WHITE PAPER

INSIDER'S GUIDE TO CHOOSING A DNS SERVICE

4 Critical Qualities in a Foundational Service

neustar®
Security Services

TABLE OF CONTENTS

DNS Services: The Qualities You Need to Thrive Online

The need that DNS (the domain name system) was created to address seems simple enough: where can I find this digital asset? A query is routed to a DNS server, which responds with an answer. Simple.

Except it's not.

The actual mechanics of these theoretically simple transactions are extremely complex. There are tens of millions of DNS servers – no one knows exactly how many. The number of digital devices and services people are looking for has grown explosively. With IPv6, there are more than 340 undecillion possible internet addresses. That's 340 followed by 36 zeroes.

It's a lot to keep track of, and it changes every day, all the time. In addition, when DNS was invented the internet had a very limited number of specialized users. Security wasn't even considered. Partly as a result, cyberattacks against and through DNS have become commonplace. In recent years they have grown more numerous, more serious, more varied, and more complex.

At the enterprise level, DNS involves all these complexities, just at a smaller scale. The number of device and service names has skyrocketed in the last few years, and they change every day. Every new or changed name requires updates to multiple DNS servers in multiple locations. Ensuring security while maintaining a high level of performance has never been more difficult.

In the face of these growing challenges, more and more organizations, particularly large enterprises with global operations, are turning to DNS service providers to operate their authoritative DNS.

Since DNS is fundamental to every aspect of today's digital enterprises, it's essential to choose a service provider that is fully committed to ensuring flawless execution of every query despite complexities, challenges, and threats.

To deliver on that promise, a provider must be relentlessly committed to four fundamental principles underpinning their service offerings:

- **Security:** to deliver uninterrupted operations in the face of threats and directed attacks
- **Performance:** to maintain lightning-fast response times despite unpredictable network issues and traffic fluctuations
- **Reliability:** to ensure constant and unimpeded access to your internet assets for customers, partners, and staff
- **Support:** to address any configuration or service issues that may arise quickly and painlessly.

This whitepaper pulls back the curtain to explore what is actually involved in delivering each of these fundamentals of DNS service, and how you can identify providers you can trust to **enable your business to thrive online.**

1 Security

WHY IT MATTERS

- **More than 1/3 of all cyber attacks are deployed via DNS**[1]
- **72% of organizations experienced a DNS attack in the last 12 months**[2]
- **Security is as critical for managed services as for on-premise DNS**

WHAT TO LOOK FOR

- **Enterprise-grade DDoS protection for your DNS assets**
- **DNSSEC (DNS Security Extensions)**
- **Service segmentation**
- **Commitment to security**

There are two reasons that DNS draws the attention of cybercriminals: it is a ubiquitous core technology of the internet, and it was designed without significant security protections. For these reasons it has become a common and attractive attack vector and target for bad actors.

The most prevalent and egregious threats include DDoS (distributed denial of service) and DNS amplification attacks, DNS tunneling for data exfiltration, and DNS hijacks and cache poisoning to impersonate or take over digital assets.

You cannot afford security lapses in your DNS service. The security practices of your DNS service provider are absolutely critical.

DDoS protection. The number of DDoS attacks has trended upwards by double digits since April 2020, and they have also grown in size: in November 2021 one Neustar Security Services UltraDDoS customer was hit by a 1.3 Tbps (terabits/second) attack.

DNS reflection and amplification is one of the most frequently exploited vectors for DDoS attacks. This technique exploits the vast numbers of Open DNS resolvers, including both authoritative and recursive resolvers, to flood and paralyze the target organization's DNS access, exhausting network capacity, blocking legitimate DNS queries, and shutting down access.

[1] *"Measuring the Economic Value of DNS Security," GlobalCyberAlliance.org*
[2] *Neustar International Security Council survey, September 2021, reported by HelpNetSecurity.com*

Other common attacks with the potential to exhaust DNS resources include dictionary attacks and pseudo-random pre-pend label attacks involving a vast stream of queries for non-existent but real-looking names.

This onslaught is a very real threat that can effectively paralyze any DNS infrastructure, on-premise or off. An attack can prevent customers from reaching your applications and freeze out your connected workforce –unless your DNS service provider is prepared. They need both the expertise and the infrastructure to instantly mitigate a large, complex, intense DDoS attack targeting your DNS.

