Secure Remote Access

Reliable remote connectivity for your mobile workforce

Endpoints remain the most common attack surface for ransomware and other malware attacks. Users continue to make mistakes with web, email, and other applications, resulting in security compromises. Application and operating system (OS) vulnerabilities continue to proliferate endpoint devices and are challenging to identify and patch.

Work from home and mobile workers increase this risk as they are not behind corporate next-generation firewalls (NGFWs), and users are inclined to exercise riskier behavior ("out of sight, out of mind"). This risk is greatly increased with users accessing applications while being remote and from locations that may not have needed security controls in place. Additionally, secure VPN connectivity is prone to misconfigurations and disablement by users, which increases risk.

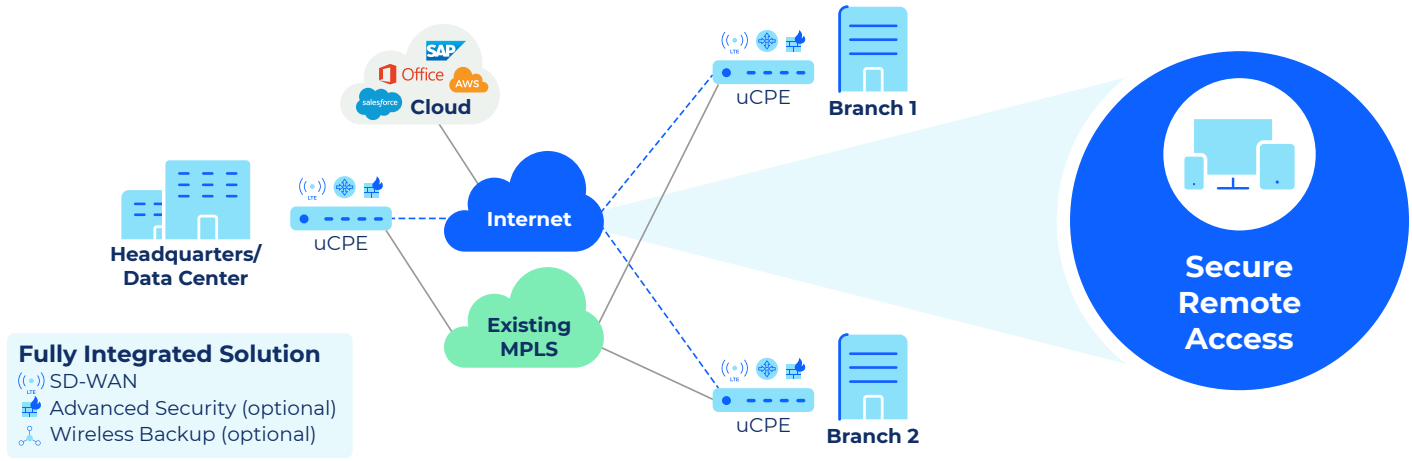
Unrestricted web and application access can sometimes cause distractions and wasted time for employees, as well as security and liability risks for unsanctioned usage, ultimately impacting employee productivity. And, diverse and mobile endpoint environments are challenging to manage, and often lack visibility, including security policy compliance, software inventory, and vulnerability exposure. Remote connectivity through endpoint VPNs is critical for employee productivity (access intranet applications) but is challenging to manage and can impair the user experience.

Extend the Corporate WAN to Remote Workers

Secure Remote Access combines endpoint security, connectivity, and management into a turnkey secure remote solution. Now, remote employees can connect seamlessly to your corporate network from home with secure SD-WAN connectivity for reliable, easy-to-deploy, high-performing VPN connectivity. It also offers cloud scalability, meaning there are no management servers to deploy and maintain.

Leverage our support team 24/7 to help you with configuration guidance and troubleshooting. Plus, our optional 24/7 security operations centers (SOCs) ensure critical endpoint security alerts are promptly identified and responded to for risk mitigation.

Your Network is Now Available at Home or Anywhere



COMCAST BUSINESS | MASERGY

Features & Benefits

Our Secure Remote Access solution is powered by industry leader Fortinet using their Forticlient Endpoint Protection product.

