idemeum

Secure Remote Access

Replace overburdened legacy VPNs with fast, simple, cloud-based connectivity that is enforcing least privilege and zero trust principles.

Problems with VPNs today

Secure, seamless remote access is a business enabler – it boosts user productivity while reducing the time IT teams spend to onboard and maintain user-to-application connectivity with agility and resilience. And yet, remote access remains a challenge for many organizations.

Once upon a time, VPNs offered a simple way to connect a few remote users to corporate networks for brief periods of time. As workforces became more distributed, however – and organizations needed to keep remote users securely connected for longer periods of time – the flaws in this approach became evident, from sluggish performance and increased security risks to scalability concerns.

WEAK SECURITY

The network-level access and default trust granted by VPNs create security gaps - attackers may enter your network through a less sensitive entry point after stealing credentials, and then traverse to find more business-critical information to exploit. With this lateral movement exposure you are inviting attackers to go anywhere and take anything.

POOR PERFORMANCE

Employees suffer through slow and unreliable connections that simply weren't built for today's scale of remote access. Legacy protocols such as IPsec add huge packet processing and CPU overload, and bandwidth is always a limitation especially with non-horizontally scalable hosted VPN servers.

CLUNKY USER EXPERIENCE

VPNs can be frustrating for administrators to configure, and clunky for users to handle. VPN clients are not adept at fluidly handling user mobile and desktop roaming, requiring users to repeatedly re-authenticate – causing lost productivity and creating IT tickets.

*In fact, Gartner predicted that "**by 2025, at least 70% of new remote access deployments will be served predominantly by ZTNA as opposed to VPN services, up from less than 10% at the end of 2021."** By prioritizing a ZTNA project, IT and Security executives can better shield their business from attacks like ransomware while simultaneously improving their employees' daily workflows. The trade-off between security and user experience is an outmoded view of the world; organizations can truly improve both if they go down the ZTNA route.*

Why idemeum remote access?

Offloading applications from your VPN and moving toward idemeum secure remote access can have measurable benefits for your business even in the short term. Many of our customers speak to improvements in their IT team's efficiency, onboarding new employees faster and spending less time on access-related help tickets.

STRENGTHEN YOUR SECURITY POSTURE

With idemeum zero trust principles you eliminate implicit trust and reduce the risk of security breaches. You can replace broad security perimeters with one-to-one verification of every request to every resource. Enforce Zero Trust rules on every connection to your corporate applications, no matter where or who your users are.

DELIVER A BETTER USER EXPERIENCE

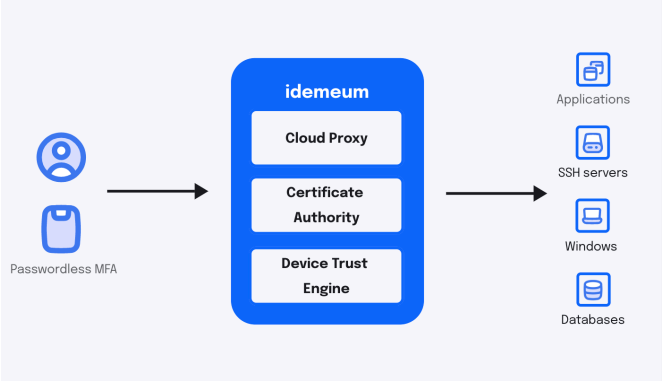
Users have familiar seamless access to any resource from the centralized application portal, where any on-premises resources feels like a SaaS application. Familiar login flow, paired with strong passwordless authentication removes the tedious part of managing VPN clients.

LEVEL UP YOUR ACCESS STRATEGY

Empower your admins with comprehensive visibility and granular controls to determine who should interact with your internal tools and under what authorization conditions.

How idemeum remote access works?

Instead of authenticating a user and providing access to everything on your corporate network, idemeum secure remote access authorizes access per resource, effectively eliminating the potential for lateral movement. Each access attempt is evaluated against **Zero Trust Rules** based on identity, device posture, geolocation, and other contextual information. Users are continuously re-evaluated as context changes, and all events are logged to help improve visibility across all types of applications.



STRONG AUTHENTICATION

Protect resource access with strong forms of authentication such as Passwordless MFA and biometrics.

MICRO SEGMENTATION

Enforce least privilege with secure reverse proxy tunnels for every resource.

GRANULAR POLICY CONTROLS

Easy to use rules for location, network, device posture, user information authorization enforcement.

MULTI PROTOCOL SUPPORT

idemeum supports RDP, Web, and SSH protocols to access various on-premises resources.

ZERO TRUST AS A SERVICE

Deploy secure remote access with our instant cloud platform.

Get in touch with us

Idemeum can help you design and implement zero-trust secure remote access. Schedule a demo today.

idemeum is a Zero-Trust Passwordless platform that offers one place to manage access to your workstations, applications, and infrastructure, all without passwords.