DNSSEC: These security extensions secure DNS processes by adding integrity protections for DNS data. DNSSEC uses public key cryptography to digitally sign authoritative zone data, so that when responses are sent they include a signature that validates the response.

DNSSEC dramatically reduces the risk of a cache poisoning attack, in which a compromised recursive DNS server provides a deliberately false DNS response from its cache that could direct users to an IP controlled by the attacker. In one well-publicized incident[3], customers of a Brazilian bank were redirected to a malicious imitation of the bank's real website, where they entered their login credentials and had their accounts cleaned out.

Look for a robust DNSSEC implementation with user-friendly management tools that allow your team to easily apply extensions across a complex, multi-provider environment. An ideal implementation will simplify the process by allowing protection to be applied for any and all zones with a few clicks.

Service segmentation: Since DNS service can be scaled relatively easily, some providers may decide to serve hundreds or even thousands of customers and many more domains using shared network resources and even the same nameserver.

It's highly efficient as long as nothing goes wrong. But if one of the customers is the target of an attack – even a single domain –the effects are likely to be felt by other customers sharing the resources. Such an attack on an unrelated domain in a shared environment could affect other customers' service and potentially damage their reputations.

Security-conscious DNS providers segment their DNS services, clustering customers in smaller groups sharing a nameserver announcement. They can then distinguish traffic by customer, and provide multiple control points in the traffic path to ensure that problems affecting one customer will not affect others. Some providers offer their customers the option of a fully dedicated name segment to provide complete isolation.

An effectively implemented service segmentation strategy significantly reduces the chances your assets will be collateral damage in an attack targeting someone else.

Provider commitment: The reality of DNS is that even a small security lapse or oversight can have significant consequences for your business. It's not enough for a provider to just check the boxes for security capabilities. They have to put in the time and effort – the hard work – required to ensure that your DNS is as fully secure as humanly possible.

That means cultivating and maintaining a constant focus on security, and thinking first and foremost about security when developing and implementing any changes or enhancements to their services.

Security has to be a priority. Always.

[3] *"How Hackers Hijacked a Bank's Entire Online Operation," Andy Greenberg, Wired, April 4, 2017*

DNS FROM A SECURITY COMPANY

Neustar Security Services is as much an IT security specialist as a DNS service provider. Our DDoS mitigation platform is one of the largest dedicated data scrubbing networks in the world, with a capacity of more than 12 Tbps. Our security operations center (SOC) ingests sophisticated threat feeds, tracks cyberthreats across the Internet, and handles attacks as a matter of daily routine.
Security is an essential consideration in every aspect of every product and service we bring to the marketplace, including our DNS services.

2 Performance

WHY IT MATTERS

- **DNS is the guidepost to your content – and users want to get there fast**
- **A 1-second delay reduces customer satisfaction by 16%** [4]
- **Nearly 70% of consumers admit that page speed influences likelihood to buy** [5]

WHAT TO LOOK FOR

- **Purpose-built DNS network based on DNS expertise**
- **Global infrastructure with:**
  - **Scale**
  - **Flexibility**
  - **Co-located authoritative and recursive servers**
- **Commitment to maintaining and improving infrastructure**

A consistently high level of performance in your DNS service is not just a nice feature; it's a business imperative. Study after study shows that the slightest delay in reaching website content negatively affects every user metric from bounce rate to satisfaction to conversion. Your goal is to optimize for speed, and the first opportunity to deliver is the DNS lookup.

You cannot afford poor performance in your DNS service. The practices your provider follows to ensure the fastest response to every DNS query are crucial to the experience you deliver to users, customers, and staff.

Purpose-built network based on DNS expertise. DNS involves a single use case – a DNS query that requires the fastest possible response – and there is no latitude in fulfilling that mission, millions of times a day. A DNS provider can't prioritize traffic or use batch processing to improve efficiencies; they must respond immediately to every request. Response time can't be adjusted based on traffic loads or malicious activity. Every response to every query must be immediate, every time.

4 *"Website Load Time Statistics: Why Speed Matters in 2021,"* *WebsiteBuilderExpert.com*
5 *"Think Fast: The Page Speed Report Stats and Trends for Marketers,"* *Unbounce.com*

That requires a DNS-first network, designed specifically to handle DNS traffic efficiently in every circumstance. It requires a streamlined infrastructure optimized to handle millions of queries at any given time, with no unnecessary layers or unneeded devices in the path. And because success in DNS service ultimately relies on network infrastructure that is owned and operated by other entities for transit, your service provider must do everything possible to make it easy for DNS servers to exchange queries and responses everywhere across the wider web.

