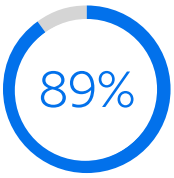
GUIDE

Secure your network with modern solutions

Help guard against attacks and efficiently enable remote work

Spectrum BUSINESS®

Today's IT leaders face multidimensional security challenges as corporate networks and their would-be attackers become more sophisticated. Threats can now include the use of AI to generate malicious code and automating processes to exploit vulnerabilities. These threats can become even more severe if IT can't keep pace with safeguarding the growing number of connections to the network that open more avenues for malware and unauthorized access to data.



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

Attack surfaces are changing and growing as trends evolve. Cloud computing and hybrid networks are nearly ubiquitous, with 89% of organizations using multi-cloud architectures.[1] The growth of the remote workforce has increased the number of endpoints cybercriminals can attempt to penetrate, while bring-your-own-device (BYOD) programs present additional avenues for security breaches. At the same time, hackers are developing more powerful distributed denial of service (DDoS) attacks that can bombard networks and applications with greater volumes of malicious traffic than ever before.

Navigating these challenges requires a new set of defenses for networks and resources in the cloud. Organizations that fail to counter evolving cyberthreats can pay a high price. The global average cost of a data breach in 2024 was $4.88 million, a 10% increase over 2023 and the highest total ever.[3] Breaches can lead to detrimental reputational consequences, including high legal and financial costs, as well as decreased consumer trust. For industries that depend on data in motion — such as digital commerce, manufacturing and utilities — downtime can mean lost revenue and data, employee dissatisfaction, as well as critical business disruptions. As a result, security teams are adopting a defense-in-depth strategy, with layers of protection throughout a network.

Spectrum BUSINESS®

Here are four key actions companies should consider to help solidify their enterprise network security foundation as threats evolve:

Adopt zero trust network access

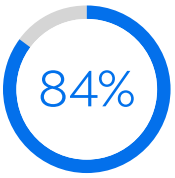
Today, a single enterprise data center is no longer the focal point for user access.

Network security has traditionally authenticated users once and then allowed them unfettered access to all authorized network resources without further verification. Today, a single enterprise data center is no longer the focal point for user access and this approach is increasingly problematic given the expanded attack surface caused by connect-anywhere work and multi-cloud networks.

To safely allow users to log in anywhere, organizations are using a new framework: zero trust network access (ZTNA), a solution that continuously verifies the credentials of network users. Multi-factor authentication (MFA) provides another measure to help prevent unauthorized network access, especially through compromised credentials. It requires a second source of authentication to verify users' identities before they access sensitive data.

Secure Access with Cisco Duo from Spectrum Business® enables validation of users, devices and locations. 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. Secure Access is a fully managed, cloud-based MFA security solution, with experts available to guide configuration and provide ongoing maintenance and support, easing the workload of network administrators.

Bolster cloud security



of organizations cite managing cloud spend as a top cloud challenge.[5]

The popularity of cloud architectures — with their benefits that include efficiency and resiliency — has not escaped the notice of cybercriminals. About 40% of all breaches involve data distributed across multiple environments, such as public clouds, private clouds and on premises.[4]

IT teams need to manage the added complexity of securing their hybrid cloud network to maintain consistent security policies throughout the distributed environment. Because cloud-based resources are so essential to many organizations' operations, enterprise security solutions must be effective and seamless. Cloud security should be integrated into the network without introducing latency or impeding users' access to applications.

Spectrum Business Cloud Security with Cisco+ Secure Connect offers a centralized, streamlined platform to implement your security priorities across every cloud and device. As a fully or co-managed solution, it also streamlines network security management for your team with continuous monitoring, regular updates and adaptation to new threats.

Cloud Security enables ZTNA to verify users and grant access to specific applications on-premises and clouds based upon user, device and location. This solution uses a cloud access security broker (CASB) to detect all cloud applications in use across the organization and apply uniform IT policies and access controls to those applications for workers, partners and contractors. Its data loss prevention capabilities can help identify and stop outflows of large data sets. Additionally, the solution's secure web gateway (SWG) and cloud firewall help identify and stop malware and advanced threats before they penetrate a network. An SWG with a cloud-based proxy can also enforce acceptable use policies across locations.

Spectrum BUSINESS®

When paired with software-defined wide area network (SD-WAN) solutions, such as Managed Network Edge and Enterprise Network Edge from Spectrum Business, Cloud Security can help organizations establish a secure access service edge (SASE) framework for their security. Multiple protections within the SASE framework make it easier to deliver defense in depth while creating a unified security policy. IT administrators also benefit from visibility of their networks from a single portal, providing control across the entire enterprise.

