

## Competitive Battle Card – Nokia VitalQIP – February 2016

### Why Customers Need to Care

DNS, DHCP, and IPAM (DDI) network services are becoming increasingly critical:

- **Scalability & Performance:** As enterprises grow and implement strategic initiatives such as IoT and Big Data instrumentation, most DDI approaches simply fail. Further, a poorly implemented DNS infrastructure causes performance problems that are difficult to detect.
- **Automation:** DDI network service integration is crucial to SDN, VM mobility, and other network-dependent automation processes.
- **Security:** DDI Network Services, particularly DNS, are actively being exploited by hackers – both criminal and sponsored by governments – to penetrate enterprises and to steal sensitive information. Further, Distributed Denial of Service (DDoS) attacks are directed at the DNS layer and so protection must also be provided within the layer at a minimum.

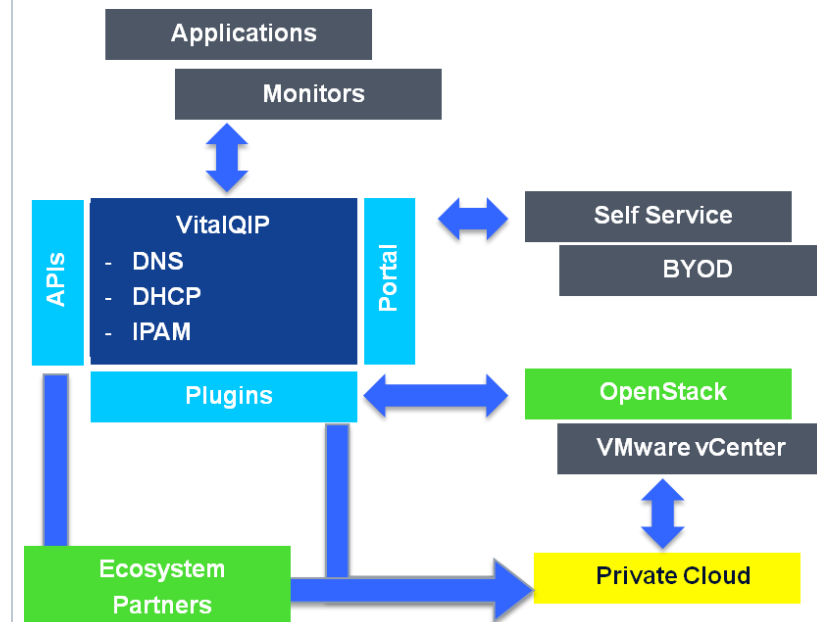
### Best Response to Market Needs – Nokia VitalQIP

DDI Network Services approach proven at Global 2000 Enterprises with high performance and security needs (e.g. Financial), Government, and Service Providers worldwide.

### Unique Functionality

- **Integrated DNS, DHCP, and IPAM Software Platform:** Unique integrated approach versus “black-box” appliances such as Infoblox and Blue Cat.
- **Interoperability Across DNS & DHCP appliances and modules:** Unique in managing Microsoft DDI for example versus requiring consolidation and replacement of other DDIs as does Infoblox.
- **Scalability and Performance:** Highest in the industry, exceeding that of Infoblox as an example.
- **Open Approach:** Enables customers to fix problems by providing source docs and assisting with debugging. Black Boxes do not provide this capability and typically do not even provide root access to the appliance.
- **High Internal / Extended Security:** Black Boxes rely on their own security only. In contrast VitalQIP works with best-of-breed security partners for that unique environment (e.g. Cloud or SDN).

### DDI Network Services Software Platform Architecture





### Competition – By Category (applies to most competitors within the category)

Category	OS Utility	Black Box	Platform
<b>Example</b>	Built-in Microsoft Utilities and DDI Suites (e.g. Solar Winds)	Infoblox and Blue Cat	VitalQIP
<b>Packaging</b>	Part of or installed into OS	Discrete hardware appliances per task	VMs
<b>Interoperation</b>	NA – must consolidate onto server. For Microsoft, must integrate with Active Directory, resulting in DDI silos by OS.	Consolidate on 1 platform by vendor PS group	<b>Works across multiple vendors' DNS / DHCP products</b>
<b>Scalability &amp; Performance</b>	Limited / fixed limits (e.g. Microsoft IPAM limits were 500 then 1,000 addresses, now IPAM on Windows Server 2012 supports 6000 DHCP scopes and 150 DNS zones)	Limited by appliance or governor if shipped as a VM	<b>Limited only by resources available to VMs</b>
<b>Lifecycle</b>	Tied to OS – server refresh often involves rework	Tied to appliance – 3 or 5 years	<b>Perpetual software license</b>

### Competition – Infoblox

Category	Infoblox – the poster child for Black Box	VitalQIP
<b>Use Case</b>	Large Homogeneous Datacenters (Enterprise and Government), Field / Temporary (Government e.g. FEMA), Co-hosted DCs (since appliance is hardened externally)	Private Cloud & Heterogeneous DC (Enterprise and Government), Transaction-based Computing (Financial)
<b>Packaging</b>	Purpose-built appliance per function – DDI, Reporting, etc. and per implementation – external and internal DNS.	Suite of functionality packaged into VMs
<b>Scalability</b>	Appliances have fixed limits; <b>VM option governed to be same as appliance</b>	<b>Unrestricted (Utilizes all resources available to VM)</b>
<b>Interoperation</b>	Replace / consolidate all DDI. <b>For integrations (e.g. OpenStack), Infoblox Grid is required at a very high starting price.</b>	<b>Works across multiple vendors' DNS/ DHCP products. Leverages standard plug-ins to Cloud Platforms.</b>
<b>Implementation</b>	<b>Via an up to 6 month vendor professional services engagement</b>	Overlay approach minimizes implementation
<b>Security</b>	<b>Black Box external / internal hardening only</b>	Internal plus <b>best-of-breed partner extensibility for that environment (e.g. Cloud, IoT &amp; BYOD, SDN/NFV)</b>
<b>Debugging</b>	<b>Customers cannot resolve issues standalone due to no root access, no docs, etc. Infoblox has lost a big customer or two due to this issue.</b>	Open approach includes source access
<b>Lifecycle</b>	Tied to appliance, typically 3 (enterprise) or 5 years (Gov't). <b>Strong customer backlash due to EOL of product versions dating back around 10 years or so.</b>	<b>Perpetual software license</b>
<b>Support costs</b>	Range around 20% for 24x7-4 hour support	Range around 15% for 24x7-4 hours support