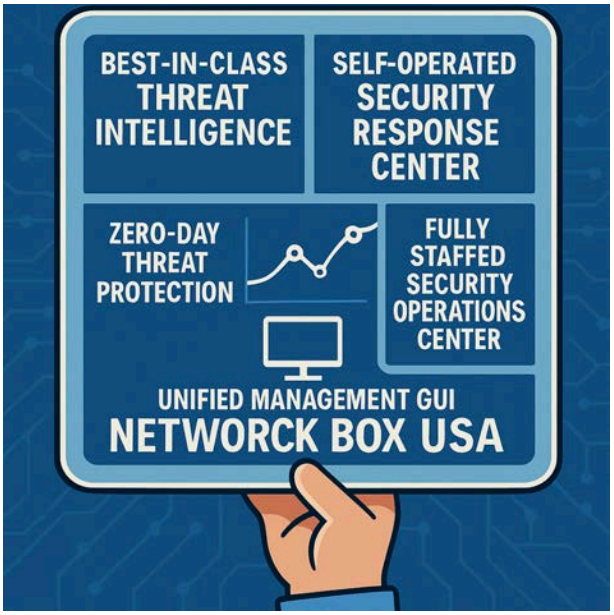
NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs



THE RESULT IS A "SINGLE PANE OF GLASS" COVERING EDGE-TO-ENDPOINT THREATS

Network Box USA (NBUSA) takes a notably different approach to detection and response:

Whereas competitors offer software-centric platforms (largely focused on endpoints/cloud and designed for MSPs or internal teams to deploy), Network Box USA is a **Managed Security Service Provider (MSSP)** that delivers a fully integrated suite of security services as a turnkey solution.

In other words, NBUSA is more of a "**security-as-a-service**" provider with our own unified technology stack, combining network security hardware, endpoint security, SIEM, and SOC services.

The next pages detail out the key ways in which Network Box USA differs as a cyber security provider.

POWERED BY NETWORK BOX USA.
THAT'S CYBERSECURITY DONE RIGHT.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Holistic Integration of Network *and* Endpoint Security: Unlike most cyber security providers, which primarily focus on endpoints and cloud apps, NBUSA covers the full perimeter and network layer as part of our standard service. Network Box provides **managed Unified Threat Management (UTM)** appliances, which are essentially firewalls loaded with multiple security functions (IPS, web filtering, anti-malware, VPN, etc.), that sit at the customer's network edge. These Boxes form the first line of defense. NBUSA's platform then links those network devices with **endpoint detection & response (EDR)** agents on endpoints, and ties everything together with a **cloud-based Security Information & Event Management (SIEM+)** system.

All security events from the network (firewall, IDS, etc.), endpoints, and even third-party logs feed into NBUSA's SIEM, where correlations are done (our SIEM+ includes an "advanced correlation engine" for multi-source analysis / XDR). This means NBUSA isn't just correlating endpoint and cloud telemetry like the others; we're also correlating network intrusion data, web traffic logs, email spam filtering logs, etc. from ou own devices. The result is a "**single pane of glass**" covering edge-to-endpoint threats. In essence, NBUSA's strategy treats the customer's entire environment (network, servers, PCs, cloud services) as one integrated system to protect, providing **unified visibility across all layers**. This deeply integrated approach can reduce gaps, e.g., if an endpoint is infected, NBUSA's firewall might catch outbound traffic and the EDR might catch the process, and together with SIEM correlation, the SOC gets a full picture immediately.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Customization & A la Carte Services: Network Box USA offers services in a highly **customizable, à la carte manner.** Clients can choose the pieces they need: for example, some may utilize NBUSA's **Edge Defense** services (like UTM firewall, Secure Web Gateway cloud filtering, Secure SD-WAN), and/or the **Managed Detection & Response** components (SIEM+, SOC monitoring, Endpoint Detection), and/or additional services like **Managed Email Security, Vulnerability Scanning, Penetration Testing, or Security Awareness Training**. NBUSA emphasizes that **all services are fully integrated** if you use them together, but importantly, they can also integrate with existing customer tools. For instance, NBUSA's SIEM+ can **ingest third-party logs via syslog** from non-NBUSA devices. This means if a client already has a certain firewall or cloud system, NBUSA can pull those logs into its monitoring platform.

