

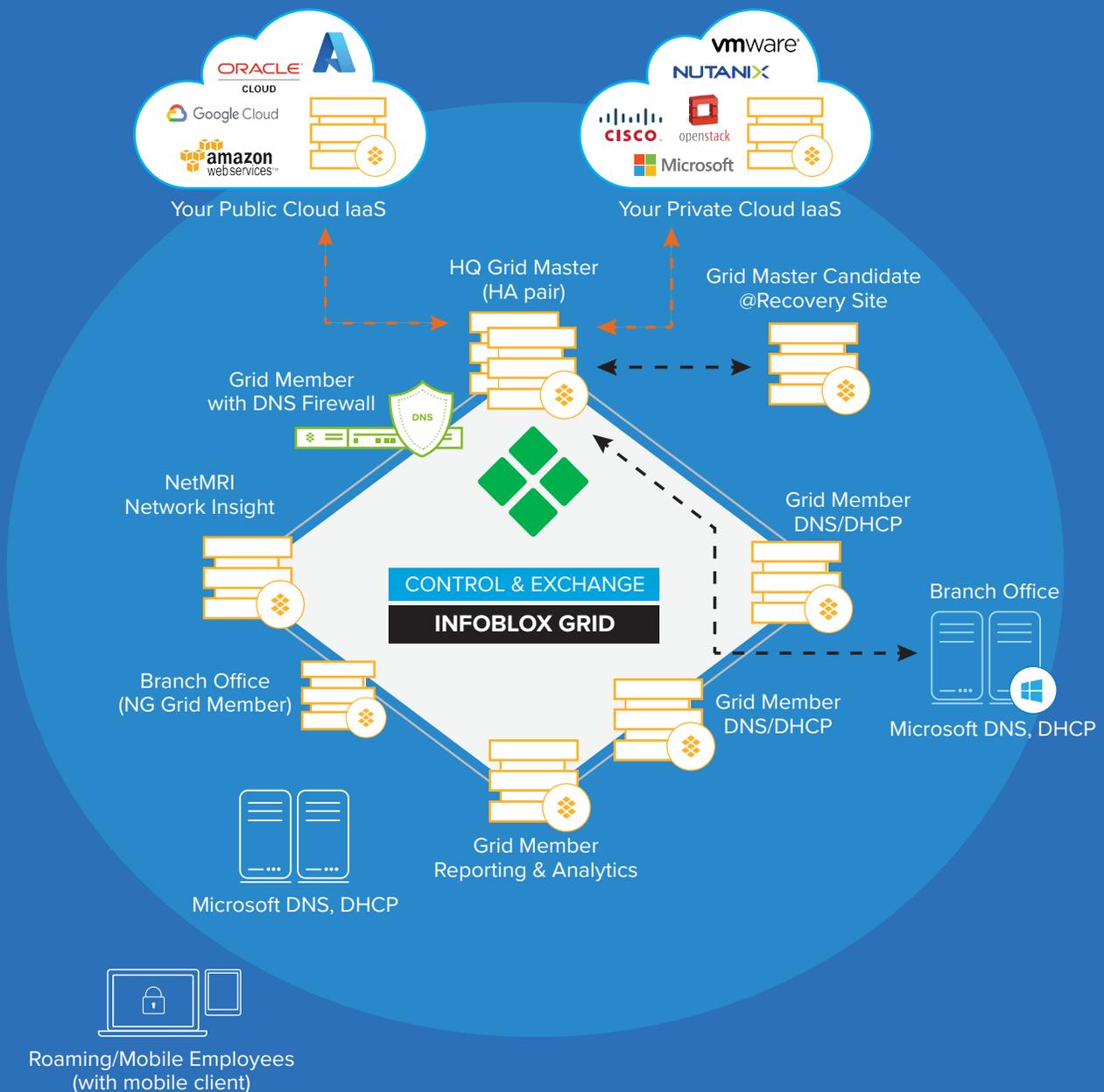
# SOLUTIONS FOR FEDERAL NETWORKS

SECURE | CONTROL | AUTOMATE



## Who We Are and What We Do

Infoblox has been delivering solutions to the federal government since 2000 with a keen focus on network services—DNS, DHCP, and IPAM. As network technologies have evolved, so have our offerings, to include public and private cloud, and cybersecurity protection against malware, APTs, and data exfiltration. From the mobile end device to the cloud, Infoblox delivers the network control, security, and analytical insight that federal organizations demand.