Endpoint Security

- **Advanced threat detection** against exploits and malware leverages latest global threat intelligence to help stop known and unknown attacks.
- **Signatureless machine learning** enables static and dynamic analysis of threats.
- **Anti-exploit engine** detects suspicious payloads from legitimate applications.
- **Cloud sandbox** analyzes all file downloads for threats and leverages global threat intelligence to stop files before impacting endpoints.
- **Ransomware protection** stops unauthorized changes to key files and folders.
- **URL filtering** blocks user access to known malicious websites, such as "watering holes."
- **Agent technology** works well with other endpoint agents, as well as Comcast Business' Managed Endpoint Detection and Response (EDR) offering.

Application Controls

Endpoint application controls block access to malicious or risky traffic, such as botnets, unsanctioned file sharing, proxy, P2P, and remote access apps.

Vulnerability Scanning

Integrated scanning agent identifies OS and application vulnerabilities, and in many cases, enables automated or one-click patching.

VPN

Optional integration with customer-provided Multi-Factor Authentication. Permits or denies split tunnel connectivity on an application-by-application basis, based on defined risk posture and use cases.

Employee Connectivity & Productivity

- **Endpoint VPN client** integrates with Masergy SD-WAN for seamless and effortless remote connectivity.
- **Auto-selecting VPN gateways** ensure high performing user experience.
- **Web URL filtering** blocks or reminds users of unproductive web activity.
- **Policy-based VPN tunnels** split off direct Internet traffic for SaaS for optimal user experience.
- **VPN automatically connects** to simplify user start-up and reduce risk.

Endpoint Manageability

- **EMS management console** provides a unified view and endpoint status across all devices, including Windows, Mac + iOS, Android, and Linux.
- **Software inventory** catalogs all applications by device, to audit vendor software licensing and for security visibility with application risks.
- **Role-based access controls** support multiple customer admin accounts with needed privileges.
- **Endpoint agent** integrates with Active Directory (AD) for consistent and automated policy, and also supports customized groups.
- **Cloud service** managed by Comcast Business is easy and fast to deploy, reducing workload on your IT team.
- **Integrates with Comcast Business ISC customer portal** for unified visibility and consistent security policy across SD-WAN and endpoints.

COMCAST BUSINESS | MASERGY

Comcast Business Network Operations Center (NOC) Services

Secure Remote Access is supported by the same NOC team that delivers Comcast Business' award-winning SD-WAN services to ensure synergy as a turnkey service.

Our NOC services provide:

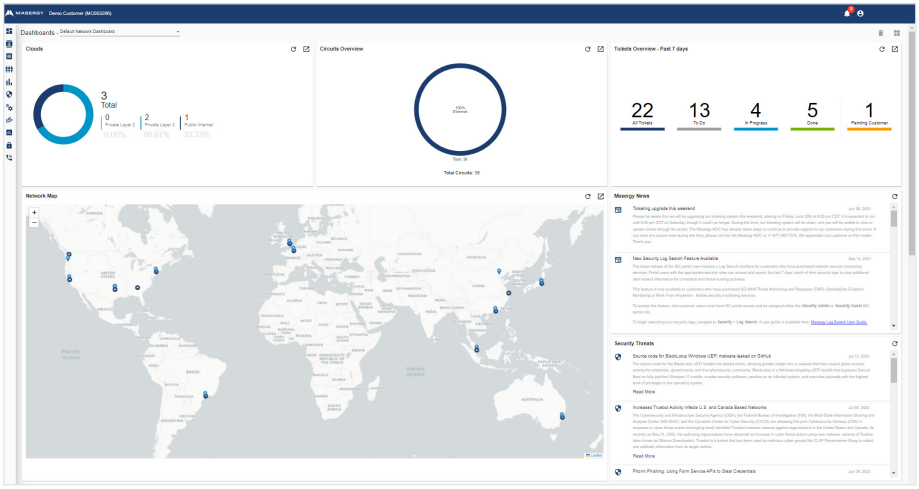
- Configuration for all SD-WAN VPN gateways with Secure Remote Access management service, making deployment easy.
- Baseline endpoint app controls and web filtering policies synchronized with SD-WAN next-generation firewall, which can be fine-tuned for specific customer uses cases.
- Phone support and troubleshooting available 24/7.

