GUIDE

Deploy strong defenses to actively protect your network

Without reliable authentication, your workforce is at risk of being targeted by cyberthreats

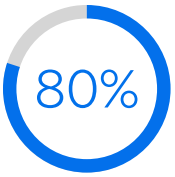
Spectrum BUSINESS®

Business leaders confront increasing security vulnerability and more sophisticated threats as networks expand and become more complex. As remote and hybrid work extend the network to every connected device your workforce employs, each endpoint represents possible access for a cyberattack. With more than 75% of employees who can choose to work remotely doing so at times, safeguarding the expanded attack surface poses a daunting and enduring challenge.[1]

Almost 90%

of organizations are using multi-cloud architectures.[2]

Many organizations have adopted cloud-based architectures and software as a service (SaaS) to support increasingly distributed employees, partners and contractors who need reliable, low-latency access to applications and systems to be productive. Because of the efficiency, resiliency, expediency and ubiquity of cloud-based architectures, almost 90% of organizations migrating from traditional on-premises and private networks have adopted multi-cloud architectures.[3]



of breaches involve data in the cloud or hybrid environments.[5]

Though the cloud offers scalability and performance advantages, it also introduces vulnerabilities. Notably, the growing number of services, applications and users connecting to the network with company-owned and bring-your-own-device (BYOD) options make the cloud a ripe target with many potential access points — as of 2024, 80% of breaches involved data in the cloud or hybrid environments.[4] For modern networked organizations with users connecting from anywhere to access data, cloud services and applications, it's imperative to establish secure access policies that continually validate users and devices, regardless of location.

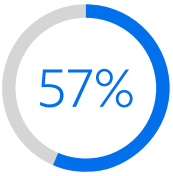
Secure user access limits network entry points

Validating user identities, securing hybrid and remote workers, as well as identifying and mitigating threats is vital to safeguarding your network from the data center to the cloud. For example, a single user who employs easily guessable passwords (the most common passwords in 2024 were **12345**, **123456**, **123456789**, **qwerty** and **password**[6]) or manages passwords unsafely can unintentionally make your network vulnerable to bad actors that could subject your organization to attacks with real business implications.

$4.88M

The average cost of a data breach.[7]

Risks to your revenue and reputation lurk with each cyberthreat, from data breaches to distributed denial of service (DDoS) attacks. The average data breach cost $4.88 million as of 2024, a 10% increase over the previous year.[8] The threats show no signs of easing, with 49% of executives expecting cyberattacks on accounting and financial data to increase.[9]



of workers say cutbacks at their organization put them at moderate or extreme risk of cybersecurity attacks.[13]

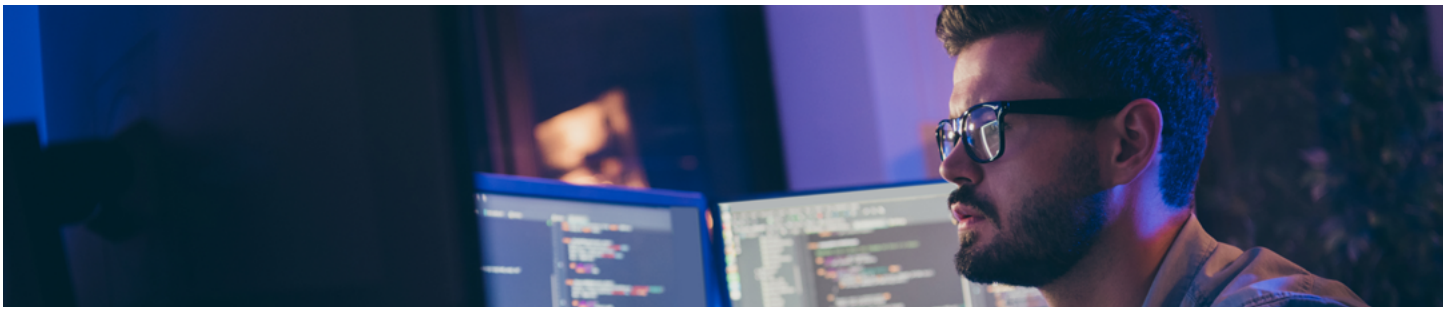
Managed security services maximize protection

Actively guarding against these relentless threat actors can overtax resource-constrained IT staff. There's consensus that cybersecurity is important — CIOs ranked cybersecurity their top priority for the last three years[10] — but intention does not always match operational capabilities. Workers at 57% of organizations say cutbacks put them at moderate or extreme risk of cybersecurity attacks, indicating the gravity of the staffing challenge.[11] Moreover, 78% of executives say their organization does not have the in-house skills to reach their cybersecurity objectives.[12]

In response to escalating cyberthreats and persistent IT resource limitations, organizations often look outside for help. Selecting a technology partner you trust is critical to developing an effective security strategy that protects your network from unauthorized access, has the flexibility to adapt as risks evolve and considers the big picture to safeguard your entire network.

