FAQs

1. What is BSL's Apps Defender and how does it differ from traditional security solutions?

BSL's Apps Defender is not just a conventional security solution, it represents a transformative shift in network security strategy. In today's cybersecurity landscape, most solutions focus on addressing specific vulnerabilities and mitigating symptoms, which creates a false sense of security. Apps Defender takes a different approach: it redefines Zero Trust Networking from the ground up by eliminating the root causes of traditional network weaknesses.

Instead of adding more layers to address individual security gaps, Apps Defender fundamentally changes how networks operate by implementing advanced techniques such as **Level 4 micro-channels**, **Client-to-Client (C2C) topology**, and **advanced port mapping**. These methods ensure that no inbound ports are ever exposed, static IP addresses are concealed, and complex firewall rules become unnecessary. This architecture not only prevents attackers from exploiting known vulnerabilities but also removes the reliance on outdated paradigms like perimeter defences.

Apps Defender's intrinsic security model locks down networks at a foundational level, eliminating lateral movement and enhancing resilience by design. By addressing the core weaknesses of traditional network architectures, Apps Defender achieves long-term security with a streamlined, holistic approach that focuses on eliminating vulnerabilities rather than just mitigating them.

2. How does BSL's Apps Defender's Client-to-Client (C2C) Topology work, and are there any similar concepts in the IT world?

The Client-to-Client (C2C) Topology is a network structure where all inbound ports are permanently closed on both client and server endpoints. This means that there are no open ports to scan, no IPs to attack, and no lateral movement possibilities. The idea is similar to how video conferencing tools like Zoom, Teams, and remote desktop applications like AnyDesk and TeamViewer work. They rely on an intermediary broker or server to facilitate communication, thereby allowing both endpoints to keep their ports closed. Apps Defender expands this concept to any service by creating encrypted micro-channels between endpoints, ensuring that services can communicate securely without exposing their real network interfaces.

Moreover, Apps Defender's approach can be seen as a practical implementation of concepts used in the **dark web**: hidden services with no open inbound ports, accessible only through pre-authenticated, encrypted channels. In essence, Apps Defender takes the best practices from secure communication methods and applies them in a structured, enterprise-grade network security solution.

3. What is the difference between BSL's Apps Defender and a VPN?

While both BSL's Apps Defender and a VPN create secure communication channels, the similarities end there. Apps Defender provides **control beyond encryption**, focusing on:

- **Micro-Segmentation**: Apps Defender's Level 4 micro-channels isolate services on a per-connection basis, ensuring that each communication path is securely segmented. A VPN, in contrast, simply creates an encrypted tunnel between endpoints, which means that an attacker can still leverage vulnerabilities inside the VPN (e.g., insecure applications).
- **Network Lockdown:** With BSL's Apps Defender, there are **no open inbound ports**, meaning no external connections can even reach the service, unlike VPNs, which rely

on exposing certain ports for communication. This eliminates entire categories of attacks such as port scanning, brute-force attempts, and DoS attacks targeting exposed services.

- **Advanced Authentication**: Apps Defender uses Multi-Dimensional Authentication (MDA), ensuring that not just the user, but also the device, application, time, and location are verified. VPNs usually rely on a single factor (e.g., a certificate or password), making them vulnerable to credential theft.

- **Control Over Data Flow**: BSL's Apps Defender enforces a strict data flow policy, allowing only specific services and endpoints to interact. In contrast, VPNs often operate on a **"rubbish in, rubbish out"** principle: they don't inspect or control the quality of data, allowing potentially malicious payloads to traverse the network.

In summary, a VPN is a basic security tool that only ensures encrypted connectivity, while Apps Defender implements **real Zero Trust principles**, isolating services, enforcing strict access policies, and eliminating inbound attack surfaces. Apps Defender treats every part of the infrastructure as a potential weak point and builds security around minimizing the impact of any breach.

