Infrastructure Protection

SUMMARY

Business disruptions are costly and attacks on critical infrastructure, like those from distributed denial of service (DDoS) incidents, can bring a business to a halt. The Infrastructure Protection solution from Infoblox enables network teams to discover what’s on the network, what devices are being used, and what configurations those devices are running. The solution also automatically detects non-compliant and misconfigured devices, blocks DNS-based DDoS attacks and automatically shares information with the rest of the ecosystem for network-wide remediation. Our solution provides a solid foundation that enhances your entire security stack, empowering you to elevate infrastructure reliability to a whole new level.

DDoS Attacks Disrupt Business

To ensure high availability for applications and services, you must protect critical network infrastructure such as DNS, DHCP servers, switches, routers, storage, network devices and the DMZ. An essential asset in today’s connected enterprise, the Domain Name System (DNS) is also the number one service targeted by application-layer attacks (81 percent are DNS-related). It is also the number one protocol used in amplification/reflection attacks. Such attacks have resulted in significant financial damage to enterprises; the average cost per distributed denial of service (DDoS) attack is $2.5 million. With the digital transformation of every business, not having network access has gone from a minor inconvenience to one that impacts revenue and profits.

Networks today are often complex and diverse. They consist of physical, virtual and cloud components, distributed across geographies. It’s becoming increasingly difficult to identify noncompliant devices across this diverse infrastructure, which means your network could be hiding vulnerable elements. You may not even know when new devices join the network or when virtual machines (VMs) are being spun up. The bottom line is you can’t protect what you can’t see.

Key Elements of Our Infrastructure Protection Solution

Infoblox’s Infrastructure Protection solution addresses these challenges enabling security operations teams to:

- Discover what’s on the network, who’s on the network, what devices they are using, and what configurations those devices are running
- Automatically detect non-compliant and misconfigured devices
- Block DNS DDoS that bring critical services down
- Distribute the database of discovered devices throughout the security ecosystem for vulnerability scanning, enhanced compliance, and improved audit scoring
- Automate the IT service management ticketing process
- Get more value out of adjacent and complementary products with two-way data sharing

Discover What's on the Network
With Infoblox, you can readily see every network asset, IP address and switch port, VLAN, username and topology and consolidate your core network infrastructure into one comprehensive, authoritative database. You also can see attack points and patterns, identify new or unmanaged devices quickly and manage devices intelligently as their numbers grow. Infoblox can discover network devices from multiple vendors and across physical, virtual and cloud environments to give you a single view of your distributed network.

Automatically Detect Non-compliant Devices
A key element of the Infoblox solution for Infrastructure Protection is the ability to easily find non-compliant network devices, which could hide vulnerabilities. Our solution also identifies new devices as soon as they join the network. In addition, it remedies configuration issues and helps enforce compliance mandates and security policies.

Automatically Block DNS-based DDoS
Protecting your infrastructure must start with the core component of your network: DNS. Infoblox’s solution:

- Automatically detects and stops the widest range of DNS attacks, including reflection, DDoS, NXDOMAIN, amplification, TCP/UDP/ICMP floods, tunneling, reconnaissance, cache poisoning and protocol anomalies

- Maintains DNS integrity, detecting and providing alerts when DNS hijacking occurs
- Ensures application availability and enhanced reliability even under attack

Data Enrichment of the Ecosystem
Infoblox enriches your security infrastructure with up-to-date, curated threat intelligence. It includes threat data and attack event information with security information and event management (SIEM) and Network Access Control (NAC) tools via easy-to-consume APIs, syslog and SNMP. For example, you can notify your vulnerability assessment automatically when a virtual workload is spun up. Additionally, when a new device appears, you can scan for vulnerabilities before it is allowed on the network. This automated orchestration helps close the loop between networking teams and security operations to speed responses.

Threat Management with Centralized Reporting
Infoblox supplies detailed and consolidated reports that:

- Harness rich network data to gain actionable insights
- Monitor and analyze your network, devices and applications
- Provide details on attacks by severity, category and time

Figure 1: Infoblox solution for infrastructure protection
Conclusion

Ensuring app and service availability is a vital aspect of infrastructure protection. With the Infoblox solution, you gain visibility across your entire network, the intelligence necessary to identify vulnerabilities before they are exploited and the vital context your teams need to rapidly resolve threats when they occur. With our solution, you can protect your infrastructure against the widest range of DNS-based attacks. And with a single view of your network, you can achieve new levels of security and reliability.

Learn more about our solution at