infoblox

CASE STUDY

Infoblox Subscriber Services helps leading EMEA provider deliver safer internet experiences

SUMMARY

Infoblox Subscriber Services, combined with the threat intelligence and categorization feeds from BloxOne® Threat Defense, lets service providers offer a cost-effective yet comprehensive value-added service: It gives parents the tools they need to control where their kids can go online.

Infoblox provides network-level household parental control offerings in an easy-to-use self-service solution that requires n o software downloads or complicated management. Parents gain a consumer-friendly "set it and forget it" solution that allows them to personalize Internet access settings across all devices for each household member.

THE CUSTOMER

Headquartered in EMEA and operating in 22 countries, providing services across Europe, Africa, Asia and Oceania, this multinational Tier-1 telecommunications service provider is one of the largest fixed and mobile network operators in Europe. Beyond offering voice, broadband and digital television services to millions of subscribers, the company also strives to innovate and leverage new technologies that empower consumers and businesses to stay safe, connected and thriving. It recognized the challenges its subscribers faced, not only from Internet-based threats but also the need to control online time for children. In 2015 it offered its mobile subscribers a comprehensive yet simple-to-deploy value-added security service.

> *"Users typically pick convenience over security, especially with technology. By leveraging Infoblox with our existing network infrastructure, we can cost-effectively deliver a scalable value-added offering that can simultaneously span our mobile and wireline subscriber base to seamlessly combine proactive protection and control, providing a fast and safe online experience for all"*
>
> **Technology and Products Director at the company**

THE CHALLENGE

Enable safe internet across millions of devices—mobile and fixed

While the service provider's security service was popular with its mobile subscribers, the company recognized that it accommodated only a fraction of customer devices. Today's connected households face an explosion of broadband-connected devices, too, representing a large and growing attack surface requiring comprehensive protection. Beyond the expanding numbers of scams and malware threats, parents want control over where and when their children can go online—protecting children from themselves by limiting their ability to make bad choices across their many devices used inside and outside the home. The provider recognized that by expanding its offering into a converged service that accommodated both its mobile and fixed broadband subscribers, it could offer a compelling service that differentiated it in the market and opened new revenue streams. However, the provider also realized that it needed to expand its architecture to accommodate millions of additional subscriber devices. The service still needed to be simple to use and require no software downloads. Yet, at the same time, it needed to support traditional and untraditional subscriber devices (including those without conventional operating systems like video game consoles and smart TVs) across its broadband and mobile networks.

THE SITUATION

The need for massive yet cost-effective scale

The architecture supporting the original service was built using a deep packet inspection (DPI) approach to deliver end-user security and parental control services. With DPI and proxy-based solutions, the concept is relatively simple in principle. All user traffic flows through the DPI or proxy infrastructure, and predefined filtering and security policies are applied. However, when that traffic grows, things can get tricky. As the number of subscribers increases and resources move closer to the end users, all traffic flows through DPI. This approach creates scalability challenges that sometimes require massive investments in incremental hardware.

DPI approaches can also create extensive performance impacts because all traffic is analyzed from paying and non-paying subscribers. The strain that future 5G deployments will put on service providers will be massive. Enhanced mobile broadband will increase the growth of Internet of Things (IoT) devices, which will drive new applications that increase bandwidth consumption. Therefore, the simple "sniff all traffic" approach cannot keep up without enormous DPI and proxy capacity investments.

Another challenge that legacy DPI or proxy approaches face is their inability to identify individual users behind gateways or routers, resulting in "blind spots" with gaps in specific subscriber user details for those using devices behind home gateways and routers. Other solutions may require users to download, install and manage complex software agents to use the service, leaving devices such as video games, smart TVs and IoT appliances apart from a comprehensive solution.

Customer: *Leading European telecommunications provider*
Industry: *Telecommunications*

INITIATIVES:

- Provide an easy-to-use, safe Internet solution to millions of households
- Expand existing wireless-only service into a comprehensive wireless and broadband solution
- Support massive scale while maintaining optimal performance

OUTCOMES:

- Network-level protection for children in and outside the home across all devices
- No software downloads or complicated management
- Increased flexibility and scale
- Increased revenue and brand differentiation

SOLUTIONS:

- Infoblox Subscriber Services
- Infoblox Subscriber Parental Control
- BloxOne Threat Defense

DNS—An Overlooked Source of Subscriber Revenue

In contrast to stand-alone solutions such as DPI tools or proxies for subscriber services, a DNS-based approach leverages existing core networking infrastructure to provide extended visibility, content control and security to end users. DNS is a part of the foundational DDI infrastructure services that all service providers use in delivering Internet access. DDI integrates 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 power of DNS can be harnessed in service provider network infrastructure to bolster security, improve performance and increase subscriber revenue.

Infoblox's relationship with this particular carrier, a long-standing Infoblox customer, began with DNS Cache Acceleration for ultra-fast network response and Advanced Data Protection for protection against DNS attack floods and other threats designed to take down networks. Still, the operator had realized there were more straightforward, more cost-efficient means to deploy value-added security services. For example, DNS-based deployments can scale with the number of subscribers or clients instead of throughput, enabling pay-as-you-grow business models. A DNS-based approach not only offers better scalability, but its segmentation features also can distinguish between subscribers and non-subscribers, freeing providers to offer convergent subscriber services for both fixed and mobile access. These capabilities dramatically reduce the additional up-front investment needed to provide value-added offers by eliminating costly, stand-alone tools while improving revenue potential.