4. Shall I install an agent on each endpoint, especially on the server side?

Installing BSL's Apps Defender agents on every endpoint, including servers, is recommended to achieve the highest security level and ensure full control over each connection. When agents are installed on every endpoint, each service or device can only communicate through pre-defined, secure micro channels, eliminating any possible lateral movement or unauthorized access.

However, Apps Defender also offers a more flexible deployment through the use of **Access Points**. An Access Point is a secure gateway that can be deployed in front of a group of servers or services, creating a Trusted Are*. This setup provides security isolation similar to that achieved with full agent deployment but without modifying the server infrastructure. The Access Point manages all communications and enforces security policies at the perimeter, allowing for easy integration in environments where agent installation is not feasible, such as legacy systems or tightly controlled server environments.

5. What if the Apps Defender agent itself is vulnerable, or if servers have vulnerabilities in services or protocols, such as REST APIs?

The security model of Apps Defender assumes that vulnerabilities may exist in agents, services, or protocols. However, since Apps Defender's architecture closes all inbound ports at both client and server levels, these vulnerabilities cannot be exploited externally. In other words, even if a service has a known vulnerability, attackers cannot reach it because the server does not have any open ports to accept connections.

This aligns perfectly with the **assumed breach model** and a robust **cyber resilience strategy**: the infrastructure is designed to be secure even if some components are vulnerable. Apps Defender's micro channel approach ensures that only authorized communications are allowed to traverse the network, so even if the agent or the protocol is vulnerable, there's no way for an external attacker to initiate an exploit. This isolation not only prevents exploitation but also mitigates the risk of lateral movement, ensuring that even if an endpoint is compromised, the rest of the network remains secure.

6. Why do conventional cybersecurity vendors not offer a similar strategy?

The reason is not technical—it's business-driven. Most conventional cybersecurity vendors have established product lines centred around VPNs, firewalls, routers, and other traditional tools. If they were to migrate to a strategy like BSL's, they would face a significant loss in revenue because their current products would become redundant. For them, adopting Apps Defender's architecture would mean not being able to sell hardware and services that are staples of their business model.

This market block is rooted in the profitability of selling multiple, isolated products that address different aspects of network security instead of adopting an integrated approach that could reduce their clients' reliance on various standalone solutions. The shift to Apps Defender's model requires a change not just in technology but in mindset, which many vendors are hesitant to embrace due to potential disruptions to their current revenue streams.

7. Can BSL's Apps Defender eliminate the need for firewalls, routers, and endpoint detection solutions (EDRs)?

Yes, Apps Defender can significantly simplify your infrastructure by removing traditional elements like firewalls, routers, and EDRs. However, this is a journey that requires a shift in mindset and the adoption of new strategies. While Apps Defender's architecture renders many traditional tools redundant by permanently closing inbound ports and using micro-channels for communication, endpoint solutions like EDRs can still be used if there is a need to monitor and control endpoint activities. However, from the **assumed breach model** perspective, the endpoint is considered expendable. The focus is on protecting the infrastructure and preventing the infection from spreading.

The goal is to reach a point where you can afford an infected endpoint because BSL's Apps Defender ensures that such infections do not propagate and compromise the entire organization. With Apps Defender, you build your security around intrinsic, network-level protection, eliminating the attack vectors that would typically be managed by firewalls, intrusion detection systems, and segmentation routers.

8. How does Apps Defender's Level 4 Micro Channels differ from traditional IP-based segmentation?

Level 4 Micro Channels operate directly at the TCP/UDP transport layer, creating segmented, service-specific communication paths that inherently include firewall-like properties. Unlike traditional IP-based segmentation that relies on routing and ACLs, Apps Defender's micro channels ensure each channel is independently authenticated and encrypted, making them more secure, efficient, and resistant to common attacks such as IP spoofing or routing manipulations.

