GUIDE

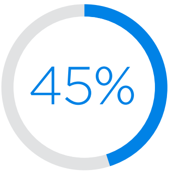
SECURE DISTRIBUTED EMPLOYEES AND CLOUD RESOURCES

How to easily and flexibly extend protection for your expanding network edge.

Spectrum ENTERPRISE™

Security threats have migrated to the cloud just as quickly as business applications and corporate data.

In fact, one study found nearly half of known security breaches occurred in cloud resources.[1] Trends toward remote work, business use of personal devices and tighter regulatory requirements are challenging IT leaders to build security strategies that go well beyond the protection of their private networks and in-house servers.



of data breaches in 2022 occurred in the cloud.[2]

Organizations must protect not only their internal systems, but also data and employee credentials that are spread across an ever-expanding attack surface of cloud-based architectures. This guide explores the benefits and resulting challenges that come with more distributed computing, as well as new approaches to security that can strengthen protection while making it simpler to manage.

Fast changes, new risks

The shift away from centralized networks and private data centers shows no signs of slowing. Nearly three-quarters of companies surveyed by KPMG in 2022 said they are migrating strategic workloads to the cloud.[3] The benefits are apparent to employees who can now conduct their work anywhere, across a range of devices, using software as a service (SaaS) to collaborate on projects that would have required the resources of a corporate office not long ago. Business leaders, likewise, can shift technology budgets from large capital costs to ongoing operating expenses that scale easily as their needs grow.

This often leaves IT with the responsibility for managing legacy networks and the integration of cloud services with widely varied security features. With limited resources, IT teams can quickly fall behind on policy enforcement, updates and network maintenance as the landscape of applications within their organization grows more complex. Bad actors have taken note: 62% of organizations say they've experienced a security event that affected resilience.[4]

An analysis of penetration tests across nearly one million IT assets found that 7% of them were associated with a critical vulnerability that can cause program failure.[5] The study also noted that **weak credentials, infrequent patching and unfixed misconfigurations were among the most frequent weaknesses in organizations' cybersecurity**. When criminals exploit vulnerable systems, the consequences can be extremely costly. A recent estimate by IBM and the Ponemon Institute placed the average cost of a data breach in the U.S. at $9.4 million, with the typical incident taking about nine months to identify and resolve.[6] There can also be impact to brand reputation and erosion of consumer trust.

$9.4 million

average cost of a data breach in 2022.[7]

Complexity — from the cloud, from remote users or from distributed locations — makes vulnerabilities harder to identify and resolve. Strategies that simplify and consolidate IT operations have become essential for effective security as applications move further from the protections of a private network.

Securing the edge

One of the biggest risks to any network architecture is also one of the simplest: user credentials. **The two of the most common initial attack vectors in 2022 were stolen or compromised credentials — responsible for 19% of breaches — and phishing, which was responsible for 16% of breaches.[8]** Weak, reused passwords exposed elsewhere or credentials acquired by phishing or other fraudulent means frequently allow bad actors to access sensitive data and systems. The best firewall and the most up-to-date firmware won't prevent a breach when someone can simply log in. New solutions have become essential at a time when nearly two-thirds of organizations in one study reported security incidents that jeopardized their business operations.[9]

As a result, more organizations are moving toward zero trust security, where entry of a username and password are not enough for ongoing access. Whether inside or outside a network, devices are subject to continuous monitoring and verification by security systems that use different techniques to confirm their authenticity and privileges. One of the most common tools to validate users is multi-factor authentication (MFA), which uses secondary verification methods like text messages, biometric data or encrypted keys managed in security applications. These can ensure policy enforcement and prevent access when credentials are shared or stolen.

> "Whether you call it multi-factor or two-factor authentication, this simple step can make you 99% less likely to get hacked. Think of it like an airbag or the seatbelt in your car — an extra layer to keep you safe in the event of an accident."
>
> **CISA Director Jen Easterly.[10]**

Similar tools specifically help secure and manage access to resources in the cloud. A cloud access security broker (CASB) enforces IT policies when employees use cloud services, ensuring connections are authorized and secure. Secure web gateways (SWGs) provide additional protection by monitoring web requests and preventing access to potentially harmful websites and applications.

Cloud-based security solutions, such as MFA, CASB and SWG, enable organizations to extend their security policies and controls outside the corporate firewall, providing visibility and control over cloud applications and data. They can also add additional security to virtual private networks for remote workers and help document compliance with regulatory requirements for consumer data protection. Protect your entire network infrastructure — from cloud applications to remote workers — with solutions that complement each other's functionality resulting in more efficient and effective security outcomes. Managed services for firewalls, switches, software-defined wide area networks (SD-WANs) and all-in-one networking solutions also enhance the effectiveness of IT operations, giving their teams the bandwidth to focus on initiatives beyond immediate security risks.

Better frameworks for cybersecurity

Consulting with a trusted service provider can give IT leaders confidence in their migration to the cloud or remote work, along with the security enhancements they require. A partner that offers multiple, integrated security solutions also ensures comprehensive protection across cloud service providers and physical locations — plus options for managed services that supplement the availability and skills of in-house teams.

Layered, cloud-based security services coupled with SD-WAN can help protect the entirety of an IT footprint across clouds and locations. This framework, known as secure access service edge (SASE), can be difficult for organizations to piece together on their own using multiple vendors and legacy networks.

Spectrum Enterprise can help implement a SASE solution

Secure Access with Cisco Duo: A secure access management solution with multi-factor authentication, Duo enables policy-based controls for end users, devices and applications.

Cloud Security with Cisco+ Secure Connect: This solution provides cloud access security broker, secure web gateway, zero trust network access and firewall as a service functionality to effectively extend corporate security practices to the cloud.

But a trusted, national solutions provider like Spectrum Enterprise® can tailor a wide range of complementary services that span security, networking and connectivity to meet your exact requirements.

Spectrum Enterprise delivers integrated, comprehensive and managed protection solutions for networks, users and their workflows, regardless of location. Implement cloud-first, remote or hybrid work solutions to improve cybersecurity while making it easier for resource-constrained IT teams to protect their organizations. Discover how you can enhance and protect end users' experience with confidence wherever their work takes them.

Learn more

1. "Cost of a Data Breach 2022," Ponemon Institute and IBM Security, July, 2022.
2. Ibid.
3. "KPMG Global Tech Report 2022," KPMG, September, 2022.
4. "Security Outcomes Report, Volume 3, Achieving Security Resilience," Cisco Secure, December 2022.
5. "Year in Review 2022: Horizon3.ai's NodeZero Changes the Game," Horizon3.ai, 2023.
6. "Cost of a Data Breach 2022," Ponemon Institute and IBM Security, July, 2022.
7. Ibid.
8. Ibid.
9. "Security Outcomes Report, Volume 3, Achieving Security Resilience," Cisco Secure, December 2022.
10. "CISA Challenges Partners and Public to Push for 'More Than a Password' in New Social Media Campaign," Cybersecurity & Infrastructure Security Agency, June 6, 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.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply.