FORTRA

3 Reasons VPNs Can't Protect Your Private Apps and Data

Why is perimeter-based data security a thing of the past?

Virtual private networks (VPNs) emerged when remote work was less common, and people only occasionally required access to corporate resources.

Back then, most experts believed security could be maintained by confining users, data, and applications within a secure perimeter and by restricting users to company-issued devices. VPNs essentially extended this implicit trust by granting all users access to corporate resources upon authentication.

Times have changed, of course. Users now work virtually anywhere, often via devices and networks you don't manage. Private apps, which continue to house some of your most valuable data, are increasingly in the cloud.

As a result, the security perimeter is no longer sufficient. To effectively safeguard your data you need to first understand the shortcomings of VPNs. This e-book outlines the three reasons why VPNs are inadequate in today's cloud-first, hybrid work environment.

HIGHLIGHTS

- See how threats to private apps have changed in a remote-first world
- Find out why VPNs are no longer adequate for secure access
- Discover more effective modern-day options for data security

REASON 1

VPNs are cumbersome to administer and impede productivity

VPNs are typically integrated into your organization's hardware suite alongside other data center appliances. Like many on-premises solutions, they require a lot of effort to manage. This complexity is compounded by the rise in remote workforces and the proliferation of private apps hosted in the cloud.

VPNs are a drain to your resources

- **Complex setup:** Private apps are now just as likely to reside on premises and in the cloud, often in multiple IaaS environments. As a result, you have to manage multiple VPN concentrators or string together a variety of clients and destinations.
- **Resource-heavy management:** VPNs require time-consuming and manual processes that rely on networking routing tables that are often outdated.
- **Poor end-user experience:** VPNs can make it difficult to access private apps in the cloud, requiring all inbound traffic to first go back to the data center before going to the user. This leads to latency or downtime and requires users to install an agent, which hinders their ability to use personal devices.

REASON 2

VPNs are primed to be exploited

56%

of organizations reported cyber incidents related to VPN vulnerabilities in 2024.

- Cybersecurity Insiders

As with other on-premises appliances, and unlike cloud-based solutions, VPNs require frequent manual patching to address potential vulnerabilities.

Another concern: VPNs allow users to initiate sessions, exposing your data to risk through external connections and internet vulnerabilities.

How VPNs expose you to risk

- **Countless vulnerabilities:** As critical entry points to organizations, CVEs (common vulnerabilities and exposures) are constantly being discovered in VPNs. Your team must manually patch each one, which significantly complicates efforts to minimize the number of exploits.
- **Frequent misconfigurations:** Due to their complexity, it's easy to misconfigure your VPN's settings. Whether it's through unused passwords, not-yetdeprovisioned users, or accidental exposure to the internet, misconfiguration can easily be exploited by attackers.
- **Corporate perimeters at risk:** Your VPN is a virtual extension of your security perimeter. So any issues with the VPN will impact your networks. Of particular concern: Your VPN must create an opening in the enterprise firewall to receive traffic from a remote endpoint. This exposes your perimeter to a wide range of vectors for attackers to leverage.an agent, which hinders their ability to use personal devices.

