

Selecting Secure Remote-Access Technology and Services

Arabella Hallawell, Jay E. Pultz, Mark Nicolett

The fast-growing demand for secure remote access requires a combination of remote-access services and virtual private network solutions, including new SSL-based VPN technology and managed remote-access services.

ANALYSIS

Enterprises must address the need to maintain the security and integrity of networks, applications and data as the number of mobile workers, modes of enterprise connectivity and methods of external access grow rapidly. Delivering secure, "anywhere, anytime" access to remote workers requires enterprises to protect:

- Enterprise computing assets
- Data on external networks
- Mobile devices (data and connections)

It also requires secure, scalable methods to connect business partners to networked resources.

Encryption is essential to protect the data carried on public networks. Virtual private network (VPN) technology is the primary encryption method. Traditional VPN technology provides strong encryption, but it does not offer the ideal solution for all modes of remote communication. A full-function VPN client consumes too many resources to be practical for all types of mobile devices — for example, the need for a separate login causes problems for mobile handheld users. It also requires a reliable connection to avoid repeated logins following network interruptions.

Secure Sockets Layer (SSL)-based VPNs offer a comparatively lightweight alternative to traditional VPNs. In many ways, they are more suitable for meeting the requirements of mobile users. Enterprises can evaluate SSL VPN vendors using:

- "SSL VPN 1H03 Magic Quadrant"
- "SSL VPN 1H03 Magic Quadrant Evaluation Criteria"

Secure remote access requires more than VPN software at both ends. Enterprises also must consider a bewildering array of network service providers and brokers to obtain the services that they need to connect, secure and support users outside of their traditional boundaries.

Enterprises can evaluate remote-access vendors using:

- "Managed Remote-Access 1H03 Leaders, Challengers"
- "Managed Remote-Access 1H03 Visionaries, Niche Players"
- "Managed Remote-Access 1H03 Magic Quadrant Criteria"

Arabella Hallawell

Editor in Chief

Security & Privacy

spotlight.feedback@gartner.com

Jay Pultz

Editor in Chief

Enterprise Networking

spotlight.feedback@gartner.com

Mark Nicolett
Contributing Editor
Security & Privacy
spotlight.feedback@gartner.com

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509