether customers need **consultancy, turnkey implementation, or managed services**, Getronics provides **expertise and execution tailored to your business model**.

Getronics' ZTNA Solution Highlights

1. Identity-Centric Access Control

At the core of our ZTNA solution is a strong identity framework. Getronics integrates with major identity providers to enforce multi-factor authentication (MFA), role-based access control (RBAC), and single sign-on (SSO).

1. Context-Aware Policy Enforcement

Access policies are dynamically applied based on real-time context, including user role, device health, location, and time of access. This minimises lateral movement and ensures that users only access the resources they need.

1. Seamless Integration with Existing Infrastructure

Our ZTNA solution is vendor-agnostic and designed for hybrid environments. Whether clients are operating fully on-premise, in the cloud, or across both, we implement ZTNA with minimal disruption.

1. Secure Application Access, Not Network Access

Instead of exposing entire networks, Getronics' ZTNA architecture provides application-level access. This reduces attack surfaces and mitigates the risk of data breaches.

1. Continuous Monitoring and Analytics

ZTNA is not a set-it-and-forget-it solution. We provide ongoing visibility and analytics on user behaviour, anomalies, and access attempts to continuously fine-tune security postures.

1. Flexible Deployment Models

Whether clients need a cloud-native ZTNA, an on-premises deployment, or a hybrid model, Getronics tailors its solution to meet compliance, performance, and scalability needs.

Why Getronics?

Getronics is experienced in delivering ZTNA solutions from industry-leading vendors including Fortinet, and Zscaler. Whether customers require end-to-end implementation, operational support from Level 1 to Level 3, or integration with their existing infrastructure, our vendor-agnostic approach ensures a fit-for-purpose deployment aligned to business needs.

Our deep experience in managing secure digital workplaces and critical infrastructure across multiple industries enables us to deliver ZTNA solutions that are both secure and practical. We understand that security must enable productivity, not hinder it.

Our approach also ensures that ZTNA implementation supports industry frameworks like GDPR, ISO27001, and NIS2.

FORTINET®

zscaler™

getronics

About Getronics

Getronics empowers businesses to stay competitive by offering **flexible, secure, and reliable** technology services, tailored to their unique needs, helping to drive growth, increase efficiency, reduce cost, and deliver measurable success. Getronics is committed to **low-carbon and sustainable development** through its IT solutions to help companies reduce their environmental impact.

As a global leader in technology solutions with over 4,000 colleagues in 22 centres, and as the leading and founding member of the Global Workspace Alliance (GWA), Getronics can provide comprehensive end-to-end IT solutions around the globe.

It is one of the 18 companies from around the world positioned within the Gartner's 2025 Magic Quadrant for Outsourced Digital Workplace Services, and is committed to delivering exceptional customer service, to enable businesses to focus on their core strengths while entrusting their IT needs to Getronics.

For more information, visit:
www.getronics.com/about-us