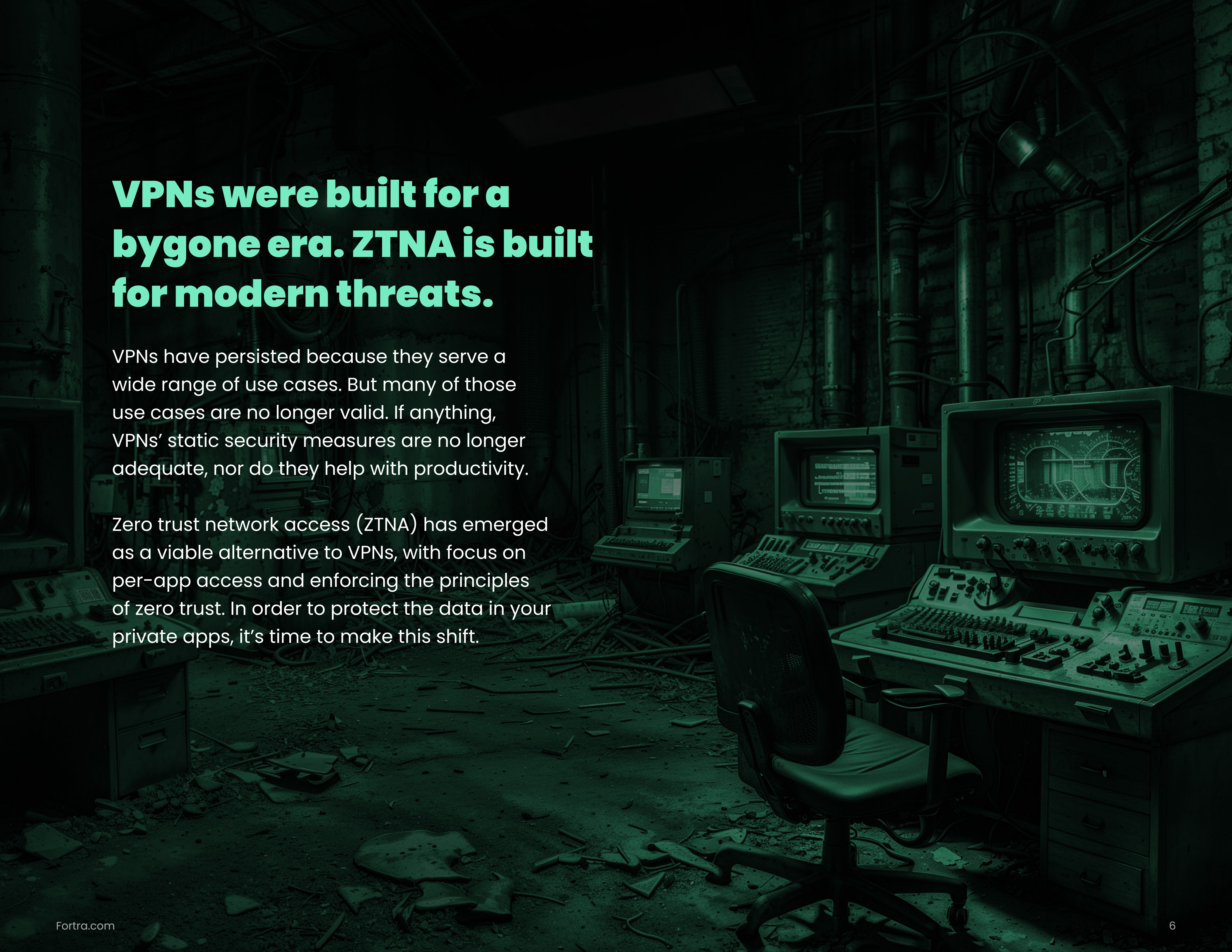
REASON 3

VPN defenses can be easily circumvented

Breaches often start with compromised accounts. These attacks succeed because static verifications that VPN uses, like passwords and MFAs can be circumvented. And once a user is connected, organizations have no visibility into how they're interacting with apps and data.

VPNs are a drain to your resources

- **Connects first, authenticates later:** To secure a connection, your VPN can integrate with third-party identity providers. But since they're designed to provide access, verification usually occurs after a connection is already established, which means an attacker has time to gain a foothold.
- **Provides network-wide access:** Your VPN uses IP-based routing to place a device in your network. But since your network is probably coarsely segmented, any user with access can move laterally within it, find other vulnerabilities, and compromise valuable data.
- **No visibility into user activities:** Not all threats are as black and white as a wrong password or the inability to produce a second factor of authentication. A compromised account may start out appearing to be benign but quietly begin taking risky actions, such as accessing sensitive data or exfiltrating a massive amount of information.



VPNs were built for a bygone era. ZTNA is built for modern threats.

VPNs have persisted because they serve a wide range of use cases. But many of those use cases are no longer valid. If anything, VPNs' static security measures are no longer adequate, nor do they help with productivity.

Zero trust network access (ZTNA) has emerged as a viable alternative to VPNs, with focus on per-app access and enforcing the principles of zero trust. In order to protect the data in your private apps, it's time to make this shift.

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.