SECURE64®

CASE STUDY

US Government Agency Builds Secure DNS Network with Secure64

ORANIZATION
US Government Agency

BUSINESS CHALLENGES
- Build a secure DNS network
- Build a network with failover to insure 100% availability
- Improve resilience to DDoS attacks
- Reduce need to patch
- Implement DNSSEC across agency domains
- Prevent user devices from introducing malware into the network

SOLUTION
- SECURE64® DNS AUTHORITY™
- SECURE64® DNS CACHE™
- SECURE64® DNS SIGNER™
- SECURE64® DNS MANAGER™
- SECURE64® DNS GUARD™

BENEFITS
- Maintained 100% customer availability
- Prevented intrusions into the DNS
- Reduced patching frequency & cost
- Fulfilled government mandate
- Prevented user devices from introducing malware into the network
- Prevented devices in the network from getting infected

"From our first experience with Secure64 and DNS Signer, we knew we had found the right partner for The Agency... After years of running with Secure64, I really couldn't feel more secure about our DNS – a rare feeling these days."

– IT Specialist, The Agency

The US Government Agency (The Agency) is a bureau within a cabinet level department of the federal government of the United States. It serves the 325 million plus citizens of the United States and uses a geographically diverse network.

Driven by Mandate
The Agency initially contacted Secure64 because it was subject to a mandate from the US Office of Management and Budget (OMB) that required all federal government agencies to deploy a standard for securing their DNS with DNSSEC (Domain Name System Security Extensions). Deploying DNSSEC, however, is a complex operation and the cost of making mistakes is high. The Agency purchased and deployed Secure64 DNS Signer, which securely and simply automated the DNSSEC signing, making The Agency compliant with the mandate, and securing their domains against fraudulent activity.

The Need for a Secure & Always Available Network
The Agency then turned to Secure64 because they were looking to replace their DNS network with one that was not based on BIND, easy to implement and highly secure. The Agency required an always available network to serve a large client base, and needed increased security and decreased patching then what they had been enduring. Unlike most other commercial DNS products, Secure64 is not based on BIND and is immune to any BIND-specific vulnerability, greatly reducing the need to drop and patch. Even more compelling to The Agency was the patented micro OS and built-in DDoS capabilities in Secure64 DNS Cache and DNS Authority, which offered a level of security that no other DNS vendor could match.

The Agency then purchased and deployed Secure64 DNS Authority and DNS Cache across their geographically diverse network, where the DNS servers have been running non-stop for years.

A Single Pane of Glass
More recently, The Agency procured budget to add Secure64 DNS Manager to manage all the DNS servers in their network. Secure64.

CASE STUDY

US Government Agency Builds Secure DNS Network with Secure64

DNS Manager provides a single pane of glass to manage servers across geographic regions, enabling administrators to roll out new software, revise configurations, monitor network load and set alerts in real time, create reports, and more from a single central point. DNS Manager is also a prerequisite to deploying the Secure64 security service from Secure64, DNS Guard.

Protection against BYOD (Bring Your Own Device) and IoT (Internet of Things)

The Agency was grappling with employees bringing in their own devices and plugging them into the network, putting it at risk. Because of this, The Agency added Secure64 DNS Guard, a service that uses the DNS to protect users and devices from phishing attacks and malware infections, while it neutralizes infected devices so they cannot cause harm to the network. DNS Guard provides protection for and against all devices on the network without requiring the device to be touched in any fashion, even those devices that have little to no security on them at all, such as IoT. It provides real-time security information to stop malicious activity on the network across all devices.

The Agency purchased and deployed DNS Guard to protect the network against infected user devices and to give them visibility into which devices are infected, allowing further preventative measures to be taken.

The End Result

The Agency has now built an always available, secure DNS network that is capable of protecting all devices in the network, including BYOD and IoT, from malware, and protecting the network from attacks caused by infected devices brought into the network.

"From our first experience with Secure64 and DNS Signer, we knew we had found the right partner for The Agency," said The Agency's IT Specialist, "The company and all of their products were built to be secure because security was of primary importance to them. This resonated strongly with us, because security is critical to us, as is availability. After years of running with Secure64, I really couldn't feel more secure about our DNS – a rare feeling these days."

Learn more about Secure64 DNS Solutions at **www.secure64.com**

SECURE64®

303.242.5890 | **www.secure64.com**