TATA COMMUNICATIONS

DELIVERING INTEGRATED NETWORK SECURITY AT THE EDGE

Rising security challenges posed by a hybrid workforce

It's no secret that the world has changed a lot in the wake of the Covid-19 pandemic. One of the most significant changes has been in how enterprises operate. Before 2020, many companies regarded digital transformation as a slow process that would take time. However, Covid forced organisations to speed up their digital journey from two to three years to two to three months, often without a well-thought-out plan.

With many employees working remotely and customers increasingly relying on digital channels, enterprises have been forced to re-evaluate their IT infrastructures. With 98% of companies using some form of cloud-based infrastructure, the cloud has emerged as the preferred IT platform for businesses. It's clear that the cloud is here to stay, with 76% of companies today having multi-cloud deployments that include services from two or more cloud providers.

While the cloud-first approach is advantageous, multi-cloud environments can make it difficult for companies to adhere to regulatory requirements. 57% of organisations find it challenging to adequately protect their data in multi-cloud environments in line with corporate policy and regulatory requirements. The expanded threat surface posed by remote employees also makes organisations more vulnerable to targeted attacks as each hybrid worker affords new opportunities for malicious actors. A recent survey corroborated this, finding that 51% of CISOs have witnessed more targeted attacks since enabling widespread remote working.

The breakdown of "traditional" network security

The advent of the digital age has made it easier for customers to connect with the businesses they need when they need them. But as more and more transactions move online, enterprises are finding themselves under attack.

In the past, most corporate networks were contained within a single physical location where a company housed its valuable digital assets. Businesses planned their network security architectures around this location, which would typically be the data centre. However, today the rapid adoption of cloud access and anywhere operations has triggered an "inversion" of the network, making it more vulnerable than ever.

An enterprise's digital assets protected by traditional network security are under attack like never before. Putting a firewall at the network's edge is no longer enough to separate the business's resources from the "outside." Bad actors increasingly target enterprises' digital assets, leading to costly outages. So much so that 54% of cybersecurity leaders report that their business-critical applications have suffered unplanned outages related to cybersecurity incidents at least once a month. The median time to get back online after a cybersecurity incident is 14 hours, and the estimated cost of this downtime averaged about $200,000 per hour.

Lateral movement woes: The network security paradigm has changed over the years. In the past, companies used a high-trust ecosystem that only required authentication once and let people move around the network freely after that, meaning that once a user or device connected to a corporate network, they could move laterally about the network unhindered. So, if a hacker compromised a privileged account with network access, they could jump from system to system, exfiltrating data and causing financial and reputational damage. Given that **stolen credentials led to nearly 50% of attacks in 2021**, this is an extremely risky proposition.

The added cost of backhauling network traffic: While the data centre approach to network security may have once sufficed, it was not designed to support the load of the remote work environment. Backhauling remote traffic to the centralised data centre inside the perimeter for inspection and then back out can cause major bottlenecks on the enterprise network and slow down performance for both remote and on-premises users.

The problem of disparity: In the past, network security products often came from different vendors, which did not always work together. Each product had its own console and required duplicate and overlapping policies to be set up. Sometimes, it even needed its dedicated agent, making it hard to deploy and route traffic. Separate contracts and purchase agreements had to be made for each product. Because of this, organisations had to spend more time managing these separate security controls instead of using the information these solutions gave them.

Securing networks in a remote workplace

The traditional network security architecture is no longer adequate in the face of today's digital challenges. Enterprises must move to a more modern approach that considers the distributed nature of the workforce and the cloud. The ideal next-generation network security solution should be able to protect both on-premises and remote users, as well as data in hybrid environments. It should also be easy to deploy and manage, with a single pane of glass for visibility and control. Lastly, it should be scalable to meet the needs of today's businesses.

Let's take a closer look at some of the steps that can be taken to solve problems with network security today.

Adopt a defence-in-depth approach: With the hybrid workforce needing access to the web, the cloud, and the data centre, it is essential to adopt a defence-in-depth approach, which will protect against different threat vectors, irrespective of their origin. Security coverage across different layers makes it much more difficult for attackers to access sensitive data or systems. In addition, defence in depth can help you reduce the impact of any successful attack and provide a better chance of recovering from an incident. Ensure you have the basic network security controls and augment them with more advanced solutions.

Move security to the edge: Moving security to the edge is crucial to achieving effortless technology experience and security. Backhauling security data to the data centre for inspection can slow network performance, leading to a poor user experience. To avoid this, employees may try to bypass security controls altogether, putting themselves and the company at significant risk.

Moving security capabilities to the edge, closer to the end user, is essential for securing the network and keeping employees happy. By inspecting data at the edge, cloud-native security provides the same level of protection as traditional systems without requiring time-consuming data transfers for inspection. This way, enterprises can create an effortless experience for their workers while maintaining a high level of security.

Cloud-native security solutions also offer several other advantages over traditional security solutions. First, they can be deployed more quickly and easily. And second, they can scale more rapidly to meet the needs of a growing organisation.

Integrate network security controls: When it comes to protecting your organisation's network from threats, an integrated approach is essential. Integrating different network security tools into your IT environment can help protect your organisation from the edge of the network to the core. Consolidating security functions into a single platform simplifies management and reduces operational burdens and costs. When businesses are short-staffed and have a tight job market, anything that makes administrative work easier and less complicated is a good thing. In addition, integrated network security provides better visibility and control over the entire network, making identifying and mitigating threats easier.

Think zero trust: It would help if you considered adopting a zero-trust approach to your network security. Adopting zero-trust can block attackers at every point in the attack chain. For example, if the attackers have found a way around user authentication, their devices won't be allowed access because they also need to be verified separately. Zero Trust also ensures that bad actors wouldn't get unfettered access to an organisation's IT systems, so they wouldn't be able to move laterally. Furthermore, if a breach occurs, unpermitted access would be confined to the permissions scope of the hacked user, device, or network with the Zero Trust security architecture in place.

Explore a managed service approach: You might consider partnering with a managed service provider (MSP) for your advanced network security needs. This is because your existing internal teams may not be familiar with the advanced security controls technology. Then there's the issue of implementing them. Such projects take time, resources, people, and expertise. Can you say with certainty that you can give all of these things to the project for a long time? You could, of course, hire more experts to work for you. But hiring people is expensive and takes a lot of time, and you can't be sure you'll find the right people at the right time. **Working with an MSP can help here. They can provide the manpower and expertise required to implement new security controls quickly and efficiently**. Additionally, MSPs can spread the cost of new technologies and expertise across their client base, making it more affordable for individual companies.

Conclusion

Integrated network security at the edge is the way of the future. There are many benefits to moving network security to the edge and adopting a zero-trust approach. These include simplified management, reduced costs, better visibility and control, and improved user experience. Businesses must also explore working with a managed service provider to help them with their advanced network security needs.

References:

- The Biggest Cloud Security Challenges in 2022
- CISOs worried about material attacks, boardroom backing
- State of Security 2022 Report Reveals Increase in Cyberattacks While Security Talent Remains Scarce - Express Computer
- Verizon DBIR: Stolen credentials led to nearly 50% of attacks

For more information contact us or visit our Advanced Network Security page