9. What is Advanced Port Mapping and how does it enhance security?

Advanced Port Mapping isolates services using synthetic IP addresses and virtual loopback interfaces, allowing BSL's Apps Defender to dynamically map ports without exposing the underlying IP plan. This approach provides robust service-level segmentation, making it impossible for attackers to deduce real IP addresses or access unauthorized services. It also integrates seamlessly with existing TCP/ UDP protocols, ensuring zero overhead and no performance degradation.

10. How does BSL's Apps Defender handle micro-segmentation?

BSL's Apps Defender introduces micro-segmentation at the service level through TCP micro-channels and advanced port mapping. Each communication path is defined and isolated at the

transport layer (OSI Level 4), allowing only specific service-to-service communications. This design ensures that, even if devices share the same subnet, they can only communicate through predefined secure channels, preventing any form of unauthorized interaction or lateral movement.

11. What role does Multi-Dimensional Authentication play in BSL's Apps Defender?

Multi-Dimensional Authentication (MDA) validates multiple attributes simultaneously—including user, device, application, location, and time. This ensures that only legitimate entities can establish a connection. For example, even if an attacker has user credentials, they will still be denied access if the device, application, operational environment, time or location does not match the expected values. This granular approach to authentication goes beyond traditional multi-factor authentication (MFA) by adding contextual and continuous verification layers.

12. How does Apps Defender implement Quantum-Resistant Security?

Apps Defender integrates Post-Quantum Cryptography (PQC) algorithms to secure communications against future quantum threats. It also employs a cryptographic control channel that manages real-time key evolution, noise generation, and algorithm swapping. These measures ensure that BSL is not only secure today but also future-proof, providing long-term protection as new threats emerge.

13. What is the impact of Apps Defender's approach on network infrastructure?

Apps Defender's security architecture is designed to work seamlessly on top of existing infrastructure without requiring major changes. The solution operates at the network overlay level, meaning there is no need to reconfigure firewalls, routers, or subnets. This allows for easy integration into current environments while achieving advanced security without disruptions or costly upgrades.

14. Can Apps Defender be used in a hybrid cloud or multi-cloud environment?

Yes. Apps Defender supports deployment in various environments, including on-premises, private cloud, public cloud, and hybrid setups. The flexibility of Apps Defender's architecture ensures that security policies are consistently enforced across all environments, regardless of where the applications or services reside. It isolates cloud instances using virtual private networks within the C2C topology, maintaining secure communication paths even across geographically distributed cloud infrastructures.

15. How does Apps Defender impact network performance and latency?

Apps Defender's architecture is optimized for zero overhead in encryption, latency, and bandwidth usage. By using efficient cryptographic methods and leveraging Layer 4 transport-level segmentation, App's Defender ensures that its security measures do not introduce significant latency or congestion. This allows for smooth performance even in high-demand environments such as financial services and IoT ecosystems.

16. What about compliance with standards like PCI-DSS or GDPR?

Apps Defender's micro-segmentation and zero-trust architecture provide a strong foundation for

compliance. By implementing strict control over who can access what and enforcing continuous verification, BSL's Apps Defender meets and often exceeds the requirements of standards like PCI-DSS, GDPR, and others. It ensures that sensitive data is isolated, encrypted, and only accessible to authorized entities, making it easier for organizations to demonstrate compliance.

17. How is Apps Defender deployed on the client side?

Apps Defender can be deployed as a lightweight agent on client devices, or as an SDK integrated into applications. This allows for flexible deployment options depending on the use case, ranging from mobile applications to enterprise workstations. The agent or SDK manages secure communication channels, authentication, and encryption without interfering with the normal operations of the device or application.

18. How does Apps Defender address DDoS and Penetration Attacks?

By design, Apps Defender eliminates open ports and static IP addresses, significantly reducing the attack surface. With no exposed endpoints, DDoS attacks cannot find a target to overload. Moreover, the use of multi-dimensional authentication and continuously evolving cryptographic keys ensures that penetration attempts are blocked at multiple layers, making traditional attacks like port scanning and brute-force ineffective.