## SECURITY

Infoblox security solutions help our customers identify threats through DHCP fingerprinting, automate discovery of rogue devices, prepare for cybersecurity readiness initiatives (CCRI), secure mobile users wherever they are, and extend control and security from the mobile edge to devices deployed in the cloud. Our unique understanding and control-point access of the services running the network is our key differentiator. Our capabilities allow IT teams to continuously visualize network services and automate the process from a single trusted solution on the network, and DNS level visibility strengthens SecOps efficiency to speed threat investigation and response activities.



## ANALYTICS

Built-in behavioral analytics protect networks against DNS-based threats, and automated discovery and detailed dashboards and reports deliver data-driven insight for pinpointing infected devices, uncovering hard-to-detect threat patterns, and exposing internal attempts at data exfiltration. In addition, a complete and easily accessible view of network assets improves availability, ensures compliance, and supports capacity planning.



## CLOUD

Infoblox solutions for private, public, and hybrid cloud make it easy to efficiently control and secure deployments. They consolidate hybrid cloud management and integrate with a broad range of industry-leading cloud platforms, delivering a centralized view of all physical, virtual, and hybrid network resources. Automatic provisioning and de-provisioning of IP addresses and DNS records lend efficiency and consistency. Cloud-ready DDI, powerful APIs, unparalleled visibility and auditing, and elastic scalability give IT managers control in the cloud. And cloud-specific security features protect users everywhere—on site, roaming, or in branch offices—with automated, high-quality threat intelligence feeds and behavioral analytics delivered as a cloud service.



## NETWORK CONTROL

The Infoblox Grid™ architecture combines built-in disaster recovery, central control from a single pane of glass, and automated failover, backup, restore, changes, and updates. Additional capabilities include automatic discovery and mapping of network configurations. Core network infrastructure and service data are consolidated into a single, comprehensive, authoritative database. Automation and simplified management make it easier to enforce best practices, compliance mandates, and security policies in multivendor environments. And with Infoblox, network teams can automate change, provision rapidly, monitor, and enforce policy compliance.

**SECURITY | Eliminate network vulnerabilities and thwart attacks on critical network infrastructure**

Infoblox enables IT to secure networks from the core by addressing typical network vulnerabilities caused by lack of insight into the network, and by comprehensively addressing the DNS-specific attacks that are becoming the weapons of choice for hackers, cybercriminals, and rogue states.

The most common service targeted by application-layer attacks is DNS. In addition to targeting the DNS service itself, cybercriminals rely on it to infect devices, propagate malware, and exfiltrate data. Intruders often use DNS as a pathway to exfiltrate data because it's commonly overlooked by security solutions that focus on firewalls, IDSs, and proxies.

Infoblox security products make it possible to mitigate challenges that arise from network complexity and

DNS-based threats. Our Protective DNS security solutions combine automation, centralized reporting and policy management, enhanced visibility, and unique actionable intelligence drawn from the data residing in the network core.

- BloxOne® Threat Defense offerings and Infoblox Advanced DNS Protection defend against the widest range of web and DNS-based attacks.
- Detect and control threat activity at the DNS layer that other defense are unable to see.
- Threat Insight technology detects data exfiltration, DGA, DNS tunnels and other malicious behavior with ML/AI.
- BloxOne Threat Defense protects users everywhere—on the premises, roaming, or in branch offices.
- NetMRI proactively monitors networks to validate layer-2 and layer-3 configurations against NSA SNAC, DISA STIG, PCI, or custom policies and to meet requirements for continuing monitoring and cybersecurity readiness.

# CURRENT INFOBLOX TECHNOLOGY ALLIANCE PARTNERS

## Next-gen Data Center

Strategic



In Development



Public Cloud

Cloud Mgmt.

OpenStack



Ecosystem



Engagement



Development

Technology



**ANALYTICS | Analyze, control, and secure the network with actionable network intelligence.**

Devices and applications are growing exponentially and can access networks anytime from anywhere. As networks grow increasingly complex and borderless, traversing traditional, public-cloud, and private-cloud environments, visibility and insight are more important than ever.

Unfortunately, visibility and insight are both in short supply for teams that rely on manual processes and fragmented solutions to run and analyze networks. Infoblox Contextual Reporting and Analytics provides the big picture needed to make fast, accurate decisions that profoundly affect network performance, security, and availability.

Infoblox delivers actionable network and threat intelligence by combining centralized visibility with data-driven insight so that network teams can easily analyze, contextualize control, and secure networks no matter how extensive or sophisticated they become, improving availability, ensuring compliance, and preparing for future requirements.

