SECURE REMOTE ACCESS

Protect your users and data wherever work happens

Today's businesses are navigating a complex landscape – where employees work from anywhere, applications live in the cloud, and cyber threats are more sophisticated than ever. Our Secure Remote Access service is aligned to the SASE framework and is designed to support your business' compliance needs. Secure your workforce's access to the internet, cloud and SaaS applications while increasing operational efficiencies.

Who is Secure Remote Access For?

Secure Remote Access is ideal for businesses with:

- A dispersed workforce
- Workloads and applications across multi-cloud environments
- A need for a uniform ZTNA posture regardless of location across SaaS and private applications

Why Secure Remote Access?

- Reduce complexity and simplify operations
- Improve your security posture and reduce risk
- Ensure a consistent user experience across distributed teams
- Enable hybrid cloud adoption
- Support a flexible workforce
- Enable secure cloud adoption
- Meet evolving compliance needs

Secure Remote Access is designed to meet the evolving needs of modern, hybrid workforces by providing secure, reliable, and scalable access to applications and data – regardless of user location.

Delivered as a managed service and powered in conjunction with Fortinet's FortiSASE® platform, Secure Remote Access integrates seamlessly with existing WAN or SD-WAN environments or can be deployed as a standalone solution. Secure Remote Access delivers a uniform security posture managed centrally across on-premises and remote locations, managed and supported by our own Fortinet trained teams with fast tracked support from Fortinet.

Secure Remote Access Core Capabilities

- **Secure Internet Access.** Ensure your employees can browse the web safely, with harmful content blocked before it ever reaches their device. Whether they're working from home, a café, or the office, they're protected.
- **Secure SaaS Access.** Gain visibility and control over cloud applications like Microsoft 365, Dropbox, or Salesforce. Prevent data leaks and ensure that only authorised users can access sensitive information.
- **Secure Private Access.** Replace traditional VPNs with a smarter, more secure way to connect to internal systems using Zero Trust principles to verify users and devices before granting access—so only the right people get in.
- **Endpoint Security.** Add a layer of protection by checking the health of each device before it connects. If a laptop is missing a security patch or running outdated antivirus, access can be restricted until it's resolved.
- **Logging and Reporting.** Receive clear, actionable insights into what's happening across your endpoints regardless of location. From user activity and SaaS application performance monitoring to threat detection, your IT team can enhance its digital experience monitoring, seeing the full picture and responding quickly when needed.
- **SOC Integration.** Connect your environment to 24x7 security monitoring, so threats can be identified and escalated in real time, or integrate with your existing SOC.

Secure, Integrated Cloud Services

Secure Remote Access Features:

Security: What It Does	Why This Matters	What This Means
Advanced content filtering and malware protection.	Provides granular control over web access and actively blocks malicious websites and content in real-time.	Prevents malware infections, enforces acceptable use policies, and protects users from phishing and other web-borne threats, reducing cyber security risk.
Cloud-delivered next-generation firewall capabilities.	Moves firewall enforcement to the cloud edge, offering consistent security policies to all users regardless of location, without backhauling traffic.	Provides robust, scalable firewall protection for all users and devices, reducing network latency and simplifying security management across distributed environments.
Adaptive, identity-based access to private applications.	Authenticates and authorises every user and device for every application request, based on context, replacing outdated VPNs with a "never trust, always verify" model.	Minimises the attack surface, prevents unauthorised access to sensitive applications, and enhances data security for remote and hybrid workforces.
Data loss prevention to prevent sensitive data exfiltration.	Scans outbound data for sensitive information (e.g., PII, financial data) and prevents its unauthorised transmission or sharing.	Protects valuable intellectual property and customer data, helps maintain regulatory compliance (e.g., GDPR, PCI DSS), and avoids costly data breaches.
Intrusion prevention for blocking known and unknown threats.	Actively monitors network traffic for malicious activity and immediately blocks detected intrusions or attacks before they can cause harm.	Provides real-time protection against network-based exploits and sophisticated attacks, ensuring continuous business operation and data integrity.
Enhanced protection against web-borne threats.	Executes web content in an isolated, remote environment, sending only a safe visual stream to the user's device, thus containing threats away from the endpoint.	Eliminates the risk of malware from compromised websites directly impacting endpoints, enhances user experience by preventing malicious content from loading, and adds an extra layer of defence.
Powered by FortiGuard Labs AI-driven threat intelligence.	Continuously updates security protections with real-time, AI/ML-driven threat intelligence from Fortinet's global research labs.	Provides proactive and rapid defence against the latest and most sophisticated cyber threats, including zero-day attacks and ransomware, enhancing overall security posture.

Secure, Integrated Cloud Services

User Experience: What It Does	Why This Matters	What This Means
Comprehensive SaaS application visibility, control, and data protection.	Extends security policies to cloud applications, identifying shadow IT, preventing data leakage, and ensuring compliance within SaaS environments.	Secures sensitive data in the cloud, ensures compliance with data protection regulations, and provides full visibility and control over cloud app usage.
Integrated Fortinet Secure SD-WAN for intelligent application steering and WAN optimisation.	Dynamically routes traffic over the best available path, prioritising critical applications and ensuring high performance and reliability for hybrid networks.	Improves application performance for SaaS and cloud apps, reduces connectivity costs, and provides consistent user experience, especially for branch offices and remote users.
End-to-end performance insights.	Provides real-time visibility into user, application, and network performance, enabling proactive identification and resolution of performance bottlenecks.	Ensures a superior user experience, minimises downtime due to performance issues, and optimises IT resource allocation based on actual usage and performance data.
Points of presence for localised enforcement and performance.	Distributes the SASE infrastructure globally, bringing security and networking functions closer to the user, minimising latency.	Guarantees high-speed, reliable access to applications worldwide, improves user experience for global workforces, and ensures consistent security enforcement regardless of location.
Operational Efficiency: What It Does	Why This Matters	What This Means
Centralised Policy Management via FortiManager/FortiCloud.	Allows administrators to define, deploy, and enforce security policies consistently across the entire SASE infrastructure from a single console.	Simplifies security operations, reduces human error, ensures policy consistency across all users and locations, and accelerates policy deployment.
Flexible Client Options: FortiClient agent, agentless browser access, thin edges.	Supports diverse user and device connectivity scenarios, allowing secure access from corporate devices (agent) or BYOD/contractor devices (agentless), and securing small branches.	Adapts to any work environment, ensures comprehensive security coverage for all users and locations, and provides ease of deployment across various endpoints.

Our Credentials

ENGAGE
FORTINET ADVANCED PARTNER

FORTINET
ENGAGE
Partner Specialization
SD-WAN

Six Degrees

To speak to one of our experts about Secure Remote Access, click here.