Optional Comcast Business Security Operations Center (SOC) Services

Our optional 24/7 SOC services:

- Are staffed by expert endpoint security analysts acting as an extension of your IT team.
- Provide 24/7 endpoint security alert monitoring and response, assuring that critical endpoint security incidents are promptly triaged and mitigated.
- Leverage security playbooks and Security Orchestration Automation and Response platform for effective security process implementation.
- Engage you early during deployment phase to understand your business use cases and fine-tune endpoint security controls and response playbooks.
- Assists with endpoint vulnerability scanning & patching best practices.
- Engages you with general endpoint security best practices.

Masergy Customer ISC Portal



WFA Mobile ISC dashboard widgets are being developed and are expected to be available by the end of December 2023.

Masergy's Unified Management Console combines SD-WAN networking and endpoint protection with at-a-glance widgets and ticketing capabilities.

NIST Cybersecurity Framework

Complementary Capabilities:
Endpoint Protection and Managed Endpoint Detection and Response

Secure Remote Access – Endpoint Protection

- **Identify:**
  - Operating System and application vulnerabilities
  - Endpoint misconfigurations
- **Protect against:**
  - Remote traffic with strong authentication and encryption
  - Split tunneling
  - Advanced malware
  - Risky and malicious website and application traffic
  - Unauthorized data transfer on removable media

Managed Endpoint Detection & Response

- **Detect:**
  - Endpoint security protection failures
  - Unknown or suspicious processes and other attacker endpoint malicious activities
- **Respond:**
  - Remove suspicious endpoint processes and activities
  - Quarantine infected endpoints for remediation
- **Recover:**
  - File roll-back to recover corrupted/ encrypted files
  - Expert 24/7 EDR analyst support for incident response and mitigation

COMCAST BUSINESS | MASERGY

Ordering and Pricing

Secure Remote Access comes in three versions, with pricing dependent upon total endpoint devices under management:

	OPTIONS		
Capabilities	VPN	VPN + EPP	VPN + EPP + SOC
Masergy NOC Services			
Expert integration, configuration, and deployment of SD-WAN and endpoint VPN	●	●	●
Baseline Web filtering and App Control (EPP option) policy deployment with customer support for fine-tuning	●	●	●
24/7 expert phone support and troubleshooting	●	●	●
Endpoint Security Hygiene & Connectivity			
Central management via cloud EMS	●	●	●
Central logging and reporting	●	●	●
IPSEC and SSL VPN with MFA	●	●	●
Web Filtering	●	●	●
Vulnerability Scanning and Patching Agent	●	●	●
Next-Gen Antimalware Security			
Machine Learning Next Gen AV		●	●
Ransomware Protection		●	●
Application Firewall		●	●
Software Inventory		●	●
Cloud Sandbox		●	●
Automated Endpoint Quarantine		●	●
Removable Media Control		●	●
Masergy 24/7 SOC Services			
24/7 SOC Incident Monitoring & Response			●
Endpoint security best practices consultation & configuration			●
Endpoint security policy tuning and adjustments			●
Assistance with vulnerability scanning & best practices			●

Supported Platforms and Features

	PLATFORMS				
Features	Windows	MacOS	Android	iOS	Linux
Endpoint Security Hygiene & Connectivity					
Endpoint Telemetry	●	●	●	●	●
Web Filter	●	●	●	●	
Compliance Enforcement	●	●	●	●	●
Endpoint Scanning and Remediation	●	●			●
Remote Logging and Reporting	●	●		●	●
IPSec VPN	●	●	●	●	
SSL VPN	●	●	●	●	●
Windows Active Directory SSO Agent	●	●			
Antivirus	●	●			●
Cloud-based Threat Detection	●	●			
Cloud Sandbox	●	●			
Automated Endpoint Quarantine	●	●			
AntiExploit	●				
Application Firewall	●	●			
Forticlient Forensic Analysis	●	●			●
Removable Media Control	●	●			●

COMCAST BUSINESS | MASERGY