SOLUTION NOTE

COST-EFFECTIVE IOT SECURITY AT SCALE

Enable security at massive scale for Internet of Things (IoT) networks, providing detection and prevention of malware and botnet attacks

SUMMARY

Providing security around Internet of Things (IoT) devices has always been complex, but upcoming 5G rollouts will further complicate IoT security.

As rollouts hit different geographies, 5G will be essential to the IoT, providing a faster network with a higher capacity to serve connectivity needs–opening the door for a sharp growth in IoT and Industrial IoT (IIoT) deployments.

Issues such as deprecated or insecure software components/libraries, inadequate or hardcoded passwords, and the inability to securely update the device make it extremely difficult for enterprises to monitor and secure the growing number of IoT devices. Surprisingly, most IoT communications are typically unmonitored since most IoT devices are programmed to communicate explicitly with IoT gateways or other edge servers where data is sent to be analyzed. While enterprises can leverage traditional methods like DPI or proxy servers to monitor IoT network traffic, the fact that they are forced to analyze all device traffic severely limits network scalability and performance.

Service providers can offer their enterprise customers a more robust and cost-effective way to manage device security at a massive scale for IoT networks. A DNS-based approach provides numerous benefits compared to traditional methods such as deep packet inspection. Infoblox Subscriber Services provides a cost-effective and scalable DNS-based approach that allows service providers to deliver value-added offerings, including empowering enterprises to secure and control IoT operations and devices at a granular level.

A GROWING PROBLEM

According to recent research from Strategy Analytics[1], the number of devices connected to the Internet reached 22 billion worldwide at the end of 2018. It is predicted that almost 40 billion IoT devices will be connected by 2025 and 50 billion by 2030. Though some industries may see a decline in device adoption, most sectors will see consistent growth. This includes the enterprise segment, which is already considered the leading sector for using IoT devices. IoT technologies are expected to profoundly reshape sectors such as manufacturing, transportation and retail. In addition, IoT devices have very long lifecycles and perform critical tasks, with many devices expected to remain in service for 10 years or more. Enterprises will need to consider how they can protect devices from cyberattacks now just now, but several years from now.

1 https://info.infoblox.com/resources-whitepapers-virtual-domain-name-system-secures-heart-service-provider-networks

ONLY AS STRONG AS THE WEAKEST LINK

Hackers are increasingly targeting weak IoT devices they can control and use to launch massive DDoS and ransomware attacks. IIoT shares the same security/compliance/visibility issues as IoT, but because of the mission-critical nature of many IIoT systems, problems in IIoT can hurt the enterprise financially in ways that other forms of IoT can't. Most IoT devices ship into the market with default passwords, which make them highly vulnerable to hackers if not reconfigured at deployment. In addition, most IoT devices are programmed to communicate explicitly with IoT gateways or other edge servers where data is sent to be analyzed. Therefore, the majority of IoT communications are typically unmonitored. Since many devices are not sophisticated enough to host their own security software, they rely on external network elements for security.

While more advanced devices might receive code updates, patches and configurations, many IoT manufacturers will deprecate IoT devices after about four-to-five years of service. As time passes, these devices no longer get security updates and become ripe for an attacker to find and take over. Further complicating matters, some of these IoT devices have independent antennae, which allows them to perform two-way communications over the mobile network without appearing on even the strictest systems tracking the LAN and WAN. The antennae enable the devices to bypass your network while still communicating externally with the IoT gateway. Even if the IoT device is passive and silent for an extended period, eventually, it will try and do something, which is when it will be detected by a continuous authentication system fine-tuned to watch for IoT devices.

