SOLUTION NOTE

THE IMPORTANCE OF SECURITY IN MODERN TELECOMMUNICATIONS NETWORKS

OVERVIEW

Modern telecom networks are transforming into telco clouds, with complex private, public and hybrid networks across many domains.

Computing and storage resources move to the network edge for new service processing and delivery, but security risks also increase. Third-party apps and external attackers pose unprecedented and multifaceted challenges for telecom providers. These critical networks are the backbone of the digital economy but are also exposed to evolving threats. They need a new era of cybersecurity solutions to protect them from harm and ensure their reliability, privacy and integrity.

TELECOM NETWORKS HAVE EVOLVED

As a communication service provider (CSP) your network is likely undergoing a profound transformation as you transition from rigid, hardware-based systems to dynamic, software-defined telco clouds. This shift is essential to meet the evolving needs of your consumer and enterprise customers for 5G, edge computing and advanced broadband services. However, legacy infrastructure, siloed solutions and manual processes can hinder your network transformation, leading to inefficiencies, operational delays and potential errors.

In contrast to enterprise networks, which are typically smaller and more straightforward, telecom networks like yours are vast, intricate ecosystems that encompass various domains, technologies and locations. You face the formidable challenge of ensuring the agility, integration, scalability, efficiency and security of your network, which includes core, service and access domains:

- The core network is responsible for transporting and routing traffic across the network, using various protocols and technologies such as IP, MPLS, Ethernet and optical. It must ensure network infrastructure and service reliability, availability, scalability and flexibility to handle increasing traffic volumes and diversity. As a CSP, you must secure core network infrastructure and services against cyber threats like DDoS, malware, ransomware, data breaches and fraud. At the same time, your organization must also ensure the robustness, availability, scalability and adaptability of network operations, particularly with the growing diversity and complexity of traffic.

KEY CAPABILITIES

Reinforce Security Protection
Detect and block exploits, phishing, ransomware and other modern malware that other solutions miss.

Increase Visibility
Gain precise visibility and rich network context by integrating with IP address management asset metadata for optimum event understanding and correlation.

Accelerate Incident Response
Reduce time to remediation by automatically correlating event, network and threat intelligence from dozens of sources to speed investigations by as much as two-thirds.

Improve Security ROI
Recognize maximum value with minimal effort through stronger defenses and greater efficiencies in security operations—and get more out of your SIEM and SOAR platforms and other security tools.

Reduce Security Overhead
Leverage rich event, threat intelligence and AI/ML-based analytics on DNS for scalable protection against modern malware and DNS threats.

Minimize Network Disruption
Maintain DNS integrity and stop external and internal DNS DDoS attacks that can take your network offline.

- The service network delivers value-added services and applications to subscribers, using platforms like IP Multimedia Subsystem (IMS), Next Generation Networking (NGN) and cloud computing. Its mission is to provide high-quality, personalized user experiences while safeguarding data and application privacy and integrity. To achieve this mission, you must deliver seamless, personalized services across diverse devices and networks. In providing these services, your requirements are much the same as those associated with your core network. Those requirements include safeguarding data and application privacy, maintaining high availability and resilience in the face of disruptions, supporting various service platforms and technologies and defending against cyber threats, fraud and breaches.
- The access network connects users and devices with various technologies, such as smartphones, tablets, IoT/IIoT and more. It must meet the growing needs for bandwidth and coverage, while ensuring network performance, service quality, security and mobility.

THE CHALLENGE

Telecommunications service provider networks are prime targets for security threats due to their critical role in supporting essential sectors like government, finance, health, education and entertainment. These networks facilitate the transmission of voice, data and multimedia over long distances and diverse platforms while also enabling the proliferation of cloud computing, the IoT and mobile devices. They are appealing targets for cyber adversaries aiming to disrupt, intercept or manipulate communications for various ends.

Security is a paramount concern across all provider network domains, including yours, requiring comprehensive protection for network infrastructure, services, applications and users. Your organization must confront a multitude of threats and risks that can undermine network performance and integrity, potentially resulting in financial and reputational damage that can adversely impact your customers and competitiveness. With increasing resource deployment at the network edge, your security teams manage numerous pods, virtual machines (VMs) and containers across physical, virtual and cloud environments. Across such diverse infrastructure, unpatched devices can become vulnerable attack points. Endpoint protection with detection and response capabilities is a crucial security baseline. However, fully safeguarding your CSP network also requires mature cybersecurity solutions that bolster visibility, identify contemporary threats, accelerate investigative processes and streamline incident response.

