**FOOTPRINTING REPORT ON LIMELIGHT**

Company Name: Limelight

Overview:

It is a leading fashion and lifestyle brand offering a wide range of trendy and affordable clothing, accessories, and home textiles. Limelight is known for blending traditional and contemporary designs, making it a go-to choice for fashion-conscious customers.

Key Services and Products:

Offers a diverse collection of fashion and lifestyle products, including:

Women's and men's apparel (casual, formal, and festive collections)

Unstitched fabrics for customized fashion

Accessories such as handbags, jewelry, scarves, and shoes

Home textiles including bedding and décor

Fragrances and beauty products

Contact Info:

Office Address: 6 Raffles Quay, #14-06, Singapore (Postal 048580)

Email Address: support@limelightfashion.com

Domain Information:

Domain Name: limelightfashion.com

Domain Lookup:

Site: https://www.limelightfashion.com/

Netblock Owner: Cloudflare, Inc.

Hosting Company: Cloudflare

Hosting Country: US

IPv4 Address: 104.18.43.206 (VirusTotal)

IPv4 Autonomous Systems: AS13335

IPv6 Address: Not Present

IPv6 Autonomous Systems: Not Present

Reverse DNS: Unknown

Domain Registrar: markmonitor.com

Nameserver: ns1-35.azure-dns.com

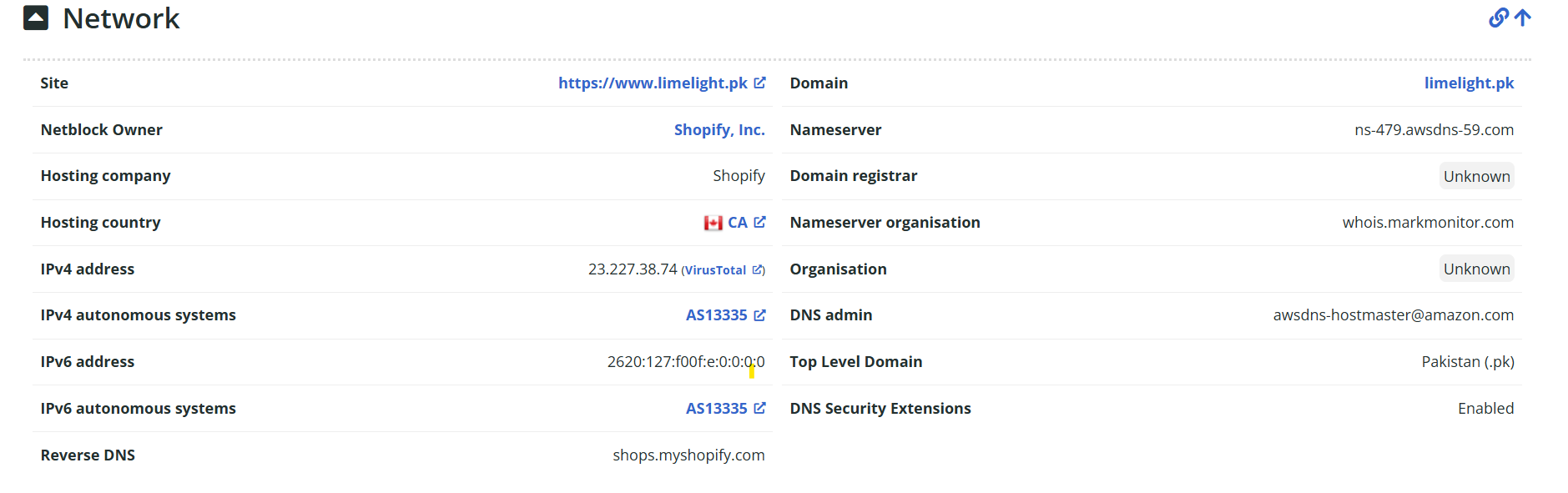
Nameserver Organisation: whois.markmonitor.com

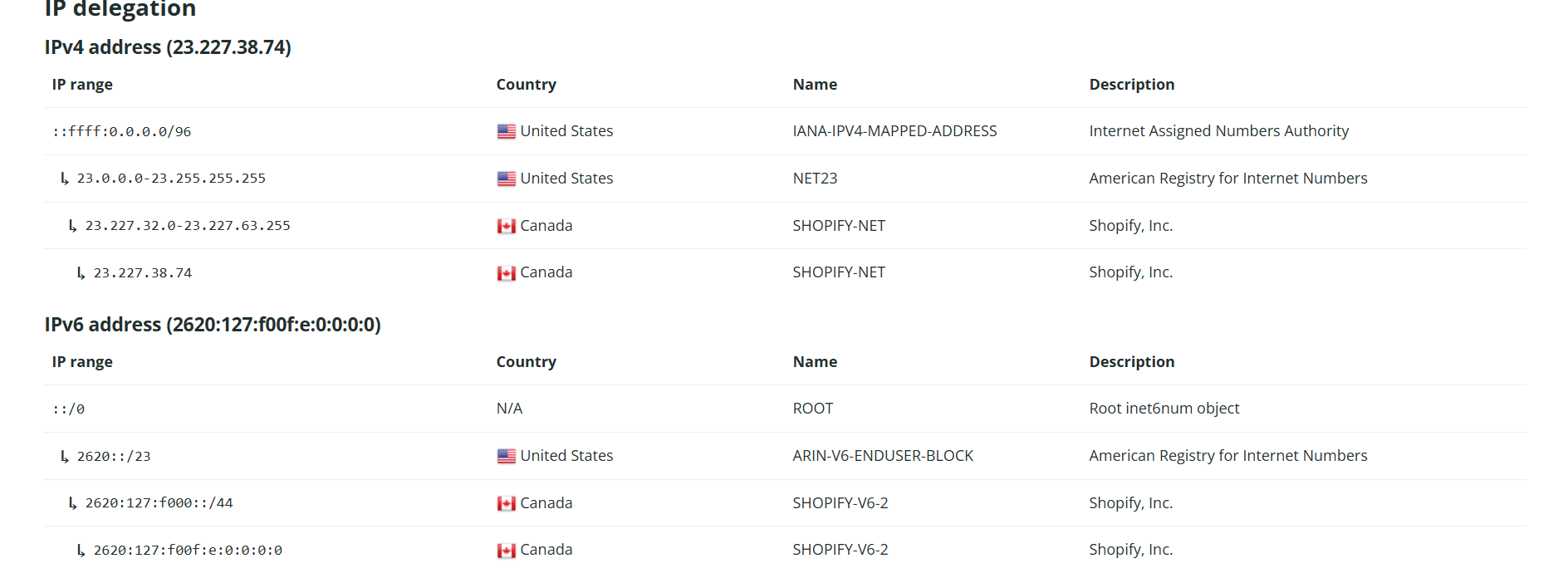
Organisation: Limelight Group Inc., United States