5G IOT ISSUES

The number of IoT devices projected to connect to networks is growing exponentially. As enterprises evolve to include more remote locations and companies incorporate BYOD devices, known and "shadow" IoT devices can introduce vulnerabilities, expand the threat surface and increase the risk of systems compromise. As 5G rolls out and hits different geographies, it will enable far more communications with remote areas that today have severe communication challenges. Advancements in wireless technologies and the development of critical communication services will drive the growth of the global 5G IoT market. By extending bandwidth to these locations, a dramatic increase in the number of data centers is expected, with each needing protection from/for tiny IoT devices. Consider what it will mean for enterprises when today's 10,000 devices per square mile become hundreds of thousands—or more—for that same footprint. Embedded IoT devices have minimal computing and processing resources and do not run robust operating systems that support more sophisticated security solutions found on larger devices. Security will become an inherent requirement of the 5G infrastructure supporting IoT, considering the growth potential.

A BETTER APPROACH: NETWORK-BASED IOT PROTECTION

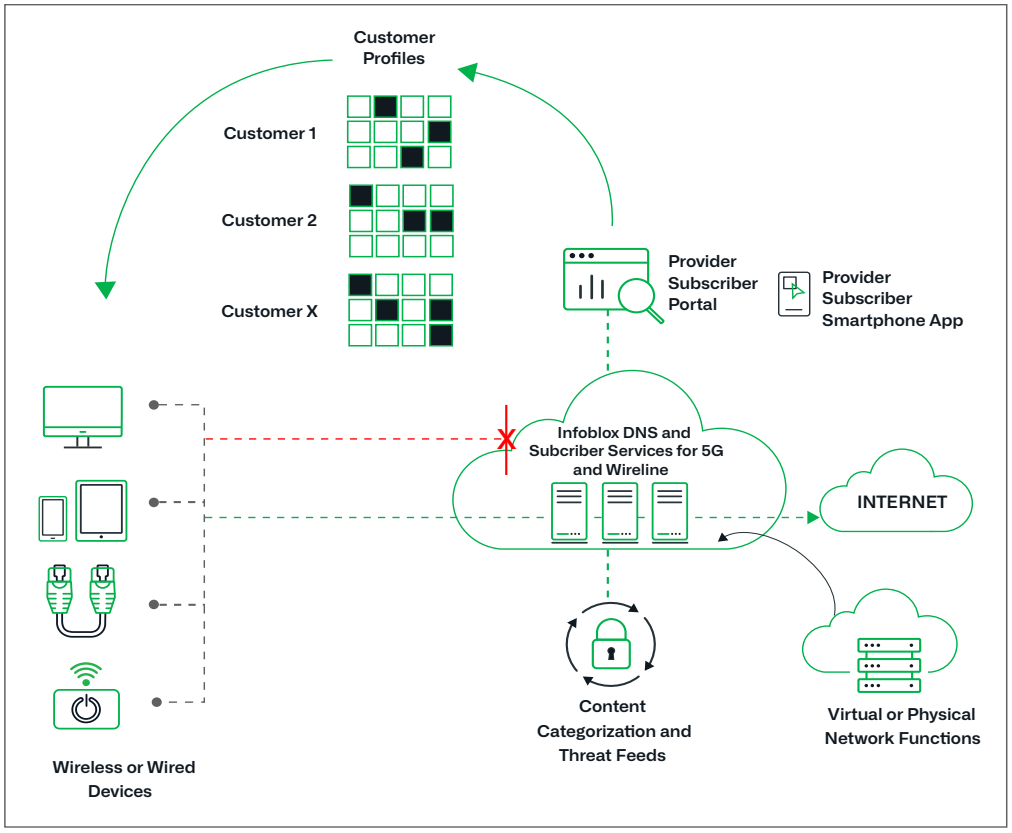
Many CSPs often overlook or fail to realize that DNS provides a more straightforward, more cost-efficient means for deploying network-based IoT device protection and other security services. DNS is part of the core DDI infrastructure that the network relies on every day. Shorthand for integrating DNS, DHCP, and IP address management into a unified service or solution, DDI services play a central role in all communications over an IP-based network. The elements of DDI can be harnessed in the service provider network infrastructure to bolster security, improve performance and increase subscriber revenue streams.