The right partner can help you implement managed cloud security, automate your monitoring, protection and governance and provide resources and expertise to analyze real-time security alerts and take action. A managed security solution can also support a consistent user experience to help optimize worker productivity while simplifying and easing the security management load for IT staff and providing peace of mind.

Spectrum BUSINESS®



A critical aspect of cloud-based security is controlling access to your network and apps so that only authorized users and devices gain entry. Employing multiple tactics to protect your network is important when controlling who has access. These include:

Validate user identity

Confirming users' identities ensures that only authorized entities can access your network. Passwords alone are not sufficient. Multi-factor authentication (MFA) provides another means for preventing credentials from becoming compromised. It requires a second authentication factor, such as biometric verification or an SMS code, to verify users' identities before permitting access to services, applications or data.

Secure your workforce

Validating users once and then granting unfettered access to network resources without further verification can leave you vulnerable. Adopting a zero trust network access (ZTNA) approach to security ensures continuous verification of each network user's credentials, placing the onus on those users to prove and re-prove they possess the necessary authorization. While safeguarding the network, ZTNA ensures employees have secure access that considers the device being used and the location of the user — enabling the business to monitor who and what devices are using the network at any time.

Identify and mitigate network threats

Visibility into the network is key to identifying threats and then taking steps to mitigate them. Implementing robust cloud-based security enables continuous monitoring across the network to assess services, applications, users and devices from the data center to the cloud to the edge. Visibility can extend to individual users and devices to monitor who accesses specific applications and apply policies that provide least-privileged access for users, devices or locations.

Securing access is particularly important for organizations that must meet regulatory compliance standards, such as HIPAA, FERPA, SOX and PCI DSS, which govern how data is handled. Denying or restricting network access to people who should not be permitted or should be limited to only specific files is key to effective cloud data security.

Delivering protection with performance

Locking down access to your network may lower your risk of a potential breach. However, even the strongest defenses should allow your workforce to remain productive and efficient. For managed security services to strike the right balance with secure access requires a trusted partner with experience, expertise and customizable security solutions.

Partnering with Spectrum Business® to adopt Secure Access with Cisco Duo can help you integrate and manage your network with on-call support to give you peace of mind. This fully managed, cloud-based security solution can help protect your organization from unauthorized access to sensitive systems, regulatory violations and data loss that can disrupt your business. The easy-to-use identity management platform can help streamline policy enforcement for application access and usage, while enabling a consistent, accessible experience for workers, regardless of location.

Secure Access from Spectrum Business includes MFA capabilities to validate users and devices. It offers IT teams enhanced visibility into their networks and potential threats with a dashboard to view and manage access for all users and devices. It can also help provide consistent, secure authentication, with experts available to guide configuration and provide ongoing maintenance and support.

In addition to Secure Access, Spectrum Business offers a range of network modernization solutions to help manage and guard your IT network infrastructure. These include:

SOLUTION	FEATURES
Cloud Security with Cisco+ Secure Connect	• Streamline IT operations with a centralized platform to implement your security priorities across locations, clouds and devices. • Enforce security measures for corporate and personal devices with ZTNA and a cloud-based firewall. • Eliminate the need to backhaul remote and branch traffic through a corporate WAN to apply security policies. • Give users secure, direct access to cloud applications using a cloud access security broker (CASB).
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 software-defined wide area network (SD-WAN) technologies. • Bolster protection by adding layers of network security with unified threat management (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.

Spectrum BUSINESS®

Cisco Partner
Gold Provider

Safeguard access to your network with Spectrum Business

Locking down access to your network may lower your risk of a potential breach. With Spectrum Business, you can confidently authenticate users and support remote work through customized, cost-effective managed security solutions and ongoing maintenance that evolve with your business. Consult with 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. "2024 State of the Cloud Report," Flexera, 2024.
3. Ibid.
4. "Cost of a Data Breach Report 2024," Ponemon Institute and IBM Security, 2024.
5. Ibid.
6. Paulius Masiliauskas, "Most Common Passwords: Latest 2024 Statistics," Cybernews, November 27, 2023.
7. "Cost of a Data Breach Report 2024."
8. Ibid.
9. "Almost Half of Executives Expect a Rise in Cyber Events Targeting Accounting and Financial Data in Year Ahead," Deloitte, February 2, 2023.
10. "2024 CIO Leadership Perspectives," Evanta, March 2024.
11. "ISC2 Reveals Growth in Global Cybersecurity Workforce, But Record-Breaking Gap of 4 Million Cybersecurity Professionals Looms," ISC2, October 31, 2023.
12. "Global Cybersecurity Outlook 2024," World Economic Forum, January 2024.
13. "ISC2 Reveals Growth in Global Cybersecurity Workforce."

Spectrum BUSINESS®