EXECUTIVE BRIEF

Navigating the evolving security technology landscape

New challenges require advanced safeguards for hybrid networks, remote devices and cloud applications.

Networks are becoming less centralized and more complex — as are the threats they face from bad actors. The attack surface rapidly expands as workplaces move more resources and remote devices outside the protection of corporate networks. Meanwhile, longstanding risks like ransomware and distributed denial of service (DDoS) attacks are growing increasingly sophisticated. IT leaders need a defense in depth strategy to protect their networks — a layered approach with multiple security solutions to address a wide range of potential threats. Organizations are also looking to centralize their security services for more comprehensive control of their protection.

The need for these solutions is clear: Lapses in network security can threaten profitability and employee and customer experience. The average data breach costs $4.45 million, increasing 15% over the past three years.[1] Even after an organization recovers from a breach, the effects on its reputation and employee productivity can linger.

The risk profile of large networks has notably changed in recent years. Almost 60% of employees can now work from home at least some of the time and workplaces are also instituting bring-your-own-device (BYOD) policies — both trends open up more avenues for intruders to breach a corporate network.[2] One study reported a 50% increase in attacks on mobile devices, with a significant increase in credential theft.[3] At the same time, nearly 90% of organizations are using multi-cloud architectures, which increase complexity and expand user access points for IT to manage.[4]

This executive brief explores the top cyber risks and security solutions organizations should consider to protect their networks.

increase in attacks on mobile devices, with a significant increase in credential theft.[5]

Security remains top-of-mind across industries

Healthcare: With databases full of customers' sensitive health and financial data, healthcare companies are rich targets for hackers.

Financial services: Trading, banking, lending and many other areas require institutions to protect data in motion and meet federal regulations as cyber criminals continuously look for ways to steal consumers' financial information.

Retail: Online shopping sites collect customer credit card and contact information — all valuable to hackers — while maintaining up-to-the-minute fraud detection capabilities and protecting ecommerce uptime.

Manufacturing: 30% of extortion attacks target manufacturing companies, as bad actors know that production interruptions can be extremely costly.[6]

Energy and utilities: Disruptions to organizations that support critical infrastructure can negatively impact entire communities.

Spectrum ENTERPRISE™

of employees say they store sensitive work passwords on their personal phones.[7]

Trends to consider to safeguard your network

IT professionals who want to bolster their organization's security are looking for manageable, sophisticated solutions that can establish defense in depth: an increasingly essential strategy that leverages layers of protection throughout a network. If one level of defense is compromised, additional layers provide backup to thwart threats. Upgrades to security solutions must address current trends and go beyond simply protecting internal data.

BYOD policies give hackers more potential entry points

With employees increasingly accessing corporate data from a multitude of devices, it has become more challenging to keep data secure. For example, more than 70% of employees say they store sensitive work passwords on their personal phones, increasing security risks.[8] Underscoring how insecure all these devices can be, 43% of employees say they have been the target of a phishing attack on a personal device.[9]

Hackers are getting smarter

Publicized ransomware attacks increased 49% in the first half of 2023 from the prior year. Not all attacks, however, are made public — in the same period, there were 1,815 undisclosed ransomware attacks, which may paint a more realistic picture of the threat landscape.[10] Because attempts to stop hackers are also becoming more sophisticated, less protected applications such as texting and messaging apps have become targets for phishing.[11] The combination of BYOD policies and employees' mixing of work and personal applications on the same device creates new opportunities for bad actors.

Security lapses bring legal and reputational risks

In one survey on litigation trends, one-third of respondents said they faced litigation regarding cybersecurity, data protection and data privacy in 2022.[12] The risk of litigation makes cyber insurance essential, but costs are growing. Even though prices have leveled off in recent months, a 28% year-over-year increase in the fourth quarter of 2022 and an 11% increase in the first quarter of 2023 mean that cyber insurance is significantly more expensive than just a few years ago.[13]

Cloud-based security is a major concern

Multi-cloud architectures allow data to flow easily between databases, apps and services in different locations. However, the popularity of multi-cloud architectures also complicates enterprise security. Almost 80% of organizations cite security as a top cloud challenge.[14] Unfortunately, addressing cloud security remains a work in progress: One study found that 82% of security breaches involve data stored in the cloud.[15]

Spectrum ENTERPRISE™

Solutions to support complex needs

How are organizations handling these heightened security demands? One way is through increased investment. Just over half of organizations say they are budgeting more spending on security as a result of a data breach.[16]

Where budget is allotted is critical. IT security professionals should look for solutions that address several key needs to augment existing protection of the network perimeter:

- **Visibility and data protection for web traffic:** With personnel logging in from more locations and with data often stored in multiple cloud-based locations, networks need new ways to monitor internet traffic. A secure web gateway (SWG) can 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.

