Leading Energy Producer Takes Cybersecurity and Reliability to New Heights with Infoblox

Facts & Figures

Industry: Oil and Gas

Location: Middle East

The Solution

Infoblox Next Level Networking, including:

- ActiveTrust® Suite
- Software Advanced DNS Protection (ADP)
- Threat Insight Subscription License
- DNS Traffic Control
- Reporting & Analytics Subscription License

The Customer

Located in the Middle East, this company is one of the world's leading energy providers. It operates across the entire hydrocarbon value chain through an assembly of fully integrated businesses, with interests that range from exploration, production, storage, refining and distribution, to the development of a wide-range of petrochemical products. The company generates the energy that is driving its region's development. The company also develops a range of innovative solutions that enhance daily life.

It recently launched an initiative to deliver three strategic imperatives—a more profitable upstream business, a more valuable downstream business and a more sustainable and economic gas supply. To meet these and other goals, the company continually implements innovative technologies that enable it to enhance recovery and ensure improved production efficiency.

The Challenge

The global energy producer sought to expand production of oil and gas and diversify its operations while improving its processes, oversight, and cost controls. It wanted a cybersecurity solution that would provide enough scalability to ensure that all web traffic would be inspected at all layers including DNS, before being sent out to the internet.

However, its enterprise network had become an impediment to those ambitions. Network management and cybersecurity operations were disconnected, error-prone, and inefficient. As a result, it lacked the management ease to control its existing infrastructure and launch new initiatives. Nor could it adequately protect its data and infrastructure from escalating cyberthreats.

Extending Network Visibility and Protection across all Subsidiaries

As the company grew to accommodate new devices, deploy new applications and improve network uptime, it wanted to manage network tasks faster and more efficiently, secure devices and applications more effectively and maintain the high availability and business continuity its global operations demanded. With Next Level Security from Infoblox, it was able to achieve all of those goals, and many more, centrally and automatically. Infoblox solutions enabled networking teams and security operations teams to enhance visibility across the company's subsidiary network deployments while extending protection to devices inside and outside the network perimeter.

Mitigating Malware and APTs via DNS

DNS is a key pathway for malware and Advanced Persistent Threats (APTs). Through Infoblox solutions, including Advanced DNS Protection (Software ADP) ActiveTrust, ActiveTrust Cloud, and Reporting & Analytics, the company obtained key cybersecurity functionality.

The energy provider can now detect and mitigate malware attacks such as zero-day exploits and APTs while blocking command and control (C&C) communications at the DNS choke point.

Infoblox provided the capability to detect and automatically block such attempts. In addition, the solution applies signature, reputation, and advanced behavioral analytics that leverage machine learning to detect not just known DNS tunnels but also zero-day techniques that often unfold over longer periods of time.

Achieving High Availability and Resiliency

With Infoblox, the energy company is now able to raise its network visibility and reliability to a new level. The Infoblox implementation with its patented GRID technology provided redundancy and eliminated single points of failure, enabling the company to achieve the high levels of availability to serve its subsidiaries and global customers without disruption. In addition, through Infoblox's advanced DNS protection the company now has the resiliency to maintain service availability even during ongoing security events, such as DDoS attacks.

Containing Threats while Improving Operational Efficiency

Through its Infoblox solutions, the company can contain security threats faster and more efficiently using consolidated, curated, high quality threat intelligence. In addition, tools such as Infoblox Dossier give security teams the ability to investigate and prioritize threats more quickly. Moreover, the orchestration capabilities in Infoblox improved efficiency of its security operations.

Integrating Security Response across the Ecosystem

In choosing Infoblox, the energy provider was able to detect and remediate cybersecurity incidents more rapidly and completely by enabling its existing security infrastructure to interact with its extended third-party tools and systems. The solution provided the capability to automatically share network events and indicators of compromise in real time with existing security tools such as next-generation endpoint protection (NGEP), next-generation firewalls (NGFW), network access control (NAC), vulnerability scanners, and security information and event management (SIEM) solutions.