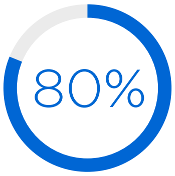
GUIDE

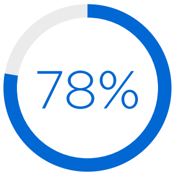
Secure your cloud-based future

Learn how managed solutions can help you guard against evolving threats

Spectrum ENTERPRISE®



of breaches involve data in the cloud or hybrid environments.[2]



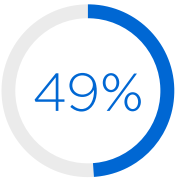
of executives say their organization does not have the in-house skills to fully achieve their cybersecurity objectives.[4]

Business leaders face a complex web of challenges as they seek to protect users, data and systems. It starts with staff who are more distributed than ever, working from remote locations on a dizzying array of devices. More than 75% of those whose jobs permit teleworking do so at least some of the time.[1] In response, organizations are turning to cloud-based architectures in greater numbers, drawn by the efficiency, resiliency, expediency and ubiquity these solutions offer.

The transition to cloud-based and software as a service (SaaS) applications brings with it new partnerships and endpoints. It also means venturing beyond the protection and performance of traditional private networks. While offering benefits from scalability to performance, moves such as the addition of remote teams, bring-your-own-device (BYOD) flexibility and cloud-based apps can introduce new and serious vulnerabilities as part of an expanded attack surface. The heightened risks include everything from costly data breaches to distributed denial of service (DDoS) attacks, with the fallout potentially impacting your reputation and revenue. In 2023, 80% of breaches involved data in the cloud or hybrid environments, inspiring 63% of organizations to plan an increase in security investments.[3]

Organizations can partner with multiple vendors to help develop a security response. However, a strategy that relies on a collection of disparate systems can expose gaps in protection, especially if those vendors or their systems are unable to work together, thus reducing network visibility and control. In addition, busy IT teams may lack the resources, time and expertise to analyze security alerts and take real-time action to mitigate constantly evolving threats. This becomes an especially important consideration as your organization grows.

Your vulnerabilities include more than a distributed workforce and moving your data to the cloud. A comprehensive, layered security approach will also help protect your people and property. This requires integration of technologies, such as smart cameras and environmental sensors, that monitor your facilities and other vital physical spaces to safeguard them against damage, theft and accidents.



of executives expect the number and size of cyberattacks on their accounting and financial data to increase.[5]

As security threats grow in number and sophistication, failure to keep up can not only endanger your data, users and systems but also undermine your ability to meet key industry regulatory demands. These include cybersecurity insurance requirements and compliance standards such as the Health Insurance Portability and Accountability Act (HIPAA) in healthcare and the Payment Card Industry Data Security Standard (PCI DSS) for organizations that accept credit card payments.

$4.88M

The average global cost of a data breach as of 2024, a 10% increase over the previous year.[9]

The threats are real — and so are the costs

Given the expanding attack surface faced by organizations, it is little surprise that security has shifted from a primarily technological concern to a critical business issue. In one survey, CIOs cited cybersecurity as their top priority.[6] Answering this demand requires investment in a range of related needs, including continual security testing and improvement as well as planning and comprehensive training. It follows that related security costs are growing — 80% of business and technology executives expected to increase their cybersecurity budgets for 2024.[7] Gartner forecasted that global security and risk management spending would jump by more than 14% in 2024.[8]

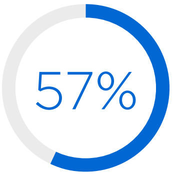
Relying on a single provider that can incorporate networking and security in one platform, including safeguarding data in clouds, can ensure protection remains up to date and help identify vulnerabilities before bad actors can exploit them. With full visibility into the network, that provider can further mitigate threats by delivering near-real-time security alerts about suspicious activity.

