DATASHEET

Infoblox for Telecom Security Groups

Improve security effectiveness and resiliency and elevate SecOps efficiency

THE CHALLENGE

Today's communications service provider (CSP) networks are evolving to telco clouds spanning private, public and hybrid networks—expanding operational domains across the RAN, cable and core networks, private and public clouds and multi-access edge locations. With compute and storage moving to the edge to enable new types of service processing and delivery at thousands of new sites, the potential for security threats, both from third-party applications and external attackers, increases dramatically. Operators store vast amounts of personal data and are responsible for the stability of their communication services. Widespread deployment of devices outside the data center also exposes an expanding number of access points and creates a massive threat surface that attackers can exploit. A data breach or service failure resulting from a cyber attack can lead to severe financial and reputational damage or impact on customers—a substantial blow for any company to withstand in a highly competitive market.

With more resources deployed at the far edge, operator IT and security teams must manage significantly more pods, VMs—sometimes hundreds at a time, and potentially thousands of containers—in physical, virtual and cloud environments. Unpatched devices can become points of compromise. And while endpoint protection with detection and response capabilities is a must-have, already strained security teams must recognize the signs of an attack no matter what in an evolving and growing network. CSPs require mature cyber security solutions that expand their visibility to identify modern threats, shorten investigations and accelerate efficient incident response.

THE SOLUTION

Infoblox solutions for service providers enable the crucial IP connections between your subscribers and their digital world. We unite DNS, DHCP and IP address management (DDI) to automate network visibility, scalability and management. Our solutions help reduce incident response times by two-thirds by enabling all the major components of your security stack, including security, orchestration, automation and response (SOAR) systems, to respond to security events sooner, before they cause harm. We also help providers minimize business disruptions caused by DDoS and other DNS-based risks and attacks.

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.

Infoblox lowers the total cost of your threat defense by reducing the burden on stretched perimeter defenses. Our solutions enable security teams to get more value out of existing third-party security solutions through the real-time, two-way sharing of security event information and through automation that lowers the costs associated with manual effort and human error. Security analysts can gain a single view into threat intelligence associated with an event and cut threat investigation time by as much as two-thirds.

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

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 Cyber Intelligence Unit (CIU) drives accuracy while minimizing 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. Block malicious site access, command-and-control (C&C) communications, DNS-based data theft and other malicious activity by leveraging multi-sourced threat intelligence and powerful AI/ML.

Minimize Business Disruptions

DNS is foundational to every organization because it provides mission-critical network connectivity. If your DNS is down, your business is down. Successful DDoS attacks can cost an organization 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 service uptime for your organization.

Speed Investigation and Remediation

Analysts need access to trusted threat intel and other contextual data about an event to accelerate responses. With DossierTM 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

Armed with a plethora of defense-in-depth tools, cyber security teams can be overwhelmed by the need to manually manage dozens of security tools and respond to hundreds or thousands of alerts every day. Infoblox’s Ecosystem Exchange offers a highly interconnected set of integrations that enable security teams to eliminate silos, optimize their SIEM and SOAR solutions and improve the ROI of their entire cyber security ecosystem.

Ease SecOps Burdens with Automation

BloxOne Threat Defense includes many features that empower you to leverage threat intelligence, event information and other data more intelligently. Automation eliminates management overhead and makes SecOps investigation and response tasks more efficient. Decrease the burden on strained perimeter security devices such as firewalls, IPSs and web proxies by using your already available DNS servers as the first line of defense.

Simplify and Streamline Network Change and Configuration Management

The roots of many network problems can be traced to changes—mistakes made when manually changing devices, the setting of poor configurations that cause problems later and the undermining of critical security policies and network protection. Infoblox NetMRI is a network change and configuration management solution that automates routine workflows such as device provisioning and security operations, enabling tighter compliance and faster incident response.

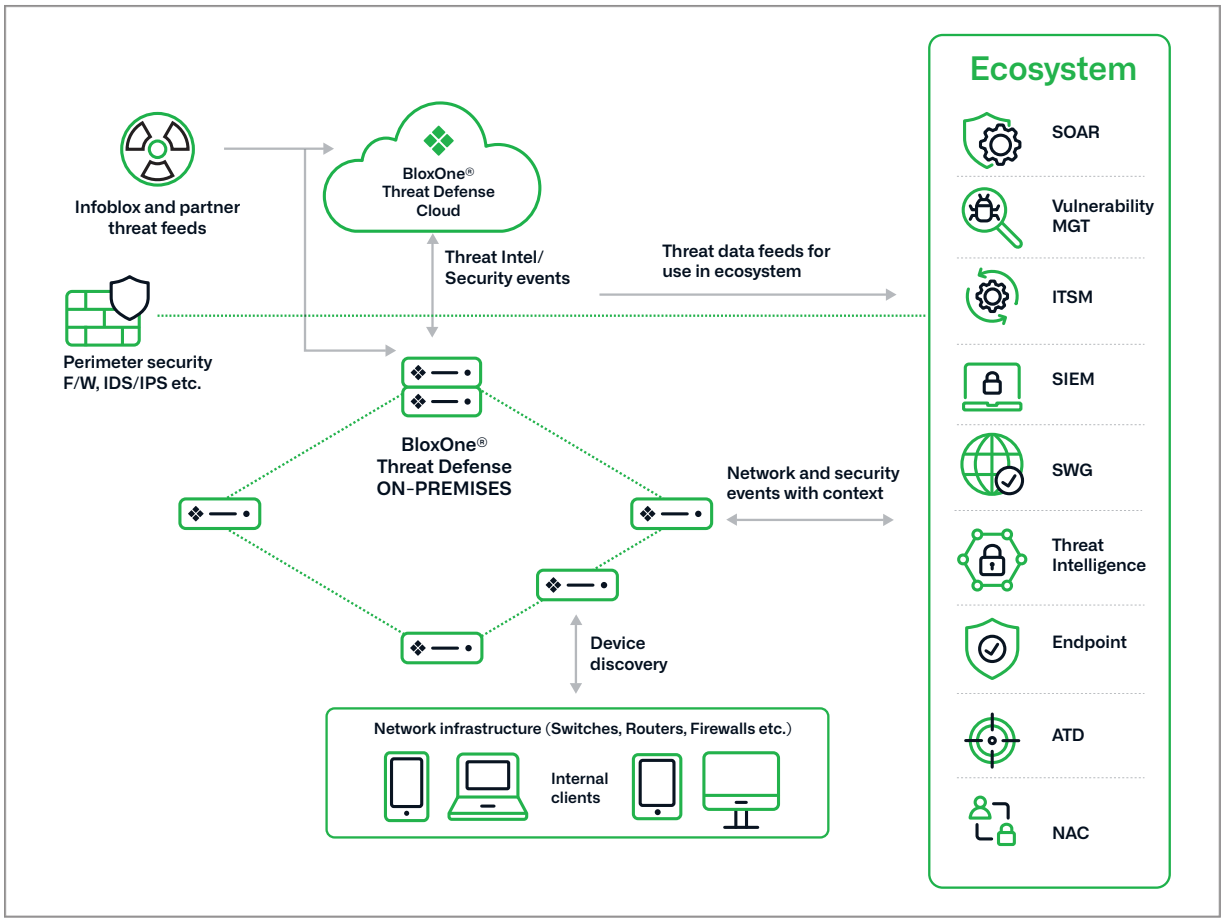

Figure 1: Infoblox strengthens and optimizes communications service provider networks

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

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

+1.408.986.4000
www.infoblox.com

Version: 20240521v1