INFOBLOX SOLUTIONS FOR TELECOMMUNICATIONS SERVICE PROVIDERS

Improve Security Effectiveness and Resiliency Across All Network Domains

With Infoblox, you can deliver reliable, secure, high-performance telecom services to your customers. Unique in the industry, our security solutions for telecom service providers unite networking and security through shared visibility and control over who and what connects the network across all on-premises, hybrid and multi-cloud infrastructure. On the networking front, our solutions automate network visibility, scalability and management. On the security side, Infoblox enables you to reduce incident response times by two-thirds. We do so by enabling all the major components of your security

BEFORE

Operational Inefficiencies

Inefficient security operations, characterized by a lack of automation and dependence on isolated solutions, coupled with integration barriers stemming from the absence of network and security product integration.

Scalability and Visibility Limitations

Challenges with scaling security during the transition from centralized to edge locations, compounded by poor network visibility and contextual gaps that foster silos and impede security response and capabilities.

Overburdened Security Operations

High alert volumes and time wasted on false-positive alerts contribute to alert fatigue among SOC analysts and possibly missed threats.

stack, including security, orchestration, automation and response (SOAR) systems, to respond to security events sooner, before they cause harm. Our solutions also reduce business disruptions caused by DDoS and other DNS-based risks and attacks that explicitly target CSP networks.

Gain New Levels of Speed and Automation

Infoblox solutions give you the enhanced speed and automation required to continually evolve your CSP network. These outcomes are made possible through centralized management that automates, streamlines and orchestrates networking and security from the data center to the edge. In addition, Infoblox enables massive scale with the highest levels of availability and resiliency.

Maximize Your Existing Threat Defense Investment

As part of the industry's leading DNS Detection and Response capabilities, Infoblox BloxOne® Threat Defense strengthens and optimizes your security posture from the foundation up. It maximizes brand protection by securing your existing networks and digital imperatives like 5G deployments, advanced broadband, edge computing and the cloud. It uses a hybrid architecture for pervasive, inside-out protection, powers SOAR solutions by providing rich network and threat context, optimizes the performance of the entire security ecosystem and reduces your total cost of enterprise threat defense.

Enhance Security Operation Center Efficiency

Reduce Incident Response Time

- Automatically block malicious activity and provide the threat data to the rest of your security ecosystem for investigation, quarantine and remediation.
- Optimize your SOAR solution using contextual network and threat intelligence data and Infoblox ecosystem integrations (a critical enabler of SOAR).
- Reduce threat response time and OPEX.
- Reduce the number of alerts to review and the noise from your firewalls.

Unify Security Policy with Threat Intel Portability

- Collect and manage curated threat intelligence data from internal and external sources and distribute it to existing security systems.
- Reduce the cost of threat feeds while improving the effectiveness of threat intel across the entire security portfolio.

Faster Threat Investigation and Hunting

- Make your threat analysts team 3x more productive by empowering security analysts with automated threat investigation, insights into related threats and additional research perspectives from expert cyber sources to make quick, accurate decisions on threats.
- Reduce human analytical capital needed.

AFTER

Enhanced Security Performance and Efficiency

Block threats sooner and reduce incident response times with automation and security tool integration.

Scalable and Secure Network Architecture

Deploy high-performance, resilient and secure networks from data centers to the far edge with advanced network solutions.

Improved Visibility and Remediation

Leverage new context to eliminate blind spots, speed up threat investigations and accelerate response with a new security stack.

KEY BENEFITS

Stop Threats That Other Defenses Miss

Better threat intelligence makes every security tool more effective. BloxOne Threat Defense collects, curates and aggregates threat information from Infoblox, your other commercial tools and third-party and government sources. Curation by the Infoblox Threat Intelligence Group drives accuracy while reducing false positives and enables you to customize the mix based on your needs. A normalized "super-feed" can then be shared across the security stack, boosting the effectiveness of every defense.

Block Malware and Data Exfiltration

BloxOne Threat Defense operates at the DNS level to see threats that other solutions do not and stops attacks earlier in the threat lifecycle. The solution leverages multi-sourced threat intelligence and powerful AI/ML to block devices from accessing malicious sites, prevent command-and-control (C&C) communications and reduce DNS-based data theft and other malicious activity.

Minimize Business Disruptions

DNS is foundational to every service provider because it ensures mission-critical network connectivity. If your DNS is down, your network and your services are down. Successful DDoS attacks can cost a service provider hundreds of thousands of dollars in lost monthly revenue. Infoblox Advanced DNS Protection (ADP) effectively shields you from the widest range of DNS DDoS attacks, maintaining critical service uptime.

Speed Investigation and Remediation

Security analysts need access to trusted threat intelligence and other contextual data about an event to accelerate responses. With Dossier™ as part of BloxOne Threat Defense, analysts gain a single view into threat intelligence associated with an event. Fast access to event-specific intelligence can accelerate threat investigations by as much as two-thirds.

Enhance SIEM, SOAR and More

Eliminate the overwhelm that comes from managing and responding to hundreds or thousands of alerts a day generated by dozens of defense-in-depth security tools by automating responses across your security stack.

Threat Intelligence Scaling

Apply comprehensive intelligence from Infoblox research and third-party providers to enforce policies on-premises or in the cloud and automatically distribute it to the rest of the security infrastructure.