THE SOLUTION

Infoblox subscriber services—leverage existing network resources

Working with the team at Infoblox, the carrier explored ways to use existing DNS capabilities to expand its value-added security services offering on top of its fixed broadband subscriber base with a fully converged wireless and broadband solution. The operator chose Infoblox, its long-term DNS provider, for its unmatched expertise delivering DDI-based foundational security. Infoblox Subscriber Parental Control and BloxOne Threat Defense integrate on top of rather than replace existing data center and security infrastructure.

Infoblox's network-level parental controls require no software downloads or complicated management that differs by device type while allowing for personalized Internet access and screen time settings for each household member. The service works behind the scenes at the infrastructure level to seamlessly protect mobile and fixed access subscribers from cyberattacks, such as phishing, online viruses and malicious websites, while providing parental controls to enforce screen time limits and protect children from online predators and other Internet dangers. Infoblox simplifies threat mitigation at the infrastructure level, maintaining and optimizing the service provider's growing network even as the operator expands its 5G and IoT offerings.

Key components of the Infoblox solution include:

- **BloxOne Threat Defense:** Maximizes brand protection by securing existing networks and subscriber imperatives, such as 5G, IoT the network edge and the cloud. It works with a service provider's existing defenses to automatically stop malware from spreading inside a network—detecting malware at the DNS layer, preventing devices from connecting with malicious destinations, isolating compromised devices and then triggering their remediation.
- **Infoblox Subscriber Services:** Supplies a unique DNS-based approach that empowers service providers to differentiate themselves and quickly open new revenue streams with intelligent, customizable, value-added security services. These new services can minimize the initial investment to launch value-added offers for both fixed and mobile subscribers.
- **Infoblox Subscriber Parental Control:** A subset of Infoblox Subscriber Services, it provides robust content controls. Parents can gain a central view of complete household Internet usage. They can establish separate user profiles for each household member and apply policies based on age or device, leveraging predefined content categories to dial in the desired level of protection.

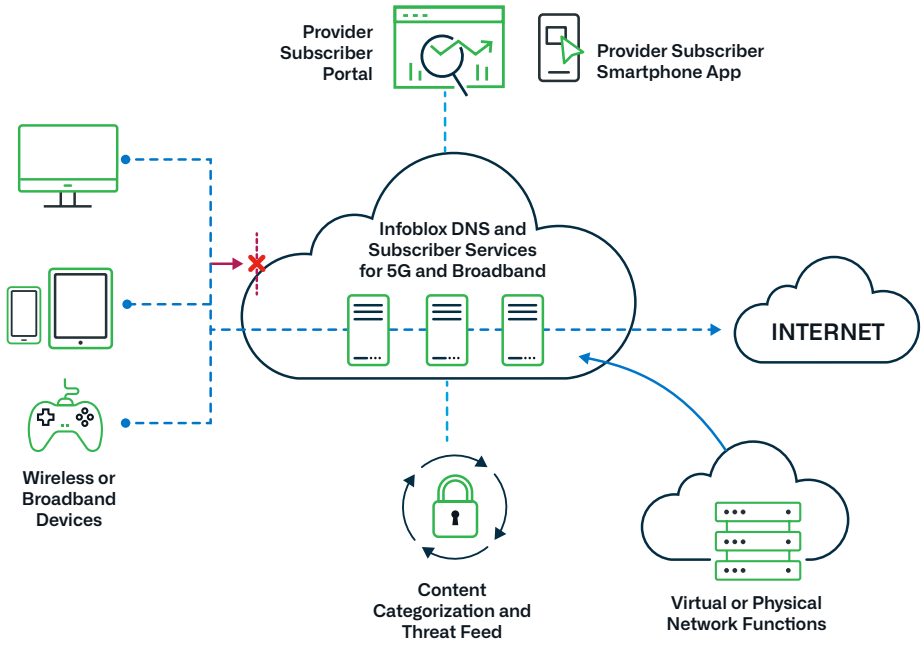

Figure 1: Components of Infoblox Subscriber Services

The combined solution works at the network level so parents can manage Internet access both inside and outside the home across all devices, including computers, tablets, mobile phones—and even game consoles (Figure 1.) If parents suspect their child is exposed to harmful content, they can instantly pause Internet access to review the situation.

Plus, it's easy to extend access past bedtime for holidays and other special occasions. Besides controlling content, parents can also establish time constraints. Is bedtime 9 p.m. on school nights? Does someone need extra study time? The Infoblox solution furnishes a simple way to manage screen time to control when children can use the Internet and shut down access on an established schedule.

THE RESULT

Helping guarantee a safer internet

While the provider's original mobile security service launched over five years in nine European markets, the provider has since released the new converged solution in three countries, offering parents the security and parental control tools to manage their digital household. Using Infoblox Subscriber Services, the provider has a cost-efficient yet scalable solution that protects families while preserving optimal network performance. Thanks to Infoblox, this provider is expanding a converged mobile and broadband solution into additional European countries. Parents gain peace of mind, knowing they can protect their children from the perils of online access—by controlling screen time and dramatically reducing the likelihood that children will be exposed to inappropriate images or videos and online threats.

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

+1.408.986.4000
www.infoblox.com