INFOGRAPHIC

Security on the edge

Counter cyberthreats as they expand alongside cloud and distributed resources.

Organizations are adopting cloud-based architectures that rapidly expand the threat surface beyond the in-house servers and workstations they control. Third-party apps, device proliferation, remote teams: the trends facing IT leaders call for a new security approach to keep their operations reliable, safe and fully supported.

The most common password in the country is 123456.[1] And as more applications move to the cloud, users have more credentials to protect than ever before. Organizations with limited technical resources are challenged to enforce effective security policies and test for configuration vulnerabilities as more and more external platforms become part of how they do business.

62%

of organizations have experienced a security event that impacted resilience.[2]

Timely updates are essential for keeping legacy systems secure. But the sheer number of patches to apply across systems and devices can sometimes overwhelm IT resources and allow vulnerabilities to emerge.

A recent report from NETSCOUT found that more powerful distributed denial of service (DDoS) attack vectors are devised every year. DDoS methodology continuously evolves to bypass defenses.[3] External attacks on internet-facing assets require the immediate response and resources of a trusted connectivity partner to prevent service disruption.

1M

Monthly DDoS attacks.[4]

$9.4M

is the average cost of a data breach, which typically takes nine months to identify and resolve.[5]

The financial and reputational costs of a data breach can be devastating. The threat underlines the necessity of a strategy that can secure all critical data, both in the network and across cloud applications.

Enhanced protection

A trusted service provider with the right expertise can help keep your organization ahead of cyberthreats and the workplace and technology trends that increase your risk profile. A single partner can help identify the protection solutions or products to help you enhance resilience and enable your IT team to accomplish more.

70%

of IT security professionals feel their organizations do not have enough cybersecurity staff to be effective.[6]

Protect your data everywhere it lives.

Many teams work from anywhere. So should your security solutions.

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 provide visibility across users, their devices and the systems that support them.

Identity safeguards like multi-factor authentication (MFA) and zero trust network access (ZTNA) can authenticate access to cloud resources and data centers, continuously monitoring all devices and traffic to protect your data.

Secure the digital perimeter.

Managed services can significantly enhance the security of corporate networks while freeing technical personnel to focus on other priorities.

Provider-managed unified threat management (UTM) and next-generation firewalls can help protect inbound and outbound traffic.

Outsourced hardware ensures switches, WiFi routers and other equipment are always up to date, maintained and integrated with advanced security and encryption protections.

All-in-one solutions can combine security with SASE safeguards, SD-WAN, unified communications (UC) and other solutions for complete visibility and control of the network through one portal.

Look beyond the network.

A comprehensive protection solution should also consider malware and physical threats that are often out of network managers' control.

DDoS protection ensures your internet-accessible destinations remain uninterrupted during a volumetric attack.

Managed cameras and sensors offer peace of mind through 24/7/365 physical space monitoring, a secure cloud-based portal and alerts for unauthorized access or environmental conditions that could damage property or equipment.

One partner for your every challenge

Partner with Spectrum Enterprise® to enhance and simplify security across your clouds, premises and distributed workforce. Integrating comprehensive, fully supported services with experts to guide deployment helps organizations enhance and protect the experience of employees and customers.

Learn more

Sources

1. "Multifactor Authentication," Cybersecurity & Infrastructure Security Agency, accessed February 20, 2023.
2. "Security Outcomes Report, Volume 3, Achieving Security Resilience," Cisco Secure, December 2022.
3. "DDoS Threat Intelligence Report Issue 9: Findings from 1st Half 2022," NETSCOUT, 2022.
4. Ibid.
5. "Cost of a Data Breach Report 2022," IBM, 2022.
6. "Cybersecurity Workforce Study," $(ISC)^2$, 2022.

SE-MS-IG007

Spectrum ENTERPRISE™