A Global U.S. Defense Agency

Infoblox
CONTROL YOUR NETWORK

Profile

The Customer:
This large federal agency provides forces and resources for planning and conducting cyberspace operations and defending its own networks

The Challenge:
Protect the network from millions of connections per day to malicious domains

The Solution:
- Infoblox DNS Firewall
- 36 Infoblox 4010 appliances

The Results:
- Helps to pinpoint infected devices
- Prevents communications to malicious domains
- Adds accurate, current malware data to blacklists

DNS Firewall Protects a Global U.S. Defense Network from Millions of Malicious Queries Every Day.

The Customer

With hundreds of thousands of uniformed and non-uniformed employees around the world, this U.S. defense organization depends on its network, which links hundreds of bases globally, to be constantly secure and available.

The Challenge

The organization was experiencing millions of events per day. Some were known to be malicious. Others were unexplained, but were known to originate from malicious IP spaces or to be destined for countries known for nefarious activity. With this volume of bad traffic, the agency was struggling to maintain blacklists.

An audit in 2011 revealed only the most basic ability to identify the sources of communications to malicious destinations. They could be identified at the base level, but every base has thousands of devices. The agency needed to pinpoint the IP addresses of infected devices. In addition, mandates from regulatory agencies required the ability to inject blacklisting feeds from other agencies into the customer's own list.

The Infoblox Solution

The agency already had an extensive Infoblox installation with hundreds of Infoblox appliances and high-availability Infoblox Grids™ at two central locations. Adding DNS security to this vast network was a simple matter of installing 36 Infoblox 4010 appliances running Infoblox DNS Firewall at all the customer's regional boundaries and Grid Masters. DNS Firewall has its own feed for current malware data, and it prevents DNS-exploiting malware from communicating with botnets or exfiltrating sensitive information.

The Results

Now outbound communications with command-and-control servers and botnets can be disrupted and redirected to internal servers for analysis. Malware data feeds from other agencies can be incorporated into the DNS Firewall feed for blocking. And already-infected devices can be identified and quarantined or remediated.

About Infoblox

Infoblox (NYSE:BLOX), headquartered in Santa Clara, California, delivers network control solutions, the fundamental technology that connects end users, devices, and networks. These solutions enable more than 7,000 enterprises and service providers around the world to transform, secure, and scale complex networks. Infoblox (www.infoblox.com) helps take the burden of complex network control out of human hands, reduce costs, and increase security, accuracy, and uptime.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com