Infoblox Subscriber Services

Infoblox offers a complete end-to-end solution for subscriber services—the proxy, portal, DNS, policy managers, on-premises databases, logging management and threat intelligence. Infoblox Subscriber Services is a highly scalable DNS-based platform for delivering a comprehensive portfolio of value-added services, like enterprise content filtering and IoT protection, for mobile and fixed-wireline devices.

By monitoring DNS requests from every IP-enabled device, Infoblox Subscriber Services can quickly discover malicious activity and data exfiltration attempts via DNS, which helps a company comply with data protection regulations. The solution can monitor and halt the communication between botnet zombies and servers—in the process, stopping the flow of valuable information. Advanced and curated threat intelligence aggregated from several sources helps keep the protection up to date while avoiding conflicts and minimizing false positives. The solution leverages a component-based approach with open interfaces (APIs).

This approach enables CSPs to select the most efficient integration strategy for their current IT footprint and optimize value-added service offerings by integrating them via API communications with existing OSSs and BSSs. CSPs can leverage Infoblox's deep networking expertise and decades of investment to build out these new service offerings. Our product experts and engineers can help with critical features, including DDI management, device discovery, DNS cache acceleration, load balancing, automation and extensive DNS security capabilities. The Infoblox platform also requires minimal up-front investment and generates a predictable ROI by leveraging a flexible, pay-as-you-grow model.



Upcoming 5G rollouts will further complicate IoT security, but by monitoring DNS requests from every IP-enabled device, Infoblox Subscriber Services can quickly discover malicious activity and data exfiltration attempts.

IOT SECURITY AT SCALE

Cybersecurity is a universal need, and while enterprises are becoming increasingly aware of threats associated with cyber-attacks against IoT–that doesn't mean that they possess the ability to protect these devices. But there's good news. Surveys have shown that consumers are willing to pay for security services.[2] As a communications service provider, you are in the ideal position to build and bring to

2 https://stlpartners.com/research/the-changing-consumer-landscape-telco-strategies-for-success/

market scalable and cost-effective security offerings based on technology and equipment you already have installed in the data center. With Infoblox Subscriber Services, CSPs can help enterprises manage device security at a massive scale for IoT networks. DNS data is beneficial in discovering anomalous device behavior and prioritization. Since every IoT communication starts with a DNS request, the Infoblox solution empowers enterprises to secure and control IoT operations and devices cost-effectively. For example, if a thermostat only ever communicates to its specific application server at a designated URL, why is it suddenly resolving to a server on the other side of the world? DNS data can provide valuable network context to determine if the infected device is a high-value IoT asset that security teams must address immediately.

With Infoblox Subscriber Services, CSPs are able to offer their enterprise customers a cost-effective value-added IoT security solution that can:

- Classify and identify the numerous types of IoT devices that exist on the network and apply different classes of security based on the type of device.
- Quickly identify what devices are on the network and with whom they are communicating, and limit Internet access based on device purpose.
- Set policies that can effectively quarantine infected or malfunctioning devices based on their behavior.
- Scale to accommodate the projected massive growth of IoT and accommodate evolving technology changes–including encrypted DNS.

OPTIMIZED PERFORMANCE WITH SOLID SECURITY

With the Infoblox solution, CSPs can enable their enterprise customers to block outbound network requests to known malicious locations at the DNS layer–disrupting malicious communication from infected IoT devices to command-and-control servers. Effectively, with Infoblox, botnets can be stopped before they can form and launch attacks. CSPs can also offer their customers easy, self-service protection for shadow personal and IoT devices from cyber threats and enable compliance through control of IoT devices. In place of hardware-intensive solutions, the Infoblox DNS-based approach relies on the core networking infrastructure CSPs already have in place, with powerful DNS-caching capabilities that offer superior protection and control for IoT devices—all without sacrificing performance.

