EDGE DEFENSE

WHY YOU NEED
EDGE DEFENSE

Cybersecurity threats are growing in number and sophistication. Malware, ransomware, distributed denial-of-service (DDoS) attacks, email fraud, cloud account compromise are just a few of the threats lurking outside a business's virtual front door. Traditional cybersecurity focused on securing the perimeter (or edge) of a network by separating the "safe" business side from the public internet with security measures such as a firewall. However, the wholesale adoption of cloud services, rise of mobile computing, hybrid workplaces and insider threats have required an innovative approach to cybersecurity beyond creating a wall between a business and the internet.

The adoption of cloud services means that much of business data today resides outside of office walls and moves freely across the internet between hybrid office spaces, remote workers, and data centers. Mobile computing means that the border between a business and the internet now exists in a coffee shop, airport lounge or hotel Wi-Fi, wherever employees are working. Collaboration between suppliers, customers and employees means that threats can just as likely come from within a business's network as from the internet. Therefore, businesses no longer need just a firewall, but a comprehensive edge defense built for today's distributed cybersecurity environment.

WHY CHOOSE NETWORK BOX USA
EDGE DEFENSE

Network Box USA's edge defense is a comprehensive set of purpose built cybersecurity solutions that offers full protection to meet the needs of today's business. As required, it leverages the following powerful services:-

Secure Software-defined Wide Area Network (SD-WAN) solution optimizes network traffic and allows businesses to securely connect between HQ, branch and home offices, mobile worker locations, data centers and cloud services, regardless of network connection type. Secure SD-WAN also allows businesses to decouple the physical network from the management and operation of the Wide Area Network in a flexible, network-agnostic manner.

Secure Web Gateway (SWG+) includes FW+ (Firewall, IPS, VPN), web browsing protection modules (anti-malware for files and URLS (HTTP and HTTPS), content filtering, policy enforcement, application filtering and more, ensuring businesses are fully protected.

Web Browsing Protection (WBP+) is a user bundle comprised of a firewall, 3 intrusion prevention systems (IPS), VPN, along with web browsing protection modules including anti-malware for files and URLs (HTTP and HTTPS), content filtering, policy enforcement, application filtering, and so much more.

EDGE DEFENSE IS POWERED BY NETWORK BOX USA

BEST-IN-CLASS THREAT INTELLIGENCE

ZERO-DAY THREAT PROTECTION

SELF-OPERATED SECURITY RESPONSE CENTER

3 ISO Certifications
PCI DSS 3.2 attestation
70+ threat intelligence partners

FULLY STAFFED SECURITY OPERATIONS CENTER

UNIFIED MANAGEMENT GUI

Network Box USA Edge Defense Provides a Business with Strong Protection

A COMPLEX CYBERSECURITY ENVIRONMENT REQUIRES A ROBUST CYBERSECURITY SOLUTION

EDGE DEFENSE FEATURES

✓ **Resilience**

Network Box USA's Secure SD-WAN provides monitoring and automatic switching between alternative network paths. Whatever the physical network type, Secure SD-WAN unifies them and offers each a unique network interface. It then provides availability monitoring on either the gateway (monitoring the link and its next hop), or the link path (actively monitoring along the path, including network connectivity to the destination). This means detection of both failures of the immediate link itself, as well as routing or other connectivity issues further out in the network, is possible.

✓ **Next Generation Firewall**

The Network Box USA Firewall protects servers and workstations from network-level attacks, including protocol anomalies, connection flooding, denial-of-service, and SYN flooding, and packet fragmentation evasion techniques. Blackhole, fingerprint obfuscation and decoy technologies further shield protected networks from malicious probes. The Network Box USA firewall is tightly integrated with 3 intrusion prevention systems; this deep packet inspection is also known as a next-generation firewall.

✓ **Powerful Intrusion Detection and Prevention**

The Network Box USA IPS/IDS (Intrusion Prevention System and Intrusion Detection System) is a multilayered module that offers powerful rules languages, extensive stream, and protocol decoders without impacting performance. It operates in four modes that work together in combination with the core routing and firewall functions to provide a highly flexible, modular approach to the problem of securing network traffic.

✓ **VPN Technology**

Network Box USA's VPN (Virtual Private Network) module offers secure site-to-site, site-to-remote, and "road warrior" connections coupled with the latest encryption technologies. It is fully integrated with the Network Box USA firewall and router to provide excellent policy control. For instance, policies can be applied to encrypted vs unencrypted traffic and specific endpoints.

✓ **Advanced Routing**

The sophisticated routing system supports several dynamic routing protocols.

✓ **IPv4/IPv6 Translation**

Network Box USA has built in full IPv4/IPv6 translation capabilities. You can set up your servers with a public IPv6 IP address without having to change any settings on the servers themselves.