Global Infrastructure: Time matters in DNS service, down to milliseconds. The closer the DNS server is to your users, the faster the resolution. If your enterprise has customers in multiple countries, you want a DNS service provider with service nodes around the world.

Scale: Scaling to respond to millions or even billions of queries each day is a significant challenge. That makes the scale of the infrastructure crucial to ensure instant responses during both planned peak events and unplanned volume spikes in your traffic. A major shopping holiday, a powerful promotion, or a sudden and significant increase in queries triggered by a news story or even a social media post can all result in increased lag unless the DNS infrastructure is robust and intentionally overbuilt to handle even unexpected loads.

Flexibility: Global distribution of nodes is important, but so too is flexibility in how they are deployed. Under normal circumstances, for example, a node in Singapore may be the primary choice for DNS services involving south Asian facilities and customers. However, if that node should experience high traffic loads, or, worse, a DDoS or other cyberattack that could slow responses, the infrastructure should be designed to shift traffic automatically and seamlessly to another node to preserve service and maintain high performance.

Co-located authoritative and recursive server: If your DNS service provider also offers recursive DNS services, it's helpful when the nodes for the authoritative DNS servers are co-located with recursive servers, and to a lesser extent with top-level domain (TLD) servers. The proximity of these assets ensures near-zero latency responses and instant cache updates for hosted zones, improving both security and user experiences.

Commitment to maintaining and improving infrastructure: As you review the performance capabilities of potential DNS partners, it's important to look beyond the capabilities they currently offer. The demands on their DNS infrastructure will inevitably grow as more and more devices and more and more services are added to the enterprise networks they serve. An infrastructure that is state-of-the-art today will not remain that way for long unless the provider is actively working to update and expand its capabilities consistent with its DNS-first architecture.

Seek a provider with a demonstrated commitment to modernize and expand its DNS infrastructure and amplify its capabilities so that performance will not suffer as demands increase.

A LEGACY OF EXPERTISE, LOOKING AHEAD

UltraDNS from Neustar Security Services is the original enterprise DNS service, with a legacy of innovation that includes pioneering use of the Anycast addressing and routing methodology. Now the standard for virtually all DNS services, Anycast allows a single query to be routed to any one of multiple redundant servers, completing the connection to the nearest server or the one with the fastest response.

We're hardly resting on our laurels. We recently completed a significant upgrade and edge node redesign that greatly increased the capacity of our DNS infrastructure, while also significantly improving resource flexibility by decoupling the services we provide from the physical infrastructure that provides them.

3 Reliability

WHY IT MATTERS

- **DNS failures and slowdowns are more common than you think**
- **Authoritative DNS failure = limited or no website access and traffic**
- **Recursive DNS failure = no device(s), limited web access and apps**

WHAT TO LOOK FOR

- **Overprovisioned, fault-tolerant platform**
- **Failover service**
- **Load balancing capabilities**
- **Geographic routing**
- **Commitment to uninterrupted service**

Depending on where it occurs, a DNS failure can either make your website invisible and inaccessible to visitors or cut off access to web applications and content for your users. A DNS failure essentially breaks the internet – a truly catastrophic event for today's connected businesses.

Since the reliability of your DNS service provider stands between your enterprise and a DNS failure, it's important. An uptime guarantee backed by a solid SLA is certainly an important consideration, but not the only one. You should also look for how your provider can reroute traffic on the fly if one or more of your redundant servers experiences performance slowdowns, or to load balance excessive traffic to one location with other resources.

You cannot afford unreliable DNS service. Nor can you afford a service that can't ensure your DNS reliably provides the highest level of performance.

Overprovisioned, fault-tolerant platform. In any system in the real world, occasional failures are inevitable despite every effort to prevent them. To keep such an unavoidable failure in DNS from impacting your corner of the internet, your service provider must be prepared to handle any issues that could arise.

A platform with additional capacity held in reserve and available to respond to unexpectedly high levels of traffic – legitimate as well as malicious – is not just desirable; it's a necessity. Look for a significantly overprovisioned platform with the capacity to handle traffic volume that is many, many times higher than the current and anticipated steady-state query levels.

