FINANCIAL SERVICES

COMCAST
BUSINESS

Network Security and Customer Trust in Financial Services

The financial services sector has long been a leader in cybersecurity, due to the highly sensitive nature of its customer data. It's no surprise that banks have some of the highest levels of security among critical industries in the United States—in 2020, the finance and insurance sector was the most targeted industry by attackers.

Despite the attention financial services organizations give to security, however, breaches continue to occur as threats evolve and attacks become more sophisticated. Email phishing, ransomware, credential stuffing, vulnerability exploits, and malware are just some of the myriad ways in which attackers are breaching defenses and accessing customer information.

In 2020, the pandemic forced employees in all industries to work remotely, which cyber attackers used to their advantage. Malware increased 358% in 2020 compared to 2019, while ransomware increased by 435%, as financial institution firms focused on ensuring employees remained productive and able to provide an exceptional (and increasingly online) customer experience.

Malware increased **358%** in 2020 vs. 2019.

Ransomware increased **435%** in 2020 vs. 2019.

With the record number of breaches garnering headlines, financial services firms must work even harder to retain customer trust regarding the security of their data. Sustaining or improving network security is paramount in meeting and maintaining that level of trust among customers.

Going forward, financial services firms will need to consider the network infrastructure, connectivity, and cybersecurity solutions that will meet changing customer experience and data security needs. The combination of SD-WAN with managed security services, advanced cybersecurity solutions (such as unified security and DDoS mitigation), and high-speed broadband and dedicated internet can provide financial services organizations with an infrastructure that offers exceptional security as well as the performance necessary for providing high-quality customer experiences.

SD-WAN Sets the Security Stage

Software-defined wide-area networking, or SD-WAN, is increasingly being adopted for its ability to integrate a variety of advanced security solutions (such as next-gen firewalls, secure web gateways, zero-trust network access, and cloud access security brokers), improved network security monitoring, and policy setting. SD-WAN can extend an organization's network, enabling branch offices to connect via internet connections. Connection and movement of data, which can be encrypted and transported via secure virtual private network tunneling to help protect it in transit.

Because SD-WAN separates the data plane from the control plane, network administrators can segment, partition, and secure traffic across the network. Data from different applications traverse the network via micro-segmentation, which can mitigate the ability for an attack on the network to impact all of the data traffic running on the network.

SD-WAN also offers a higher level of visibility into the network than what is available with traditional networks. Network administrators are able to manage and orchestrate the network from one central location, which makes it easier for them to monitor and troubleshoot issues such as inconsistent application performance and network problems and help ensure security policies are engaged and running correctly.

SD-WAN security can be further bolstered by managed solutions such as next-generation firewalls, which offer advanced functionality over stateful firewalls that include packet filtering and Layer 3 protection. Next-generation firewalls typically offer intrusion detection and prevention, deep packet inspection, sandboxing of suspicious traffic, and data loss prevention.

Managed and Cloud Security Add to the Security Mix

For many financial services organizations, the ability to secure the network and data can be hampered by the lack of personnel available to manage IT security. Managed services can help to provide continuous management, monitoring, and the flexibility to scale as the needs of the organization evolve.

Managed routers connected via an IPsec virtual private network and protected by managed firewall and a unified threat management suite that includes content filtering, intrusion detection, data loss prevention, anti-virus, and anti-spam. When used together, managed security services can effectively help protect the network against external threats without further taxing in-house IT teams.

Organizations also need to protect their data from threats such as malware, spoofing, and phishing attempts even when employees aren't on the corporate network. Cloud-based security applications can provide further protection of devices connected to the corporate network.

Being Security Smart in Financial Services

The pandemic forced many organizations to transform their business models to digital-first in an effort to continue providing exceptional customer experience. While the financial services sector has always been a leader in security due to the sensitive nature of customer data, cyber threats continue to increase—and are becoming ever more sophisticated. What's needed is an end-to-end approach to security that addresses all points on the network and all the devices that connect to it, from corporate headquarters to branch offices. SD-WAN, advanced security solutions, and managed security services, combined with fast connectivity, are all elements that can blend together to help create a secure, trustworthy, and resilient financial services business.

Learn how Comcast Business is **helping financial services firms meet their digital transformation goals** with our innovative technologies and solutions.

[1] "X-Force Threat Intelligence Index 2021," research report, IBM Security

[2] "Malware increased by 358% in 2020," article, Help Net Security, February 2021

COMCAST
BUSINESS