

CASE STUDY

# Schneider Electric Simplifies Core Networking, Takes a Cloud-Based Approach to Cybersecurity with Infoblox

**Customer:** Schneider Electric

**Industry:** Energy, Electronic Manufacturing

**Initiatives:**

- Ensure DNS reliability and integrity
- Consolidate core network services onto a single console
- Improve cybersecurity posture
- Boost cybersecurity score

**Outcomes:**

- Simplified and centralized DDI across 1,000 branch locations
- Elevated cybersecurity posture and score
- Enhanced endpoint visibility, DNS reliability and integrity

**Solutions:**

- BloxOne® Threat Defense Business Cloud
- Infoblox Core DDI
- Infoblox Grid
- Infoblox NIOS Platform



## The Customer

An iconic European company with deep roots in the French economy and society, Schneider Electric develops innovative, connected technologies and solutions for safety, reliability, efficiency and sustainability. Founded in 1836, Schneider Electric has a storied history, and today is highly regarded for its advancements in software, critical power, digital transformation, the IoT and smart grid applications. Headquartered in Paris, the company employs more than 137,000 people and relies on a massive, global network that includes hundreds of branch locations.

## The Challenge—Simplifying IT and Elevating Cybersecurity Posture

Schneider Electric began working with Infoblox a decade ago, when the IT team implemented Infoblox’s DDI solution for its U.S. branch locations to manage DNS and other core network services. Since then, the Schneider Electric team has looked to standardize IT infrastructure across its hundreds of branch offices worldwide.

The company initially relied on other solutions, such as BIND and Microsoft DNS, to manage these services. As the company grew, however, so did the complexity of this network infrastructure with its mix of legacy and inherited systems. For the Schneider Electric IT team, it became clear that the company needed to consolidate its core network services onto a single management platform and modernize its network architecture from the foundation up.



The Schneider Electric IT team also looked to elevate its cybersecurity posture by improving the company's overall cybersecurity risk score. Security scores are vital to winning contracts and attracting investors. In addition, the company established a goal of improving the ways it safeguards its people, facilities, devices and intellectual property.

## Optimizing DNS Availability and Integrity

By 2016, company leadership had deemed DNS critical infrastructure and decided to consolidate all DNS to Infoblox DDI. Now that the Schneider Electric team has expanded its Infoblox implementation across all of its global branch locations, the IT team can manage its core networking services much more efficiently and with greater control and automation. They can also minimize network downtime and maintain network availability and reliability around the clock.

Yohann Royer, network security service line manager at Schneider Electric, explains that "Maintaining the availability and integrity of DNS is essential to keeping our large network up and running at all times. DNS is a critical service because if we lose DNS, nothing will work, and we will lose access to critical digital resources. That's why we continue to rely on Infoblox for the past decade and counting."

## Taking a Cloud-Based Approach to Cybersecurity

Migrating to a pure cloud cybersecurity solution was also top priority for Schneider Electric. The IT team urgently needed a scalable, automated and cloud-based network security solution that would maximize the company's cybersecurity risk score while protecting users anywhere without needing to deploy or manage additional architecture. The goal was to shift from threat recovery to threat detection to protect its brand and reputation, as well as its valued users and data wherever they are.

Infoblox's BloxOne Threat Defense Business Cloud enabled the Schneider Electric team to protect users anywhere on the network whether they are signed into their VPNs or not. The cloud solution applies advanced threat intelligence, behavioral analytics and machine learning to detect and pinpoint malicious behavior on the network. It then intercepts that traffic, automatically preventing network devices from

connecting to command-and-control servers and other cyberthreats, while allowing legitimate DNS traffic to flow freely. With BloxOne Threat Defense Cloud, security teams at Schneider Electric are able to proactively screen for and stop threats at the network edge, significantly improving the company's security posture—and security scores. Because the cloud solution is easy to deploy on a subscription model, it also gives the Schneider Electric team the flexibility to scale for future growth.

According to Royer, who is responsible for managing and protecting the organization's users, devices and its rapidly evolving network, "Infoblox's cloud cybersecurity solution gives our team complete visibility into all users and endpoints wherever they are on the network through a single pane of glass. As a result, we have successfully improved our BitSight cybersecurity risk score so that it's back in the green where it needed to be."

## A Long-Time Partnership and Superior Customer Experience

Over the years, Royer and his team conducted thorough research on Infoblox and competing vendors as objectives evolved and new solutions needed to be deployed. At each step, Schneider Electric concluded that it would have a superior customer experience and could better meet its needs with Infoblox. "We have a true partnership and an exceptional customer experience working with the Infoblox team," says Royer. "Infoblox executives visited us onsite and in person to build trust and to share their vision with us. On a technical level, what made the difference was that Infoblox was able to process our traffic for 24 hours. The high quality and stability of Infoblox's threat feeds and reports—as well as visibility and low false positive rate—met our needs more so than the competition."

---

### For More Information

Learn more about how you can proactively detect malware and protect your users and data via DNS. Speak with an [Infoblox representative](#) or [start your free trial](#) of our BloxOne Threat Defense technology today.



Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. Infoblox has over 8,000 customers, including 350 of the Fortune 500, and is recognized as the industry leader in the DDI networking market.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054  
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | [info@infoblox.com](mailto:info@infoblox.com) | [www.infoblox.com](http://www.infoblox.com)

© 2020 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).