In addition, ensure that redundancy is incorporated into every aspect of the platform architecture and service delivery infrastructure to ensure a high level of fault tolerance. Look for redundant servers in multiple service nodes around the world as well as the capability to shift services between nodes near instantaneously. Your provider should also utilize multiple network service providers with diverse delivery paths so they can instantly sidestep any single point of failure.

Failover service: It's not only issues at the provider or network level that can impact access to your digital assets. High traffic levels or outright failures in any of your web servers can delay or cut off access as well. Failover service from your DNS provider can monitor your web assets for a failure, then direct traffic away from the affected server. This prevents a server issue from impacting your website access and traffic.

Key capabilities include redundant, active monitoring agents that continually test server response times for faults and latency. If targeted thresholds in service levels are exceeded, the service should automatically activate preplanned failover processes that change DNS listings to route traffic to a redundant asset. Ideally the service and its configuration management will be easy to integrate with your network and systems through open-source APIs.

Load balancing capabilities: Effective load balancing can prevent performance-robbing traffic volumes from occurring in the first place. DNS provides a highly effective option for balancing traffic, eliminating the need to deploy costly application delivery controllers (ADCs) for this function.

Look for the option to conduct weighted balancing in addition to the traditional round-robin approach. Even better: the capability to dynamically modify the weighing factors based on real-time monitoring of server responses to DNS requests, then redirecting traffic to more responsive servers. You also want the ability to specify different routing responses based on different thresholds, and do it all without additional hardware or software requirements.

Geographic routing: For global enterprises, the ability to route traffic to different servers based on the geographic location of the user is important – not only because it improves performance by connecting users to servers located close to them, but also because it improves user experiences by enabling content customization based on geography.

In evaluating providers with IP-based geolocation capabilities, consider how much the granularity of available location assignments matters to you. For example, is the city or province of the user important, or is the country a sufficient distinction? Also consider the quality and timeliness of the data that powers geographic routing. Geolocation data has no absolute truth set, so the accuracy of geographic determinations based on a user's IP can vary considerably among providers.

Commitment to uninterrupted service: Here's a guarantee: You will never evaluate a DNS service provider that does not claim outstanding reliability. Therefore it's crucial to look under the hood and learn how they deliver the performance they cite. Ask about the details of their platform and the technologies, tools, and configurations they employ to deliver the reliability they claim – as well as the supporting data that backs it up.

Above all, evaluate their emphasis and focus when addressing the reliability of their service. A provider who isn't fully committed to ensuring the ironclad dependability of the DNS service they offer may be a risk you don't want to take.

ENTERPRISE-GRADE RELIABILITY IN DNS

Neustar Security Services UltraDNS is and always has been an enterprise-grade service, designed from the ground up to meet the reliability needs of the most demanding global organizations. We serve leading enterprises in financial services, technology, ecommerce, and other industries – none of whom can afford the tiniest lapse in DNS availability.

We recently ungraded the service edge of our fault-tolerant infrastructure, boosting capacity to trillions of DNS transactions every single day, more than 10 times the current steady state capacity. We offer a full suite of advanced, highly capable dynamic traffic management services. Our unwavering commitment to reliability is backed by a 100% SLA for DNS resolution.

4 Support

WHY IT MATTERS

- **A DNS issue can be a true emergency**
- **Even common configuration errors require prompt action**
- **Every issue deserves immediate, expert attention**

WHAT TO LOOK FOR

- **Effective, intuitive DNS self-management tools**
- **• 24/7/365 support availability with:**
  - **Prompt responses to support requests**
  - **Direct access to highly qualified experts**
- **Immediate support access in an emergency**

The characteristics we've covered so far are all about optimizing DNS performance while preventing any service disruptions, whether from malicious activities or the unpredictable, random errors that plague every complex system.

Now we turn to what happens if something does go wrong. Is someone always there to respond quickly and knowledgably if the need arises? Or will you be left hanging with no device, website, or network access, and no answers? Almost as important are effective, usable tools that provide ready access to your DNS data and enable your IT team to self-manage your DNS records and domains to whatever extent you want.

You cannot afford unresponsive or hard-to-reach support for DNS service. There's no reason to settle for poor or ineffective self-management resources, either.

