SEGRA

Table Stakes
Security Services

61% of Small to Medium-Sized Businesses Admitted They Experienced a Cyberattack, According to Verizon's 2022 Data Breach Investigations Report.

In 2023, small and medium-sized businesses had to make sure they (and their stakeholders, customers, etc.) were protected against traditional attacks such as DDoS and phishing, along with more current and sophisticated attacks such as ransomware.

Most business owners may be aware of cybersecurity defenses such as firewall, DDoS prevention, or various endpoint protection solutions, and assume some form of each may be included in the security package sold to them by a carrier or managed IT service provider. However, due to the advancement of IoT, a more remote workforce and increases in the sheer number and complexity of cyberattacks, there are next generation versions of each of these forms of protection that are available for owners and IT leaders that are now table stakes security services to protect their business.

General Firewall vs Next-Generation Firewall

When talking about cybersecurity in a business, people think about a firewall. Firewall has gone from a simple box that essentially did much what a router did in the past, plus some extra security features, to a more robust solution called next generation firewall.

Next generation firewall picks up some additional functionality that can happen in the device or firewall service including web filtering, antivirus services and intrusion prevention, which are all cybersecurity solutions that any business needs.

- **Web Filtering:** This function gives business owners the ability to block websites or allow them with some limitations. Categories can also be included to filter out the types of content allowed. Web filtering was a separate box in the past, but now it functions inside the next-generation firewall.

- **Network Antivirus:** Next-generation firewalls also provide antivirus protection. Typically, people use software like Norton or McAfee separately on their devices or network servers. These antivirus solutions only target threats that reach the device after traversing the network. With network antivirus protection, if someone clicks on a virus-infected web page, network antivirus will monitor traffic as it enters the firewall, detect the virus and stop it. This firewall-based feature complements, rather than replaces, antivirus software on devices.

- **Intrusion Prevention:** A firewall blocks attacks targeting an operating system or application on the network, similar to how it blocks viruses. For instance, if an office file server runs a program version with a known vulnerability, intrusion prevention is crucial. As traffic enters, it detects and stops attempts to exploit vulnerabilities

When looking at web filtering, network antivirus or intrusion prevention services, it's important to remember that these threats change constantly. Protection should not be purchased only once, because a single installation of software won't provide a stream of constant updates. What will allow updates is subscribing to more evergreen, managed services solutions such as hosted or cloud-based firewall capabilities delivered as a service.

Why Segra?

At Segra, we understand that winning in today's business landscape requires more than just technology – it requires a strategic connectivity game plan, relentless agility and innovation, and a human touch.

We invest in our customers, our network and our people to deliver exceptional connectivity solutions and customer service that empower businesses to thrive.

Our local-market operating model means your whole team – from sales to network engineering to customer support – are all living and working in the communities they serve.

Winning Solutions That Get You More


Firewall


DDoS Protection

Let's Create Winning Connections Together.

SEGRA.COM • 833.**GO.SEGRA**

Physical vs Hosted/Cloud-Based Firewall Capabilities

Firewall is essentially available in two formats. One is a physical box that is placed in a location that typically sits between the internet and the rest of someone's network. A hosted or cloud-based firewall sits in the cloud, taking the internet with it.

Cloud firewall can be built with geodiversity, where multiple cloud-based firewall platforms operate and allow continued secure connection to the internet even if one of the cloud platform suffers a connectivity or device failure. For example, a multi-site company headquartered in Charlotte has a physical firewall at that location. An issue with the fiber could bring down all the offices connected to the headquarter site, because the centralized Internet lives at the corporate headquarters. A level of diversity and availability is difficult to duplicate with a premise-based firewall solution.

Cloud-based firewall solutions are particularly beneficial for businesses and enterprises with multiple locations, as they eliminate the need for multiple boxes and receive constant updates if the firewall is hosted in the cloud. Cloud-based firewalls remove the worry about large capital expenditures of buying a premise-based firewall, and provide capabilities such as high availability and geodiversity.

DDoS Protection vs Carrier-Based DDoS Solutions

The next table stakes security issue is paying attention to DDoS attacks, which are attacks from multiple locations aimed at overwhelming a central point, such as a firewall or a web/application server. DDoS attacks usually intend to either take a company out of service or make a political statement.

A firewall can prevent DDoS, but if it's overwhelmed by incoming trash from an attack it stops doing its primary function, achieving the DDoS attack's goal.

The best way to combat a DDoS attack is to let a carrier deploy protection in their network, preferably at the edges, known as carrier-based DDoS solutions. If multiple businesses in the same market are affected by an attack, it can impact everyone. By pushing mitigation to the edge, the attack is prevented by the carrier before anyone notices.

DDoS protection should be considered regardless, but using carrier-based DDoS solutions is more optimal as they push protection to the edge.

A carrier-deployed DDoS solution may also benefit from threat intelligence related to attacks globally. This intelligence allows the carrier to recognize an attacker's signature before the attack spreads.

Endpoint Protection vs Holistic Endpoint Protection Solutions

The next thing that would be considered table stakes is protection of the end points in a network, known as endpoint protection or EPP. When you go online to a secure website, such as an online banking login page, you would most likely see that little lock on the left side of the address bar, which basically means that traffic is being encrypted.

Encryption is a good thing, but more and more Internet traffic is becoming encrypted. The firewall itself can't see what's going on as traffic passes through, so threats get through to the end user's computer. Something may look normal to the user and still contain malware or a virus.

And just like the firewall needs to have regular updates, it's terribly critical that endpoint protection software is updated continuously, also. Buying EPP individually and putting it on individual computers is good, but it's not ideal. What you want is a holistic endpoint protection solution for a company. A holistic approach allows business owners to apply the company policies to the computers, be alerted when someone's computer is faulty and get an alert to quarantine a threat.

Zero Trust Access Policy

As attackers get more sophisticated and are able to hide in a network and impersonate legitimate users, another table stakes solution is to implement a zero trust access policy. This is not added to a single device or application; a zero trust principal is applied to all users and all traffic. This principle states that no user or network connection should be allowed access to a network or application without first confirming who is connecting, their role, and if their role had a need and the authority to access the network or resource. The zero trust policy should be implemented in firewalls, network devices, applications and end point protection.

Overall, downtime due to data breaches or non-compliance can cripple a business, causing financial issues and impacting business operations. Relying on firewalls and antivirus software is no longer enough to protect an organization against threats – a holistic approach to cybersecurity is needed. The solutions mentioned above will help provide a well-rounded approach to give small and medium-sized business owners a safer and more effective network by looking for threats at the endpoint, firewall and out into the edge of the carrier's network.