- Ensure availability with real-time monitoring.
- Plan and manage better with granular DNS and DHCP data, custom dashboards, powerful search, and predictive analytics.
- Rapidly and automatically detect and remediate threats.
- Ensure compliance and simplify audits with advanced reporting.

**Network Infrastructure**

**Security**

**NOKIA**

**CISCO** **FireEye**

**CISCO** **ERICSSON** **HUAWEI**

**intel Security**

**SP Services** **NGDC** **Wireless**

**Vulnerability**

**SIEM / Sec Auto**

**Endpoint**

**NAC**

**Threat Intel**

**NUTANIX**

**QUALYS**

**intel Security**

**CARBON BLACK**

**Google**

**REVERSING LABS**

**SURBL**

**CYREN**

**proofpoint**

**RISKIQ**

**Check Point**

**iSIGHTPARTNERS**

**FARSIGHT SECURITY**

**CROWDSTRIKE**

**DomainTools**

**OpenPhish**

**SECURE DOMAIN**

**PHISHME**

**ThreatTrack**

**THREATWAVE**

**NEC/Netcracker**

**tripwire**

**TANIUM**

**FLASH networks** **affirmed** **aruba**

**servicenow**

**CROWDSTRIKE**

**tenable network security**

**ForeScout**

**ISC Internet Systems Consortium**

**Lumeta Network Situational Awareness**

**netskope**

**gemalto SafeNet**

**AppViewX TDBFusion**

**THALES**

**CLOUD | Maximize the capabilities of cloud deployments by improving security, efficiency, and visibility.**

Virtual and private clouds provide organizations with undeniable benefits in scalability, agility, and cost control. However, conventional network management tools don't offer the same advantages as Infoblox. Those advantages. For example, DNS and IP address configurations are largely performed manually using segmented point solutions. These tools are not designed to support elastic scalability. Nor can they provide the control, visibility, reliability, and consistency today's federal organizations demand.

That's why we created Infoblox DDI for Virtualization and Private Cloud. Actionable network intelligence makes it possible to control DNS, DHCP, and IPAM for complex distributed virtual and cloud-based environments—centrally, flexibly, and efficiently. Now network teams can support complex multi-platform workloads with confidence and maximize the full potential of private cloud and virtualization deployment strategies.

- Automate manual processes for DNS and IP address provisioning.
- Gain a consolidated view of network resources across cloud and virtualized environments.
- Bolster security and reliability by making sure multi-platform networks are consistent and compliant.
- Integrate out-of-the-box with a broad range of platforms including VMware, OpenStack, Docker, and Microsoft.

**NETWORK CONTROL | Increase consistency, reliability, and IT efficiency with centrally managed, integrated DDI.**

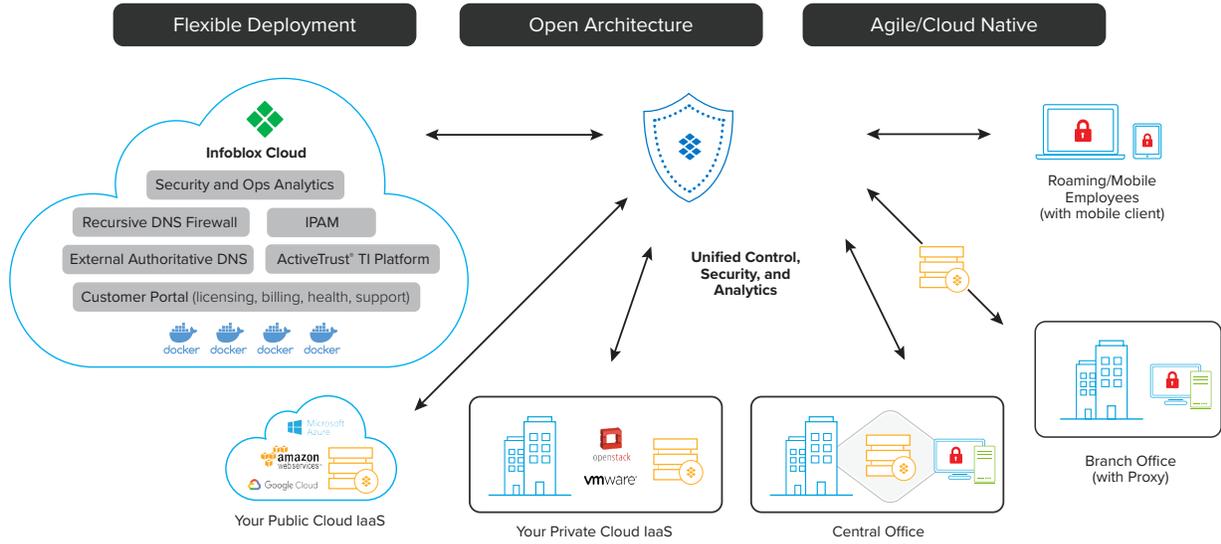
Network landscapes are rapidly evolving, driven by trends in security, virtualization, cloud, SDN, IPv6 adoption, and the Internet of Things (IoT). These demand advanced solutions for managing DNS, DHCP, and IP address management—collectively known as DDI—and complete network discovery and dynamic inventory for multi-vendor layer-2 and layer-3 devices.