Proactive DNS management tools. Some enterprises – particularly those with strong security concerns or large on-line presences and active content and microsite strategies– take a hands-on approach to DNS management. They regularly review and manage DNSSEC or add, delete, and update domains and DNS configurations. For these companies, the value of effective self-management tools is obvious.

Organizations that prefer a set-it-and-forget-it approach to DNS may doubt the value of these tools. But even occasional attention to DNS can improve network security while reducing the chance of inadvertent misconfigurations. For these companies, easy-to-use tools make periodic maintenance a far less time-consuming task.

Moreover, every enterprise can benefit from open access to their DNS traffic data and the unique analytical insights it can provide.

The key qualities to look for in a DNS toolset are secure but simple accessibility for your team, and an intuitive interface or comprehensive APIs that provide ready access to critical functions. The interface should make it simple to manage domains and records, and review and update DNSSEC configurations. It should also provide easy access to your DNS data, including audit logs, and incorporate filters and query capabilities to make it faster and simpler to isolate the specific information you want.

Give extra credit for a tool that offers automatic DNS configuration reviews that identify potential errors and issues, and provide standards-based recommendations for remediation.

24/7/365 support availability: DNS is not a 9-to-5 function. It goes without saying that you should be able to get support anytime of the day or night, any day of the year. Anything less than round-the-clock access at best leads to irritation – if a single device is misconfigured, for example – and at worst can result in serious consequences for your entire business – as when a misconfiguration involving multiple assets affects operations or compliance.

Note that "helpful" FAQs on your provider's website don't count. If some aspect of your DNS service goes south, you don't want to read about possible causes and try to work your way through an arcane troubleshooting procedure. **Round-the-clock availability of live support experts should be a non-negotiable capability of your DNS provider.**

Prompt responses to support requests: An important corollary to the 24/7/365 rule is that the support team responds quickly when you submit an email or web form. Round-the-clock support becomes far less valuable if you have to wait six or eight hours for a response to your support request. Ask your provider if they have a goal or SLA for response times, not only for genuine emergencies but for "routine" problems as well.

Direct access to qualified experts: Also important: that the prompt response to your support request comes from someone who can actually address your problem. Too many providers advertise 24/7 support that turns out to be little more than an answering service during off hours. If a configuration issue hits at 10:30 at night, you don't want to reach someone who takes notes on behalf of the experts who can actually answer your questions and solve your problem. You want to reach the experts.

Immediate support access in an emergency: Web and email forms are fine for minor or routine issues, at least when they trigger a prompt response. But in a genuine emergency that affects significant portions of your infrastructure, you can't afford to wait at all.

Make sure your provider offers direct telephone access to their support experts if you should need it -not as part of a "premium" support package, but just because you're a customer. Also make sure that their telephone access connects to actual support experts, and not to a telephone agent who is not qualified to help.

MORE EXPERIENCE =MORE HELPFUL SUPPORT

At Neustar Security Services, our approach to support has been shaped by our deep understanding of DNS and security. We know serious threats and issues impacting service must be addressed immediately with expert attention, a commitment that is embodied in our DNS support team.

One example is our goal to respond to every support request within an hour; our openly published telephone number for 24-hour support is another. But it's most evident in the deep experience our team brings to every issue. Our support team averages 7 years of experience with DNS, handling roughly 25 support requests every day. Do the math, and it comes out to more than 63,850 support requests handled, as quickly and painlessly as possible – all while earning 9.4 stars (out of 10) from our customers – along with verbatim comments like these:

"I had a problem. It was fixed quickly and painlessly. Now I don't have a problem. This makes me happy."

"Great response time. Solved issue on first creation. Great customer service."

"Fast, Friendly, and knowledgeable responses. I always use Neustar as the gold standard that all other support organizations need to strive to match."

"Prompt, courteous, and helpful communications from technician contributed to my rating of 10."

"Great support, very fast reply - appreciated! and diligent follow up."

THE FUNDAMENTALS MATTER MOST

Periodically, a well-funded start-up claims to have "reinvented" DNS and proffers a beautifully designed self-management GUI as evidence. The reality, of course, is that they've merely repackaged aspects of DNS service that may provide value – but only if the fundamentals work flawlessly.

