

# CHECK POINT REMOTE ACCESS VPN



Remote work is the new norm. Efforts to slow the spread of COVID-19 accelerated the transition of employees working from home and accessing corporate resources securely through various VPN (Virtual Private Network) technologies. In a recent Gartner CFO survey [1], 74% of companies said they intend to shift employees to work from home permanently.

Check Point Remote Access VPN provides users with secure, seamless access to corporate networks and resources when working remotely. Privacy and integrity of sensitive information is ensured through strong multi-factor authentication, endpoint system compliance scanning and encryption of all transmitted data.

## Simple and Secure Corporate Access from Windows and macOS

### SIMPLE

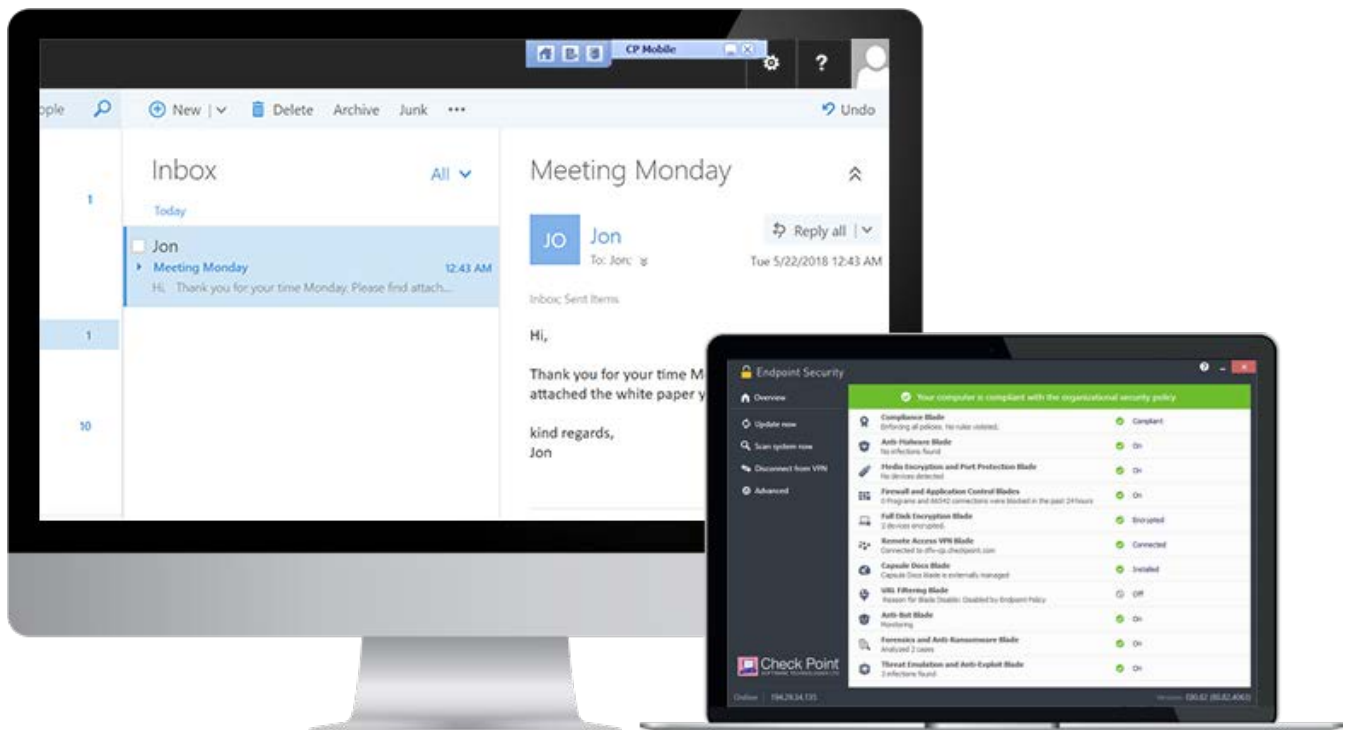
Easy access for remote workers – secure connectivity for smartphones, tablets, PCs and laptops

### SECURE

Communicate securely with proven encryption technology, and multi-factor authentication

### UNIFIED

Deploy and manage on your existing security gateways from one unified console



SECURE YOUR EVERYTHING™

## SECURE REMOTE ACCESS

### COMPLIANCE SCANNING

Endpoint compliance verifies the security level of the endpoint, and reports back to the Security Gateway. The gateway can allow connectivity to specific network resources, based on compliance level.

### DEPLOYMENT OPTIONS

Install our endpoint VPN client in one of three options.

1. Included in Endpoint Security (Windows, macOS)
  - Firewall
  - Application Control (not available on macOS)
  - Remote Access VPN
  - Compliance
2. Standalone Check Point Mobile for Windows
  - Remote Access VPN
  - Compliance
3. Standalone SecuRemote
  - Remote Access VPN

### CENTRAL MANAGEMENT

Remote Access VPN is centrally managed, enabling central policy administration, enforcement and logging from a single, user-friendly console. Centralized management offers unmatched leverage and control of security policies.

### MOBILE ACCESS OPTION

The Web Portal is best for connecting securely to corporate resources from a web browser. Through an integrated web portal, users can access native corporate applications including web-based resources, shared file and email. Administrators can customize the design of the web portal to match their corporate brand identity.

### SPECIFICATIONS

#### Secure Access

- Full IPsec VPN connectivity
- Compliance checks

#### Authentication Support

- Username/Password (including cached passwords)
- SecurID
- RADIUS Challenge/Response
- CAPI software and hardware tokens
- P12 certificates

#### Seamless Tunnel Establishment, Teardown

- Transparently establish a VPN tunnel upon demand
- Re-establishes connections when roaming
- Automatic tunnel tear down when on the corporate LAN

#### Connect Options

Hotspot detection, Office Mode IP, Split Tunneling, Hub Mode, automatic fallback from NAT-T to HTTPS

### REMOTE ACCESS OPTIONS

#### SSL VPN Portal

Mobile Access Web Portal  
SSL Network Extender for Mobile Access Blade  
Check Point Mobile for iOS and Android  
Capsule Workspace for iOS and Android

#### Layer 3 VPN Tunnel

Endpoint Security Remote Access VPN  
Check Point Mobile for Windows  
Capsule Connect for iOS and Android  
Check Point VPN Plugin for Windows 8.1  
Check Point Capsule VPN for Windows 10

See [SecureKnowledge sk67820](#) for more details.

## Complete Windows, macOS, iOS and Android Security Solutions

### SandBlast Agent

- Sandboxing (Threat Emulation)
- Content Disarm and Reconstruction (Threat Extraction)
- Anti-Ransomware
- Zero Phishing
- Anti-Exploit
- Anti-Bot
- Forensics

### SandBlast Mobile

- Malicious App Detection
- Anti-Phishing with Zero-Phishing
- Safe Browsing
- Conditional Access
- URL Filtering
- Anti-Bot
- Wi-Fi Network Security