



CASE STUDY | AMERICAN AUTOMOTIVE & TECHNOLOGY COMPANY

# Driving Innovation Together: Empowering an Automotive Company to Launch Disruptive Products

## Equipping a Global Market-Leader with secure and reliable cloud-native Infrastructure DNS

### The challenge

PowerDNS successfully supports a globally operating, market-leading automotive manufacturer and producer of advanced technology products headquartered in the USA. The company develops, manufactures, and assembles vehicles and related products at multiple production sites worldwide. It is renowned for its disruptive innovations in the automotive industry, its use of cutting-edge software for autonomous driving, and its ambitious sustainability goals.

The automotive company sought a new solution for its internal DNS infrastructure across multiple production sites. The DNS system connects employees as well as the various applications used in vehicle manufacturing and other production processes. The previous DNS solution was a fragmented mix of mostly closed-source and a few open-source applications. The primary system was a proprietary black box, preventing the company from having control over or visibility into its resolution processes. Additionally, the legacy solution was costly and inefficient, making daily operations, expansions, and modifications to the DNS infrastructure complex and resource-intensive for the IT team.

Security was a top priority for the company. Ensuring the integrity of the underlying code was a major concern, leading to the decision to adopt an open-source solution. With access to the source code, the company could rigorously test the DNS system rather than relying solely on vendor assurances. Furthermore, an open-source approach was expected to optimize costs associated with installation, migration, and ongoing maintenance.

The internal DNS infrastructure plays a critical role in the company's operations. Any failure or malfunction can disrupt production, potentially resulting in substantial revenue losses. Therefore, the new solution needed to be highly reliable, high-performing, and secure. It had to meet stringent requirements while also defending against external threats. This was to be achieved through a securely coded foundation with extensive, continuous security testing. Additionally, the system had to be capable of mitigating threats such as DNS tunneling and Distributed Denial of Service (DDoS) attacks effectively.

# A Commercial Partnership for Worldwide Operation **Based On a Shared Passion for Open-Source Solutions**

## The solution

Based on these security requirements and a strong preference for open-source code, the automotive company began searching for potential providers and DNS solutions. The emphasis on an open-source-based DNS system significantly narrowed the available options. Among the possible alternatives, PowerDNS was identified as a strong candidate and underwent a thorough evaluation.

As part of this evaluation, the automotive company initially downloaded, deployed, and extensively tested the PowerDNS community versions. Compared to other open-source solutions, PowerDNS products stood out due to their superior performance, richer feature set, and higher reliability. Following this, the company assessed the organization behind the PowerDNS community versions. PowerDNS, with Open-Xchange as its parent company, instilled confidence in the automotive company, convincing them that we could be a reliable, long-term partner. Only after this multi-layered evaluation did the global automotive company reach out to discuss additional commercial solutions and the required 24/7 support.

After gathering the company's specific requirements, the PowerDNS team collaborated with them to design a tailored solution with a customized architecture. At the core of the new PowerDNS Infrastructure DNS is the PowerDNS Authoritative Server, which serves all internal zones of the automotive company, ensuring seamless connectivity for employees and large-scale manufacturing. The ZoneControl add-on allows the organization to create zones as needed, secured through Role-Based Access Control (RBAC). Additionally, custom Lua scripts and DNSSEC provide an extra layer of security.

The PowerDNS Recursor supports the company with internal domain name lookups, again incorporating additional security layers. For instance, DNS Response Policy Zones (RPZ) block malicious content and threats from compromised applications, redirecting traffic to safe domains. Moreover, IPv4 addresses are translated into IPv6 using DNS64.

In front of both the authoritative and recursive components, DNSdist was implemented as a caching proxy and load balancer. It distributes traffic across different servers based on health and geographical checks. Lua scripts are also utilized in DNSdist, particularly for mitigating DDoS attacks. Additionally, the company's internal threat feed was integrated into DNSdist to ensure precise handling of domain whitelisting and blacklisting. Another key security measure introduced by the automotive company was encrypting DNS traffic using DNSdist. To accommodate the scale of the DNS installation and

the additional load introduced by DNSSEC, DNSdist enables the company to leverage Extended DNS (EDNS).

The entire solution was integrated with Prometheus and Grafana for data collection and analysis. This allows the company to generate reports and visualizations on demand while continuously monitoring the system through real-time dashboards.

A final critical requirement was high availability and disaster recovery. By implementing a failover architecture and the network addressing and routing method Anycast, traffic can be seamlessly rerouted at the network level to a backup site if a server at one location fails.

This setup was deployed across 20 data centers in North America, Europe, and APAC, each equipped with multiple edge servers. PowerDNS Cloud Control was used for deployment, enabling a rapid rollout of the new setup across the data centers. This cloud-native approach proved to be highly cost-effective while allowing the customer's DNS team to operate remotely and automate processes efficiently. Additionally, it ensures future scalability with elastic scaling capabilities as needed. As a result, the automotive company is well-equipped to handle its current average of 1.2 million queries per second (QPS) per data center while maintaining the flexibility to scale further.

Beyond our robust commercial products, the open-source foundation of our solutions and our commitment to keeping the core of PowerDNS products open were key factors in the company's decision to partner with us. Furthermore, our secure coding practices, ongoing security audits of our products, and continuous evaluations of the PowerDNS organization played a crucial role in their selection process.

The expertise and dedication of the PowerDNS team further solidified the partnership. Our global presence allowed us to provide local contacts for different regions. The automotive company valued our deep technical knowledge, which extends beyond our own products, ensuring a smooth and confident transition during this complex migration project.

Lastly, our responsiveness to innovation was highly appreciated. Since the customer is known for its disruptive innovations and adoption of cutting-edge technology, they sought a partner who shares their forward-thinking mindset—one that is open to new developments and willing to innovate alongside them. PowerDNS is honored to be recognized by this prestigious automotive company as a highly innovative partner and looks forward to supporting many more of their groundbreaking advancements in the future.

**Contact PowerDNS**  
for more information

**Stay up to date**  
with the PowerDNS newsletter