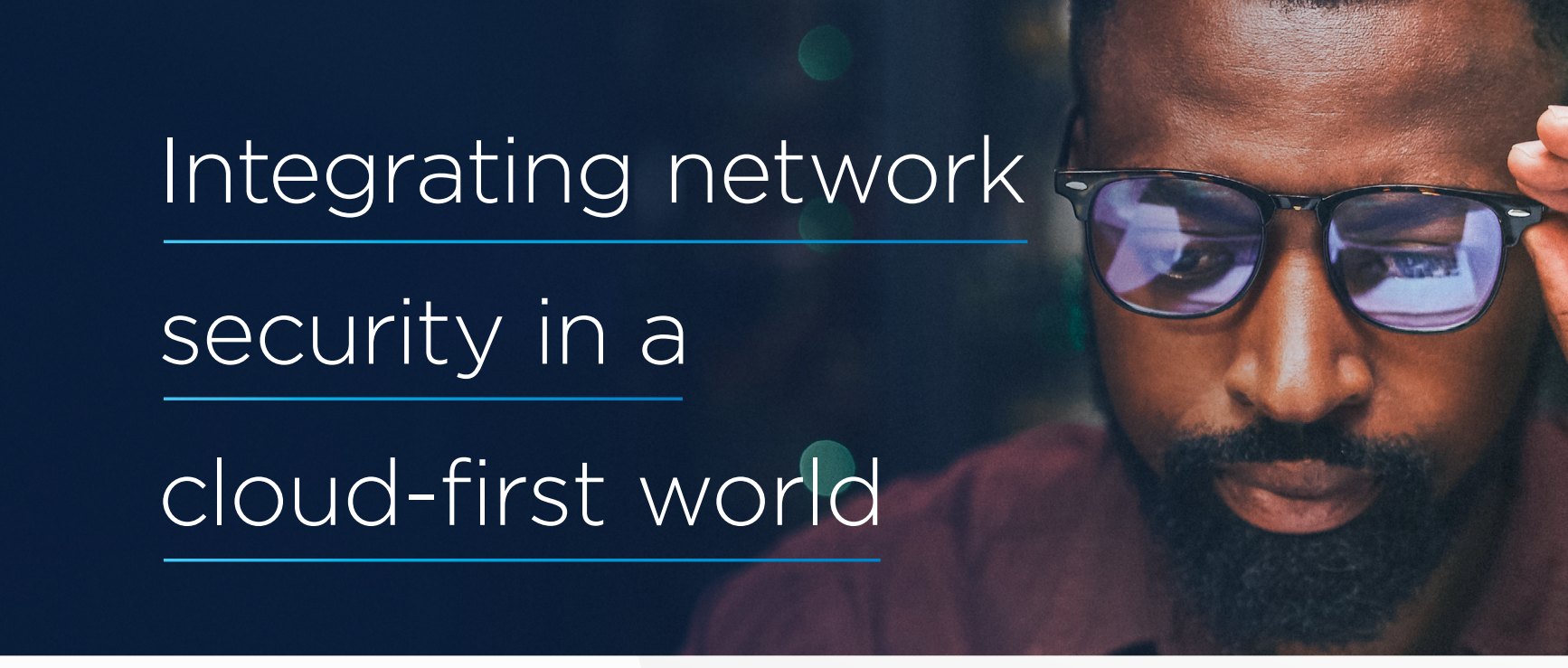
Integrating network security in a cloud-first world



Enterprise networks are transforming, becoming more cloud-dependent while work-from-anywhere access becomes more widespread.

The associated security risks can grow exponentially as the attack surface expands with the number of remote users and cloud apps. Meanwhile, there are more vendors to manage and different security measures to align. Effectively protecting today's networks requires adapting to the evolving ways that employees and organizations do business.

New challenges shaping security

~1/3

Roughly the average number of paid days spent working from home in the first half of 2023.[1]

Remote access has become a fixture of the modern workforce

More employees are accessing sensitive data and applications from outside of corporate networks. Security strategies need to move beyond VPNs alone to strengthen the way they authenticate users and enforce security policies consistently across remote devices.

Personal devices are being used for work

With access to work encouraged — or required — on employee-owned devices, security solutions must be able to monitor a wide range of endpoints from a centralized platform to quickly identify threats.

of employers in one survey require work-related apps to be installed on their employees' personal devices.[2]

of cloud adopters use a hybrid cloud architecture.[3]

Networks are becoming more complex

Technology leaders are frequently challenged to incorporate multiple cloud service providers, cloud-based business applications and on-premises networks into their security strategies. Adopting security solutions designed to work together from a single partner can help prevent gaps and streamline routine management so IT professionals can focus on higher priorities.

Network security in a cloud-driven world

Organizations continue to invest more in cloud-based applications and infrastructure. Protecting them requires new ways to manage access and monitor traffic across all the cloud resources an organization relies on.

of breaches involve data stored in the cloud.[4]

Advanced threats need advanced solutions

Networks and their security challenges will only grow more complex. As users and the cloud-based resources they rely on become more distributed, IT teams need to adapt their approach to keep up with cybersecurity. Meeting these challenges will require new solutions to extend network security into the cloud and wherever employees work.

But just because security is becoming more complex doesn't mean your service provider ecosystem needs to be. A single provider can remove the hassle of juggling multiple providers and configuring your business to work with different solutions. Plus, they can ensure network components integrate seamlessly for more effective protection.

Learn more

1. Jose Maria Barrero, Nicholas Bloom, Shelby Buckman and Steven J. Davis, "Survey of Workplace Arrangements & Attitudes October 2023 Updates," WFH Research, October 9, 2023.
2. "71% of Employees Store Sensitive Work Passwords on Personal Phones," Security Magazine, April 3, 2023.
3. "2023 State of the Cloud Report," Flexera, 2023.
4. "Cost of a Data Breach Report 2023," IBM, 2023.

About Spectrum Enterprise®

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

SE-MS-IG013

Spectrum ENTERPRISE™