Save time and resources with managed services

A complete security strategy requires a holistic, flexible approach that can scale and adapt to changing risks and threats, including those related to an increasingly dispersed technology environment. As the network edge expands away from the protection and performance of your private network, you need advanced ways to manage risks across a growing number of connections, endpoints and locations. IT must mitigate the security risks of a complex and spreading attack surface and expand and simplify protection to confidently implement a cloud and distributed architecture.

Managed services address challenges through customized, managed solutions that evolve with your business and promote peace of mind. They can help you do the following:

- Advance your cybersecurity strategy.
- Automate protection and governance.
- Support "work anywhere" mobility for employees.
- Mitigate threats and enable secure access from users and devices to applications operating outside the network.
- Integrate cloud-based security without introducing latency in network traffic, specifically to SaaS applications.



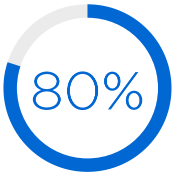
of workers say cutbacks at their organization put them at moderate or extreme risk of cybersecurity attacks.[10]

Software-defined and cloud-based security can offer the anywhere, anytime protection you need for your data and applications. For example, firewall as a service (FWaaS) offers cloud-based protection for employees across locations and can scale as your needs change. Working with the right managed solutions partner helps you navigate the complexity of hybrid cloud networking and security services and keep pace with rapidly changing network, security and regulatory conditions.

As you move to a cloud-based architecture, your IT team needs a single security policy throughout a distributed environment for threat detection, traffic inspection and user access. Success requires investment and IT expertise. Managed cloud security services can help by consolidating vendors and technologies to improve flexibility, lessen the burden on IT and reduce your total cost of ownership (TCO). Services can span solutions to protect remote network access such as zero trust network access (ZTNA). These solutions can help guard against malware and data breaches with cloud-based firewalls and unified threat management (UTM) for protection on-premises and for remote users. Cloud access security brokers (CASBs) have also become essential to establishing secure access to cloud-based applications and protecting data. Additionally, these solutions commonly include installation and continuous updates to further strengthen your security posture and support resource-constrained IT teams.

Bring networking and security together

Effective security can be built on the foundation provided by secure access service edge (SASE). This model combines networking and security, offering a cybersecurity response for dispersed technology environments. SASE blends a software-defined wide area network (SD-WAN), for unified access for branch or remote offices and network controls, and secure service edge (SSE), a cloud-based security platform centered on the identity of users, devices and operations. This combination of technologies offers a powerful framework to enable easy access to resources inside and outside the network while meeting performance demands and blocking sophisticated security threats.



of enterprises will adopt a strategy to unify web, cloud services and private application access using a single vendor's SSE platform by 2025.[11]

Spectrum Enterprise® is a leading networking services provider that offers SASE solutions to make it easier to deliver defense in depth while creating a unified security policy. IT administrators benefit from improved visibility into their networks from a single portal, providing control across the entire organization. Spectrum Enterprise offers a more integrated and comprehensive security strategy, minimizing risk and vulnerability across your business and remote workforce.

Cloud Security with Cisco+ Secure Connect

Cloud Security from Spectrum Enterprise offers a centralized, streamlined platform to implement your security priorities across every cloud and device. Defend your authorized users and data both in the cloud and on your network. Deliver a consistent, universal security experience for remote and office-based workers with solutions designed to mitigate today's security threats and prepare for tomorrow's with automated alerts. Solutions range from cloud-based firewalls to secure web gateways (SWGs) and ZTNA. A CASB gives users secure, direct access to cloud applications, helping simplify cybersecurity without compromising performance.

By implementing Cloud Security, you can stop backhauling remote traffic through the corporate WAN to apply security policies at a central gateway, thereby reducing latency and enhancing the user experience. The service can also provide welcome assistance to busy IT teams by permitting immediate visibility into devices, network traffic and network activity and threats via a single portal. This improved oversight helps protect against data loss and regulatory violations in an increasingly complex hybrid cloud environment.