This flexibility contrasts with our competitors, which largely require you to use their own agents and do not monitor external systems outside their scope. NBUSA effectively can act as a central hub for various security feeds, making it **technology-agnostic in integration**. The customization extends to deployment: NBUSA can **provide on-premise hardware** (we ship our own UTM appliances included free with the service), and we tailor the configuration (firewall rules, policies) to the client's environment. We can also customize response procedures per client (some clients might want automatic blocking of certain events, others may want notification only, and NBUSA can adjust those policies). This *bespoke, consultative approach* is possible because NBUSA is delivering a service, not just selling software licenses.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Breadth of Services (Beyond MDR/XDR): Network Box USA offers a far **broader array of security services** than the typical MDR vendor. In addition to detection & response, NBUSA provides **preventive and auxiliary services**: for example, Web Application Firewall (**WAF**) to protect web servers, **Secure Web Gateway** cloud service to filter web usage and block malware in HTTP/HTTPS traffic, **Secure SD-WAN** to securely connect branch offices, **Email Security (MCES)** which filters and sanitizes emails at the gateway, **Reputation Monitoring** to watch the client's IP/domain against blacklists, and periodic **Penetration Testing** engagements to proactively find weaknesses. They even include **Compliance-friendly reporting** (KPI reports) and SIEM log retention for 90 days by default, at no extra cost, which helps with standards like PCI, HIPAA, etc.

This breadth essentially means *Network Box USA can function as a client's full security department,* handling everything from network perimeter defense to user training. The other vendors are more focused on detection/response and do not directly manage things like firewalls or perform pen-tests (they might partner or leave that to others). NBUSA's comprehensive offerings can be a **one-stop shop** for organizations that prefer to outsource the majority of their cybersecurity needs to a single trusted provider.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Managed Service Approach vs. Product Approach: Perhaps the biggest strategic difference is that **NBUSA operates as a managed service provider** in the truest sense. When a client signs up, NBUSA **deploys proprietary technology** (often including physical or virtual appliances) and **our team fully manages those on the client's behalf**. We are "Cybersecurity Done For You" meaning that the client does not need to manage consoles, tune alerts, or respond at 3am; NBUSA's SOC handles all that. By contrast, all the other vendors, while they have MDR elements, are still platforms that the customer or MSP deploys and may co-manage. With NBUSA, many clients essentially hand over the keys: **NBUSA's SOC monitors and manages changes** (they will even do things like update firewall rules: clients just submit a request/ticket and NBUSA implements it).

We at NBUSA emphasize this fully managed aspect with slogans like "open a ticket, and grab a coffee" meaning we handle the heavy lifting. This service model can be extremely appealing to organizations without any dedicated IT security staff. It's more like outsourcing your security operations entirely, whereas other *competitors, though "managed," often involve the customer* in many actions (especially remediation). NBUSA's SOC is ISO-certified and located in Houston (with global SOC network support), operating 24x7x365 just like the others. But *NBUSA becomes the administrator of security* devices and responses in the client environment, with deeper integration into the client network (since we place our hardware on-site or at network egress).

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Integration and Real-Time Updates: NBUSA leverages a **global threat intelligence network** with 70+ security feed partners and 250k honeypots, analyzing close to 1 billion threats daily. We push updates (new threat signatures, IoC blocks, etc.) to all client devices globally in real-time using a patented “push update” technology. For example, if a new malware indicator is discovered by one sensor, NBUSA can distribute a block for it to every client’s UTM device within seconds. This means all NBUSA customers benefit from collective intelligence across the whole Network Box client base.

While other vendors also aggregate threat intel (e.g., CrowdStrike’s cloud is similar for endpoints), NBUSA’s focus on *network-level threat intelligence* and instantaneous signature deployment is a differentiator. Our “Z-Scan” zero-day protection system can propagate new protections to all devices within 3 seconds. This level of integrated update across network and endpoint is a huge strength of a vertically integrated service like ours. In contrast, a software like Huntress might rely more on detecting with behavior analytics and sending an alert; meanwhile, NBUSA should outright block the malicious traffic at the firewall and alert simultaneously, often preventing certain attacks at the perimeter.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Flexibility vs. Bundling: In terms of packaging, **NBUSA can tailor solutions per client** much more flexibly than a fixed SaaS product bundle. For instance, a client could use NBUSA's MDR (SOC+SIEM+EDR) but keep their existing firewall – NBUSA will integrate with it. Or vice versa: use NBUSA's UTM for perimeter and perhaps a different endpoint product – NBUSA's SOC can still monitor the logs. This "mix-and-match" capability is supported by their SIEM accepting third-party feeds. Meanwhile, other vendors typically assume you will use their entire stack (you install their agent, use their console; they generally don't monitor another vendor's EDR or firewall on your behalf). **NBUSA's a la carte approach** can be seen in their service menu (Edge Defense, MDR, and "More Protection" are modular categories).

