Next-level Network Security Solutions Required for Today’s Sophisticated Cyber Threats

Network security includes the strategies used to protect the computer network from unauthorized access, detect and stop cyber-attacks and ensure secure communication within the network. As security challenges continue to evolve, organizations must deploy network security solutions designed to address sophisticated cyber threats.

Traditional network security involved securing the perimeter of the internal network from the outside world. Firewalls, VPNs and intrusion detection and prevention systems worked to prevent unauthorized access and attacks from the outside.

However, factors such as cloud computing, remote work and the IoT have dissolved the traditional network perimeter. Modern network security, therefore, requires a more complex approach. This approach involves concepts such as managing identity and access, securing email and endpoints, and segmenting the network.

Network Security Challenges

Several key challenges drive network security strategies this year. In the first place, cloud computing has become the norm, offering distinct advantages but introducing significant security risks. According to Gartner, security misconfigurations contribute to the majority of data breaches. Access control issues also play a major role in securing the cloud.

Malware and ransomware continue to pose a threat to network security, and they have grown more sophisticated. Ransomware gangs employ tactics like double extortion, in which they both encrypt the victim's data and threaten to leak it. And they have turned their focus to critical infrastructure sectors such as healthcare and transportation.

In addition to ransomware, organizations must protect the network against malware introduced through mobile devices. Hackers target phones and tablets with sophisticated attacks that can steal data, spy on users or hijack device functions. Many of these mobile devices connect to the corporate network and thus introduce additional risk.

Supply chain attacks also pose a serious threat. For instance, attacks exploit security flaws in vendor software before customers patch their systems. And finally, hackers still come back to the tried-and-true attack method of social engineering to steal credentials and gain network access.

Critical Features of Competitive Network Security Solutions

To combat these serious threats, network security solutions must keep pace with the evolving threat environment. Some important features to look for when choosing a security solution include the following:

- Zero trust security – A zero trust security framework assumes no entity can be trusted by default. Thus, zero trust requires verifying every access request, and it enforces strict security policies and controls based on the principle of least privilege. That is, it grants only the minimum access necessary.
- Identity and access management – An important aspect of zero trust, this involves authenticating and authorizing users and devices based on both their identity and context. For instance, identity can refer to role or department, while context might refer to time, location, or device state. MFA also plays an important role.
- Automation – Automating security tasks such as monitoring, low-level incident response, patch management and compliance monitoring frees security teams to focus on strategic projects.

Additionally, AI and machine learning can be very useful in identifying anomalies and indicators of compromise.

- Cloud-native solutions – Cloud-native security leverages the capabilities and benefits of cloud computing to secure cloud-based applications and data. Cloud-native security solutions are designed to be scalable, resilient, agile, and cost-effective.
- Network segmentation – This involves dividing the network into smaller segments based on business needs and risk levels. It allows businesses to limit the exposure of sensitive assets to unauthorized or compromised entities on the network. It also helps reduce the impact of a breach by preventing lateral movement of attackers within the network.
- Email security – Email security solutions detect spam and phishing attempts, provide dynamic analysis of links and attachments, and offer policy-enforced encryption and data loss prevention.

Enterprise-grade Network Security Solutions

The cyber security consultants at eMazzanti understand today’s threat environment and the challenge of securing critical assets with limited resources. eCare Secure Route provides cloud-delivered network security and web filtering to protect any device, anywhere.

Comprehensive threat detection blocks phishing and malware attacks over any app, port, or protocol. And predictive intelligence, powered by big data analytics and AI, automates protection against threats both known and unknown. eMazzanti can help your organization stop 50 to 98 percent more attacks than antivirus and firewalls on their own.