SASE explained: A glossary for evolving network security

Even for seasoned professionals, modern security solutions can quickly turn into an alphabet soup of abbreviations, jargon and concepts that rapidly change as security needs shift. Bring your team up to speed on the latest technologies with this fact sheet on SASE terminology.

Read the fact sheet

Spectrum Enterprise offers a range of products and services that, along with Cloud Security, can be used to help your organization build and apply a SASE framework to your network. We can assemble, integrate and maintain the solutions for you, empowering your teams to achieve a simpler, yet stronger, security experience.

Other key security products	Security benefits
Secure Access with Cisco Duo	• Strengthen secure password policies, provide an easy and consistent login experience and address regulatory or industry compliance mandates with multi-factor authentication (MFA). • Protect employees by establishing more-secure access policies by user and device, regardless of location. • Achieve consistent, secure authentication across your cloud applications while strengthening BYOD policies and remote work security. • Help guard against data loss, regulatory violations and unauthorized access to sensitive systems.
Managed Network Edge	• Integrate security-first networking with this secure, all-in-one networking solution powered by Cisco Meraki and developed for multi-site and single-site organizations. • Simplify the transition to a hybrid network architecture built around advanced SD-WAN technologies. • Bolster protection by adding layers of network security with UTM for a better overall digital experience. • Strengthen security through switching, an advanced firewall, wireless networking, smart cameras and environmental sensors.
Enterprise Network Edge	• Rely on sophisticated configuration and a managed, secure SD-WAN to deliver exceptional performance. • Support high-capacity data center connections, large workloads and hybrid SD-WAN networks. • Seamlessly integrate public clouds and reduce reliance on legacy networks. • Strengthen security through switching, an advanced firewall, wireless networking, smart cameras and environmental sensors.
DDoS Protection	• Help guard against attacks to your network and applications, and respond to and mitigate threats with a scalable DDoS solution that easily and seamlessly expands as your needs change. • Harness adaptive intelligence to quickly evaluate your expected network activity and identify threats attacking your dedicated fiber internet service. • Automatically begin attack mitigation and reroute traffic to help keep your resources available.

Secure your network with Spectrum Enterprise

Cloud-based architectures allow you to become more flexible, efficient and adaptable when your needs change. They can, however, pose new security challenges as sensitive data moves from the safety of on-site servers to third-party resources accessed through the internet. Spectrum Enterprise offers a broad portfolio of powerful, high-performance fiber connectivity and security services that can help you successfully modernize your network.

We can help you elevate the user experience and simplify network management through customized, cost-effective managed solutions and ongoing maintenance that evolve with your business. Consult our experts and explore professional integration services to determine the optimal configuration for your needs with midsized and enterprise security solutions backed by 100%, 24/7/365 U.S.-based support.

Learn more

1. Kim Parker, "About a Third of U.S. Workers Who Can Work from Home Now Do So All the Time," Pew Research Center, March 30, 2023.
2. "Cost of a Data Breach Report 2024," Ponemon Institute and IBM Security, 2024.
3. Ibid.
4. "Global Cybersecurity Outlook 2024," World Economic Forum, January 11, 2024.
5. "Almost Half of Executives Expect a Rise in Cyber Events Targeting Accounting and Financial Data in Year Ahead," Deloitte, February 2, 2023.
6. "2024 CIO Leadership Perspectives," Evanta, March 2024.
7. Roman Kolodiy, "How to Plan an Effective Cybersecurity Budget in 2024," Tech Magic, April 12, 2024.
8. "Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024," Gartner press release, September 28, 2023.
9. "Cost of a Data Breach Report 2024."
10. "ISC2 Reveals Growth in Global Cybersecurity Workforce, But Record-Breaking Gap of 4 Million Cybersecurity Professionals Looms," ISC2, October 31, 2023.
11. "Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23," Gartner press release, June 21, 2022.

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.