- **Consistent, secure authentication:** To protect users who want to log in anywhere, organizations are increasingly turning to multi-factor authentication (MFA) and zero trust network access (ZTNA). MFA provides a second source of authentication to verify users' identities before they can access sensitive data. ZTNA is a broader security framework that helps overcome the challenges of remote work, multi-cloud architectures and data breaches by continuously reverifying the credentials of network users. This is in contrast to the more traditional approach of authenticating users once and then letting them use all network resources they have access to once they're logged in.

Just over half of organizations say they are budgeting more spending on security as a result of a data breach.[17]

- **Granular control of cloud access:** Organizations must give users secure, direct access to the cloud-based applications they rely on without interruptions or lagging connections. A cloud access security broker (CASB) can meet today's security needs by applying uniform IT policies and access controls to cloud applications for workers, partners and contractors. Along with CASB, a cloud-based firewall helps keep hybrid networks secure without routing traffic through a centralized data center, potentially introducing latency that can degrade the user experience.

- **DDoS Protection to mitigate attacks:** Even with security solutions that prevent bad actors from accessing corporate data, defense in depth requires protection from volumetric attacks. Malicious traffic from bad actors can overwhelm networks and paralyze employee and customer access to critical resources. Thwarting them requires protection from a service provider that can help identify and redirect the traffic from an attack before it can cause a disruption.

- **A centralized, streamlined platform:** Users want the convenience to log in from anywhere and IT security professionals need the visibility to be able to manage their network regardless of their users' location or device. A cloud-based enterprise network security platform provides this type of remote access. It also allows security professionals to maintain consistent security policies and monitor potential threats across every cloud, device and corporate location, regardless of where users are or what type of device they are using. Managed or co-managed services go even further, offloading many routine security tasks so IT teams can focus on more important priorities.

Spectrum ENTERPRISE™

Realizing the benefits

With a comprehensive security platform in place, IT teams can simplify their operations and the entire organization can benefit from protection against security risks. Streamlining IT operations and security enables IT professionals to confidently implement multi-cloud solutions, BYOD policies and remote work expansion — giving employees the flexibility and ease of use they need.

However, to implement an up-to-date security solution that addresses increasingly complex networks, IT teams need support. Achieving defense in depth requires a thoughtful network design. Relying on a different vendor for each piece of the security framework will likely add expense and complexity — and can lead to gaps in security.

The best way to ensure all aspects of security are integrated efficiently is to start with solutions designed to work together. Spectrum Enterprise® partners with organizations to meet the specific needs of their network architecture. Backed by 24/7/365 U.S.-based support, our managed security services are engineered and tested to work together, providing a seamless experience for both IT security professionals and the users who depend on their work.

Learn more

1. "Cost of a Data Breach Report 2023," IBM, 2023.
2. "American Opportunity Survey," McKinsey & Company, June 23, 2022.
3. Lisa O'Reilly, "State of Phishing Report Reveals More Than 255 Million Attacks in 2022," SlashNext, 2023.
4. "2023 State of the Cloud Report," Flexera, 2023.
5. Lisa O'Reilly, "State of Phishing Report Reveals More Than 255 Million Attacks in 2022," SlashNext, 2023.
6. "IBM Security X-Force Threat Intelligence Index 2023," IBM, 2023.
7. Lance Whitney, "BYOD and Personal Apps: A Recipe for Data Breaches," TechRepublic, April 3, 2023.
8. Ibid.
9. Ibid.
10. "Most Impactful Ransomware Attacks of 2023," BlackFog, 2023.
11. Lisa O'Reilly, "State of Phishing Report Reveals More Than 255 Million Attacks in 2022," SlashNext, 2023.
12. "Cybersecurity, Data Protection and Data Privacy: 2023 Annual Litigation Trends Survey," Norton Rose Fulbright, 2023.
13. "Global Insurance Market Index," Marsh, 2023.
14. "2023 State of the Cloud Report," Flexera, 2023.
15. "Cost of a Data Breach Report 2023," IBM, 2023.
16. Ibid.
17. Ibid.

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.

Spectrum ENTERPRISE™