NEW REVENUE SOURCE EASIER ATTACH

With the user-friendly and white label subscriber portal, CSPs can present branded and differentiated opt-in offers on top of existing Internet services that are simple to attach, customize and use. With no software to download and install, enterprises can be provided complete control to configure and manage the solution that can monitor all of their IoT devices with little operator or subscriber intervention.

GREATER DEVICE REACH

Besides better scalability, the Infoblox DNS-based approach allows operators to distinguish between those devices subscribed and those not subscribed to the service, dramatically improving CSP revenue potential and differentiation against competitors. The Infoblox solution supports wireless IoT devices without wired connectivity with associated telephone numbers for complete protection across the IoT network.

PREDICTABLE ROI

With Infoblox, CSPs can leverage their existing DNS infrastructure and investments, turning DNS from a network utility into a revenue-generating service. In place of the hardware-intensive, stand-alone solutions found in DPI tools or proxies that analyze all network traffic, the Infoblox DNS-based approach reduces network impact because only the traffic from specific customers is analyzed. Infoblox also minimizes up-front investment with a scalable solution and a pay-as-you-grow licensing model, so providers only pay for the number of enterprise devices attached to the service.

MAINTAINS SPEED AND PERFORMANCE

Infoblox allows CSPs to leverage powerful DNS-caching capabilities to provide a much better network experience. Designed to handle the "perfect storm" of future 5G and edge-based applications that require ultra-low latency of 50 microseconds on average, Infoblox DNS cache acceleration enables DNS query rates of up to 5 million queries per second. Through centralized management, network administrators can quickly instantiate, implement and auto-scale network services, and manage those services more efficiently through a unified family of devices.

To learn more, visit www.infoblox.com/sp or contact your local Infoblox representative today.

LOWER ADMINISTRATIVE BURDEN

Infoblox provides a pre-built and user-friendly self-service portal accessible from anywhere. CSPs can customize the portal to match branding and color schemes and expose new features to enterprise subscribers as their offerings evolve. The service also provides a user-friendly white-label administrative portal. Customer agents can view subscriber account details for assistance and troubleshooting, allowing them to see reporting on service activity, filtering trends and security threat activity. Agents can also manage subscriber onboarding, handle global policy settings and policy category groups, and set subscriber/user password rules (e.g., such as length and expiration).

SUPPORTS ENCRYPTED DNS STANDARDS

Infoblox Encrypted DNS provides efficient encryption while delivering Infoblox best-in-class DNS and value-added subscriber services. With support for DoT and DoH, Infoblox Encrypted DNS delivers a unique approach to encrypting provider DNS traffic. Unlike methods that rely on load balancers or over-provisioning, Infoblox Encrypted DNS runs as a single service for all of your DNS needs. Infoblox Encrypted DNS enables Infoblox to encrypt last-mile DNS communications between their endpoints and DNS servers regardless of which protocol the endpoint supports. It supports this capability while also solving performance concerns associated with the additional overhead related to encrypted DNS communications. From the same service, we allow CSPs to accommodate encrypted DNS with microsecond latency when the connection is already established while all other DNS features are running.

CONCLUSION

Enterprises need solutions that help them communicate with and understand the functions of each device to stop botnet attacks before they can begin. CSPs are well-positioned to offer security at scale for the massive number of IoT devices expected to come online in the years ahead. With Infoblox, CSPs can use the DNS they already have in place to deliver cost-effective value-added services like IoT device protection on a massive scale. Infoblox Subscriber Services provides a scalable, resource-efficient, DNS-based way to protect the network and subscribers. It turns DNS into a powerful tool for building value-added IoT security services, blocking threats at the source while providing consistent performance. With its lightweight footprint, Infoblox Subscriber Services is easy to deploy and manage as an offering to existing wireless and fixed wireline internet services.

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: 20230918v1