Read our guide

SASE explained: A glossary for evolving network security

Solutions to help streamline and simplify networking and security management

Managed Network Edge
Delivered over the Cisco Meraki platform, this all-in-one solution offers security features, routing, SD-WAN, WiFi, switching, smart cameras and environmental sensors. It allows IT teams to operate anywhere by giving them secure, remote access to their network services. Unified threat management (UTM) capabilities also add additional layers of network security.

Managed Network Edge eases the administrative burden for IT security teams with automated updates, full visibility through an intuitive portal and fully or co-managed options for deployment and operation. It also offers solutions to streamline and secure network access for distributed teams. Empower mobile workers with simple, secure access to your network from any device, at any time, in any location while protecting your organization with the platform's Remote Access solution.

You can also give your at-home workers the same network performance, security and data prioritization they experience while at the office with an easy-to-install network appliance. The Managed Network Edge Teleworker gateway is a portable, easy-to-install device that allows remote employees to connect safely to a corporate network.

Enterprise Network Edge
Enterprise Network Edge gives multi-site and single-site organizations that require security-first networking the ability to transition to a hybrid network architecture built around advanced SD-WAN technologies. Powered by Fortinet, Enterprise Network Edge offers access to multiple cloud instances and advanced security features with throughput speeds up to 100 Gbps, while also supporting distributed workforces. It delivers a better digital experience for your teams and creates a flexible network that can quickly meet the evolving needs of your organization.

Additional capabilities bring network functions like SD-WAN, routing, switching and WiFi into a multi-cloud-ready platform for easier management. With fully managed or co-managed options, IT professionals can oversee the network components they choose and leave the rest to Spectrum Business. Our experts take a consultative approach to solution design, implementation and support to meet each customer's unique needs.

Spectrum BUSINESS®

Establish proactive protection to thwart DDoS attacks

Controlling access is one part of a comprehensive defense-in-depth strategy. However, it's also critical to defend against volumetric DDoS attacks that flood the network with malicious traffic, denying user access to essential applications and information.

Only 25% of respondents feel their organization is fully equipped to manage DDoS attacks.[6] These attacks overload servers with malicious traffic and can make websites and cloud-based services unavailable — denying employees and customers access to essential resources.

A solution that redirects malicious traffic before it can cause a disruption is a critical piece of a comprehensive network security strategy.

Spectrum Business offers optional DDoS Protection alongside our dedicated internet solutions to automatically identify and mitigate threats. Powered by Radware, DDoS Protection uses machine learning and advanced analytics to identify anomalies in traffic. It helps minimize the impact of a DDoS attack by detecting, redirecting and mitigating malicious traffic — helping keep the network up, running and available for the employees and customers who need it.

Streamline and simplify security management

To respond to increasingly complex and ever-changing network security challenges and user needs, organizations are increasing their security investments. In fact, 63% of organizations say they are budgeting more for security as a result of a data breach.[7] However, allotting money to a different solution for each problem can create its own challenges. Working with too many vendors can make it difficult to see the holistic status of the network at a glance and can lead to gaps in security.

Because it is essential for all parts of a security solution to work together, IT professionals are turning to cloud-based platforms that allow them to manage their networks from any location, maintain consistent security policies and monitor potential threats across multiple clouds, devices and locations. Many organizations also benefit from managed security services that take over routine system maintenance, freeing the IT security team for more important tasks.

Spectrum BUSINESS®

The right partner for the future of security

Spectrum Business has the capabilities and experience to customize security solutions that are software defined and cloud delivered. Our products are designed to seamlessly work together, lessening security risks while enabling IT teams to confidently implement their cloud and distributed architectures and support employees working from all locations.

With Spectrum Business as your partner in developing and maintaining either fully or co-managed solutions, your IT security team can direct its attention to other business-critical matters. We partner with our customers to design custom solutions that best fit their needs, backed by our exceptional service and 100%, 24/7/365 U.S.-based support. Whether your current focus is on strengthening user authentication, supporting remote work or securing a hybrid cloud network, we can help.

Learn more

1. "2024 State of the Cloud Report," Flexera, 2024.
2. Ibid.
3. "Cost of a Data Breach Report 2024," IBM, 2024.
4. Ibid.
5. "2024 State of the Cloud Report."
6. "Why Multi-Layered Defense is Critical in Application Security," Dark Reading, OPSWAT, August 2024.
7. "Cost of a Data Breach Report 2024."

Spectrum BUSINESS®