19. Can I challenge penetration test companies to breach my Apps Defender-based infrastructure?

Yes, if properly configured, Apps Defender's architecture makes it extremely difficult for penetration testers to even start their evaluation. With Apps Defender, each endpoint (client or server) operates with all inbound ports closed. This means the very first step in most penetration tests—port scanning—will yield zero open ports. Since there are no accessible ports, the testers cannot establish any external connections or identify entry points to launch an attack, even if there are actual vulnerabilities in the server or application code. This effectively renders traditional penetration testing methodologies useless, highlighting Apps Defender's strength in eliminating attack surfaces by design.

20. Hackers often try to kill cybersecurity processes like anti-ransomware, anti-malware, and EDR solutions. What happens if they kill the Apps Defender agent?

In traditional cybersecurity, killing the protective agent (e.g., anti-malware, anti-ransomware, or EDR solutions) can open the floodgates for attackers, allowing them to exploit the system without resistance. However, BSL's Apps Defender functions differently. Apps Defender agents do not act as barriers but as creators of authorized, encrypted communication channels within a secure network overlay. If an attacker successfully kills an Apps Defender agent, they don't gain access to the network—instead, the opposite occurs: the server or endpoint becomes completely isolated, with all communication channels severed. This means no external entity can connect to or reach that server, making it even more secure and contained in the event of a compromised endpoint.

21. Why is the Apps Defender approach aligned with the assumed breach model and cyber resilience?

The Apps Defender architecture is built around the assumption that individual components or endpoints might be breached. Its focus is on ensuring that any breach is contained and cannot

propagate through the network. By implementing a zero inbound port strategy and ensuring that all communication channels are isolated and controlled, Apps Defender mitigates the risk of a breach spreading. This aligns perfectly with the assumed breach model and provides resilience at the infrastructure level, making Apps Defender ideal for organizations looking to achieve true cyber resilience.

22. What are some real-world use cases for BSL's Apps Defender?

Apps Defender has been successfully deployed in sectors such as financial services, critical infrastructure, and government agencies. Use cases include secure communication for remote access to critical systems, protecting mobile banking applications, and providing secure, isolated communication channels for IoT devices in industrial settings. The flexibility and robustness of Apps Defender make it suitable for both large-scale enterprises and niche deployments requiring high security.

23. How do Apps Defender's zero overhead in bandwidth, low latency, anti-shaping techniques, and automatic reconnection impact operations and costs?

Apps Defender is designed with performance and operational efficiency in mind. Unlike traditional security solutions that often add layers of encryption and routing, leading to increased bandwidth usage and latency, Apps Defender operates with zero overhead. This means that there's no additional data payload added to the packets during encryption or transport, which preserves bandwidth and reduces transmission costs.

- **Low Latency:** Apps Defender's architecture avoids the bottlenecks caused by typical security proxies and packet inspection tools. It implements encryption directly at the transport layer (Layer 4), ensuring that latency is minimized even under high load.
- **Anti-Shaping Techniques:** Apps Defender dynamically adjusts its packet flow to avoid bandwidth shaping by ISPs, ensuring stable throughput without disruption. This is especially useful in environments where bandwidth is a cost-sensitive resource.
- **Automatic Reconnection:** Apps Defender's intelligent reconnection feature minimizes downtime, maintaining secure connections even during temporary network outages or dynamic IP changes, reducing operational disruptions and ensuring that services remain available.

Overall, these features ensure that the operational costs associated with maintaining secure communication are minimized, leading to smoother performance, lower bandwidth costs, and enhanced reliability without compromising security.

24. How does Apps Defender reduce the cost of energy? Is it a green solution?

Yes, Apps Defender is inherently a green solution due to its energy-efficient design. By stopping unwanted packets at the source and ensuring that only authorized and essential communications are transmitted, Apps Defender reduces the need for unnecessary packet handling and processing, which is a common source of energy consumption in traditional network security setups.