DNS Admin: azuredns-hostmaster@microsoft.com

Top-Level Domain: Commercial entities (.com)

DNS Security Extensions: Enabled





1. Multi-Layered Defense Strategy:

DDoS Protection: Implement robust Distributed Denial of Service (DDoS) mitigation services. Limelight's DDoS Attack Interceptor (DAI) offers high-capacity on-network scrubbing, detecting and neutralizing malicious traffic before it impacts performance.

BUSINESSWIRE.COM

Web Application Firewall (WAF): Deploy WAF solutions to safeguard web applications from threats like SQL injection and cross-site scripting. Limelight's WAF is integrated into their global infrastructure, ensuring minimal latency while providing protection.

INVESTORS.EDG.IO

2. Advanced Bot Management:

Utilize bot management tools to differentiate between legitimate and malicious bot traffic. Limelight's Advanced Bot Manager ensures the availability of web infrastructure by blocking harmful bots and allowing beneficial ones, maintaining revenue-generating traffic.

SECURITY INFORMED

3. Secure Cloud Infrastructure:

Access Controls: Enforce strict access policies for cloud resources, employing multi-factor authentication and regular reviews of access rights. Limelight's administrative access to cloud resources is protected by mandatory two-factor and SSH Public Key Infrastructure (PKI) authentication systems, limited to senior technical staff.

GOLIMELIGHT.COM

Regular Audits: Conduct frequent vulnerability scans and penetration tests to identify and address potential security gaps. Limelight regularly performs these assessments to ensure a securely configured infrastructure.

GOLIMELIGHT.COM

4. Data Encryption and Backup:

Encryption: Ensure that client data is encrypted both at rest and in transit using robust encryption standards like AES-256 and TLS 1.2. Limelight encrypts client data at rest with the AES-256 algorithm and in transit using secure transmission protocols such as HTTPS, SFTP, TLS 1.2, and SSH.

GOLIMELIGHT.COM

Backups: Implement daily backups stored in highly available and durable storage solutions, with the ability to recover data upon client request. Limelight's client data backups are stored on AWS Block Storage systems with 99.99% availability and 99.999999999% durability.

GOLIMELIGHT.COM

5. Application Security:

Access Management: Control employee network access using systems like Windows Active Directory, and enforce strict password policies. Limelight employs Windows Active Directory to manage employee network access and enforces strict password policies through Group Policies.

GOLIMELIGHT.COM

Device Security: Restrict administrative privileges on employee devices, ensure encryption, and maintain up-to-date security patches. Limelight ensures that employee laptops are encrypted, do not have administrative privileges, and are regularly patched according to a formal Patching Policy.

GOLIMELIGHT.COM

6. Network Traffic Monitoring:

Leverage network observability platforms to gain real-time insights into traffic patterns, facilitating rapid issue detection and resolution. Limelight's partnership with Kentik has enabled them to reduce Mean Time To Repair (MTTR) from approximately 1.5 hours to just 20 minutes by quickly identifying and addressing traffic issues.

KENTIK

7. Compliance and Training:

Compliance: Align security policies and practices with recognized standards such as ISO 27002:2013 and SOC Type 2. Limelight organizes its Information Systems Security policies to comply with these standards.

GOLIMELIGHT.COM

Training: Provide continuous training to staff on IT security policies and best practices to foster a security-aware culture. Limelight ensures that its staff is continually trained on IT security policies and best practices.

GOLIMELIGHT.COM

By adopting these comprehensive cybersecurity measures, organizations can enhance their resilience against cyber threats, ensuring the protection and integrity of their digital assets.

**Conclusion**

Limelight (now Edgio) has developed a strong cybersecurity framework that integrates multi-layered defenses, advanced bot management, secure cloud infrastructure, encryption, application security, and continuous monitoring. Their approach ensures the protection of digital assets through proactive threat mitigation, strict access controls, and compliance with industry standards. By implementing these best practices, organizations can enhance their security posture, minimize cyber risks, and maintain a reliable and secure digital environment.