This allows clients to start with what they need and expand. It also helps in highly regulated or custom environments – NBUSA can integrate with specific systems (say, a bank's core banking server logs) by pulling logs into their SIEM, something a generic MDR platform might not support. In summary, NBUSA offers **greater integration flexibility**, which can be a major advantage for clients with existing investments or unique needs.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Advantages of NBUSA:

Breadth & Depth: Network Box USA's **breadth of services** is a big advantage for MSPs. We cover areas that competitors do not, such as network perimeter defense, SD-WAN, on-premise devices, and proactive services like pen testing. This means a client could consolidate multiple security needs (firewall management, endpoint security, SOC monitoring, compliance reporting, training, etc.) with one vendor, achieving a kind of **MSSP one-stop-shop**.

This is especially valuable for organizations that do not want to juggle multiple vendors or lack the expertise to integrate several products. NBUSA provides end-to-end coverage, which can be more comprehensive overall.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Full Managed Outsourcing: NBUSA could have a **service quality edge** for organizations that truly want to outsource security. Our *95% client renewal rate* shows high customer satisfaction. Clients often value having **hands-on experts who not only monitor but manage changes and updates in real-time**. For example, NBUSA will tune your firewall policies, apply patches, update signatures – tasks that typically an internal team or separate MSSP would need to do.

This level of service can be a **force multiplier for small IT teams**, similar in spirit to what Huntress does, but covering a **far broader scope** (network and beyond). For companies in sectors like banking, government, or healthcare (all industries NBUSA serves), this full-service model ensures security is handled by experienced professionals, which might meet regulatory expectations better than purely technical platforms.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Integration & Single Pane Visibility: With all components integrated, **NBUSA can investigate incidents holistically**. For example, if malware is detected on an endpoint, NBUSA analysts can simultaneously see if that malware communicated out through the firewall, what domain it tried to reach (reputation data), and whether any other host in the network showed similar traffic, all within their **unified console**.

This **rich context speeds up investigation and response, arguably giving NBUSA an edge** in incident handling efficiency over a scenario where network and endpoint are siloed tools (which is often the case if using Huntress or Guardz-type security alongside separate firewalls).

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

Hardware Included & Cost Efficiency: NBUSA includes certain elements at no extra cost that competitors might charge for. We provide the UTM firewall appliance hardware at no cost as part of the service, and include 90 days of log retention in our SIEM by default for compliance. This can be cost-efficient because clients don't need to purchase expensive firewall hardware or separate logging solutions. Everything is wrapped into the service subscription. Our pricing consists of a subscription per domain or per user/device depending on services. By bundling so many services, NBUSA could potentially replace the need for multiple point-product subscriptions (firewall, EDR, email filter, MDR service, etc.), which **may offer a better ROI** in some cases.

Moreover, NBUSA's long history (25+ years) means our offerings have matured and scaled to keep up with the evolving security threat landscape, allowing us to offer competitive pricing through economy of scale, especially for comprehensive packages.

Data Residency and Trust: For U.S.-based customers, NBUSA being Houston-based with US-only data centers might be an advantage for those concerned about data sovereignty (**all data stays in USA**). Some clients in government or defense sectors might prefer a provider like NBUSA due to this factor, as well as our many security certifications. NBUSA has 16 global SOCs and boasts 140+ international awards, demonstrating our reputable track record.

NETWORK BOX USA

How our MDR/EDR/XDR Strategy Differs

In summary, **Network Box USA's strategy differs by providing a fully managed, integrated security solution** that spans network to endpoint, with highly customizable service bundles. Where competitors largely deliver software platforms (with varying degrees of MDR support), NBUSA delivers a service-first experience, essentially functioning as an outsourced security department. This **integration of people, process, and technology** under one roof can lead to strong security outcomes and convenience.

Give your company the Network Box advantage with our **breadth** (covering security holistically), **flexibility** (adapting to client needs and existing tools), and **depth of management** (handling everything for the client). For organizations that prefer an all-in-one managed approach or have complex multi-layered security requirements, NBUSA can offer capabilities and personalized service beyond what a single-product MDR provider typically can.

CYBER SECURITY 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

POWERED BY NETWORK BOX USA.
THAT'S CYBERSECURITY DONE RIGHT.