Infoblox DDI is our industry-leading, integrated, and centrally managed approach to delivering enterprise-grade DDI. It uses our patented Infoblox Grid™ technology to ensure high availability DNS, DHCP, and IPAM services throughout complex distributed networks. Infoblox DDI makes it easier to support current and evolving needs, while achieving the highest standards for security, service uptime, and operational efficiencies. Infoblox DDI—working in conjunction with Infoblox NetMRI network discovery and dynamic inventory for multivendor layer-2 and layer-3 physical and virtual network elements—provides a rich central repository of actionable information for network control.

- Centrally orchestrate DDI functions across diverse infrastructure with integrated capabilities for hybrid and public cloud and virtual and private cloud environments.
- Access rich, integrated reporting and analytics capabilities for capacity planning, asset management, compliance control, and auditing.
- Boost IT efficiency and automation by seamlessly integrating with other IT systems through RESTful APIs, in conjunction with the Infoblox Grid™.



# ARCHITECTURE, DEPLOYMENT, AND TECHNOLOGY VISION



# CONTACT US

## TO FIND OUT MORE ABOUT WHAT WE DO AND HOW WE DO IT.

### GSA Contract Schedule Information

GSA forms long-term government-wide contracts with commercial firms that grant access to commercial products and services at discounted rates.

### Certifications

Infoblox products and solutions are used at every classification level in the federal government. They are approved for use by the intelligence community and certified at the highest levels, including:

- DADMS approval DADMS # ID 101020
- DISA DoDIN APL certification
- NIST and CAVP certification
- Common Criteria EAL 2 certification
- IOL USGv6 certification (DHCPv6)
- FIPS 140-2

### NASA SEWP

SEWP V is a GWAC that supports government requirements for high-performance IT by providing state-of-the-art commercial hardware, software, services, and solutions.

### Contract Information

- Agency/Program: NNG15SC16B (Category A, Group A)
- Agency/Program: NNG15SC39B (Category B, Group D)
- Expiration: April 30, 2025
- Held by: Carahsoft

### NETCENTS-2 (Coming GSA's 2GIT IDIQ)

NETCENTS-2 contracts give the Air Force a primary source of netcentric and IT products, services, and solutions. Use of the NETCENTS-2 contracts (except ITPS) is mandatory for Air Force organizations as contracts are awarded.

### Contract Information

- GSA Schedule 70 GSA Schedule Number: GS-35F-0119Y
- Held By: Carahsoft
- Period of Performance: December 20, 2011 – June 17, 2017
- NAICS: 334210

The fundamental purpose of the ITES-SW acquisition is to support the Army enterprise infrastructure and infrastructure goals and leverage specific COTS software products and maintenance.

The US Army has defined six vendors. Three of the six partners include Infoblox VAR partners—Dell, WWT, and CDWG.

### Contract Information

- GSA Schedule 70 GSA Schedule Number: GS-35F-0119Y
- Held By: Carahsoft
- NAICS: 511210
- Size Standard: Other Than Small

### Past Performance

Infoblox Federal Inc. has extensive experience meeting the needs of civilian, military, defense and intelligence agencies, and our products support industry and governmental standards, including IT governance mandates such as:

- DISA Security Technical Implementation Guide (STIG)
- NSA Systems and Network Attack Center (SNAC)
- Federal Information Security Management Act (FISMA)
- Cryptographic Module Validation Program

### About Infoblox Federal

Infoblox is the global leader in providing Secure DNS and Cloud Managed Network Services for a wide array of both Federal agencies and State and Local governments. Infoblox brings DNS security, reliability and automation solutions to on premises, cloud and hybrid deployments allowing for a single pane of glass for network management.



One Dulles Technology Center  
13454 Sunrise Valley Dr., Ste. 570  
Herndon, VA 20171

+1.844.226.4910  
info@infobloxfederal.com  
DUNS 078826227  
Cage 6YBTO