- **Energy Efficiency in Packet Transmission**: With **zero overhead encryption** and streamlined communication paths, Apps Defender requires less computational power to encrypt, decrypt, and transfer packets. This results in lower CPU and memory usage on the devices, reducing the overall energy footprint.
- **Minimal Data Processing**: Because Apps Defender blocks unauthorized connections at

the network overlay level, there is less data to filter, inspect, or drop at the endpoints. This minimizes the processing workload and reduces power consumption across the network infrastructure.

- **No Need for Constant Packet Scrutiny**: Unlike traditional security solutions that continuously inspect and log every packet, Apps Defender's intrinsic design ensures that only approved packets are processed, saving computational energy.

These factors make BSL's Apps Defender a **cost-effective and green solution**, promoting lower energy consumption and a reduced carbon footprint compared to conventional security mechanisms.

25. How is Apps Defender different from other Zero Trust products in the market or Zero Trust as a Service solutions?

Many so-called Zero Trust solutions in the market, and other Zero Trust as a Service (ZTaaS) providers, offer centralized, cloud-based inspection of your data, claiming to provide Zero Trust security. However, these solutions still rely on the conventional paradigm of data inspection and centralized control, which inherently contradicts the Zero Trust principles. You have to trust that these service providers will not collect, inspect, or store your sensitive data. In reality, this means placing a great deal of faith in a "Zero Trust" service that actually requires you to trust the provider. BSL's Apps Defender, on the other hand, operates on a fundamentally different approach:

- **True End-to-End Encryption**: Apps Defender's architecture ensures that your data is not just encrypted, but also that all channels are isolated and controlled end-to-end, with no middleman able to inspect or alter your data flow.

- **No Data Inspection**: Apps Defender is built to prevent the need for third-party inspection. Its intrinsic security principles eliminate data exposure to external entities, ensuring that your organization retains full control and visibility over its communication.

- **Beyond Detection**: Most Zero Trust solutions focus on enhanced detection capabilities, adding layers of monitoring and alerts. BSL's Apps Defender, by contrast, **changes the foundational way** you secure your network by **locking down** endpoints and isolating every communication path through micro-segmentation and Layer 4 Micro Channels. This isn't just a new layer of detection—it's a completely different approach that prevents breaches by default, without relying on inspection.

In short, Apps Defender's true Zero Trust model eliminates the need to trust third-party providers while transforming the security landscape with a **new mindset** that goes beyond detection and reaction, providing intrinsic security by design.

26. How does Apps Defender integrate into conventional environments, and what should be considered during the integration process?

Apps Defender is designed to seamlessly integrate with conventional IT environments and existing services, but it is crucial to maintain its high-security standards during integration to avoid weakening the overall security posture. While Apps Defender can interface with systems like Active Directory (AD) to import users and groups, it's important to **avoid using traditional authentication methods** as substitutes for Apps Defender's **Multi-Dimensional Authentication (MDA)**. For example:

- **AD Integration**: You can import users and groups from AD, but **do not rely on**

AD for primary authentication. Apps Defender's MDA, which includes user, device, application, location, and time attributes, should remain the primary authentication method to prevent the introduction of legacy vulnerabilities.

- **Application-Level Authentication**: Apps Defender can coexist with existing application-level authentication mechanisms, but it must still **enforce its own Post-Quantum Cryptography (PQC) authentication** to ensure end-to-end security. By bypassing Apps Defender's intrinsic authentication methods, you risk compromising the integrity of the Zero Trust model.

The key is to **integrate Apps Defender's advanced security features without diluting its foundational principles**. Maintaining Apps Defender's Zero Trust approach means that while it can work within traditional setups, you should not revert to legacy methods that may undermine the enhanced security framework.