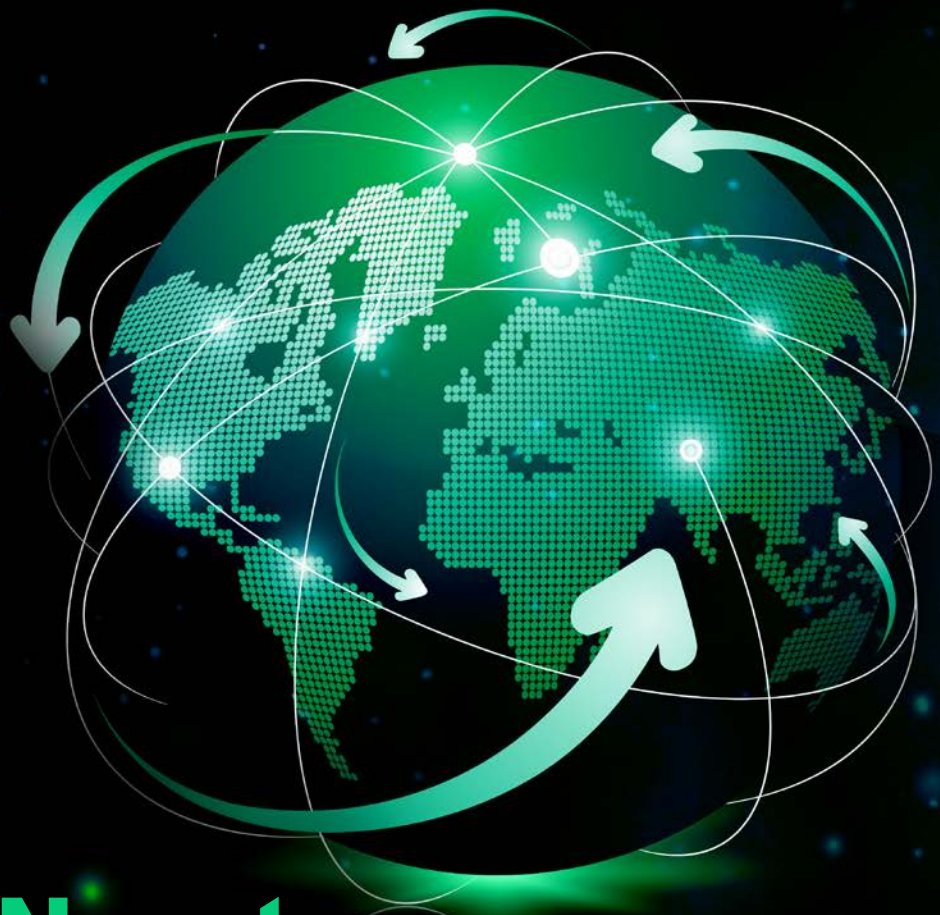
That's what you really need from a DNS service provider: flawless fundamentals. While DNS has been extended over the decades, it has not been reinvented. The core, standards-based transactions at the heart of DNS are more or less unchanged – and you need a provider who is relentlessly focused on completing them perfectly, every time.

You need a provider who specializes in enterprise-grade DNS, and understands and handles all the nuances of delivering it on a global scale – nuances that IT generalists may not appreciate.

You need a provider with a track record of demonstrated excellence in securing DNS service, optimizing its performance, delivering it with iron-clad reliability, and supporting it with deeply experienced professionals – while continually challenging itself to do better in every category.

When Neustar Security invented enterprise-grade UltraDNS service, we set a high bar for ourselves – and for other providers. Our team has worked tirelessly ever since to keep raising it to ever higher standards of excellence.

Your DNS deserves nothing less.



About Neustar Security Services

The world's top brands depend on Neustar Security Services to safeguard their digital infrastructure and online presence. Neustar Security Services offers a suite of cloud-delivered services that are always secure, reliable, and available and enable global businesses to thrive online. The company's Ultra Secure suite of solutions protects organizations' networks and applications against risks and downtime, ensuring that businesses and their customers enjoy exceptional, and uninterrupted, interactions all day, every day. Delivering the industry's best performance and always-on service, Neustar Security Services' mission-critical security portfolio provides best-in-class DNS, application and network security including DDoS, WAF and Bot management services to its global 5000 customers and beyond.

Find more information at:

neustarsecurityservices.com

Call USA: +1 (844) 929 - 0808
Call EMEA: +44 808 175 1189

WP-SS-58054-05.05.2022