Improve DNS Scalability and Resiliency

Decrease the number of physical and virtualized network functions while maintaining uptime. Improve reliability with automated HA/DR and reduce downtime by eliminating slow, manual error-prone upgrade processes. Become more responsive to changing business needs with a distributed approach that enables rapid upgrades via Infoblox Grid and more flexible responses to network architecture/topology changes.

Simplify and Streamline Network Change and Configuration Management

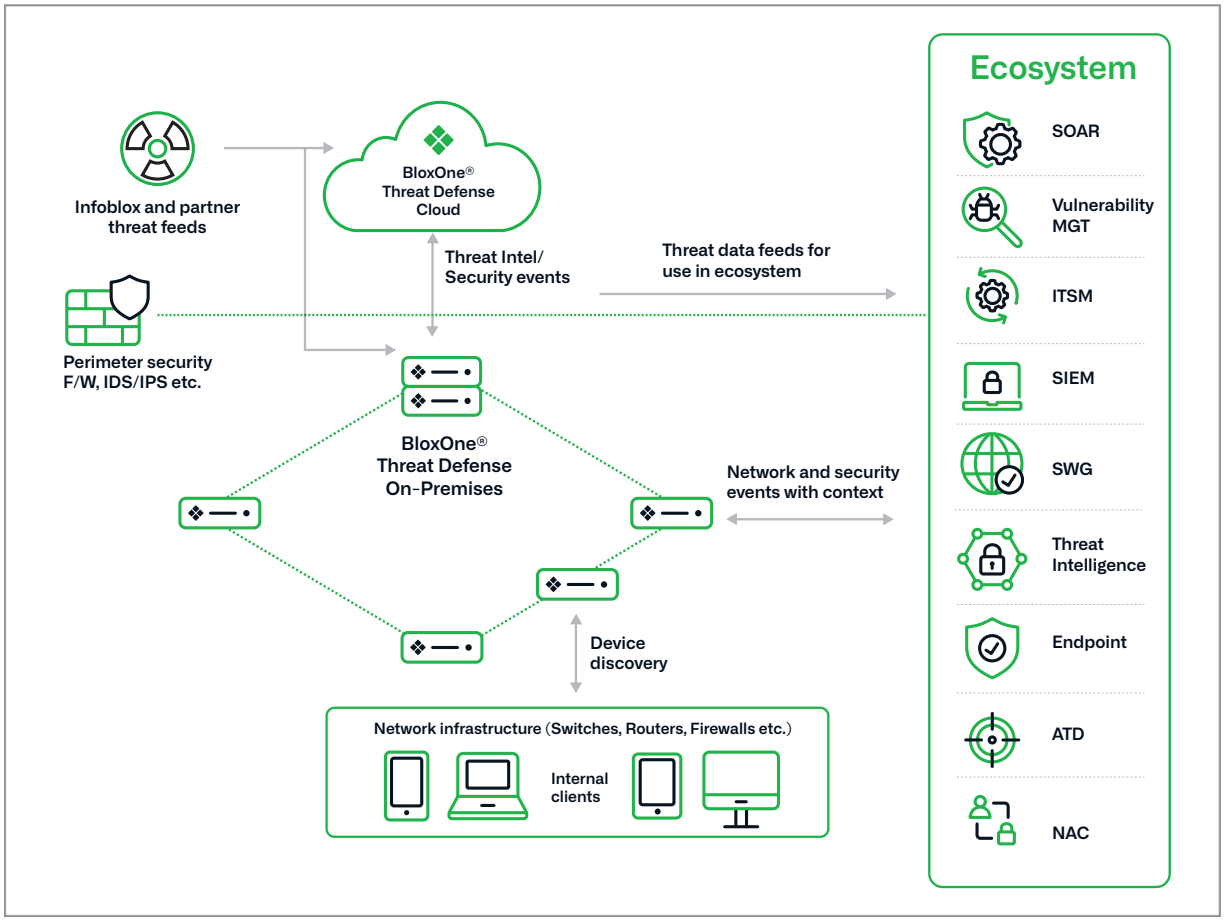

Figure 1: Infoblox strengthens and optimizes communications service provider networks

CONCLUSION

As your telecom network transforms to meet the demands of 5G, edge computing and advanced broadband services, security becomes a vital and complex challenge that requires a holistic and proactive approach. You must protect your network infrastructure, services, applications and subscribers across core, service, and access domains while ensuring network performance, reliability, scalability and flexibility. Delivering on these CSP requirements requires mature cybersecurity solutions that can provide comprehensive visibility, threat detection, investigation and response capabilities across physical, virtual and cloud environments. By leveraging Infoblox security solutions for telecom service providers, you can enhance your network's security posture, mitigate risks and consistently deliver the safe, high-quality experiences your subscribers demand.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230922v1