

INFOBLOX DDI- HYBRIDBEREITSTELLUNG

Zentralisierte Sichtbarkeit, Automatisierung und Kontrolle für das grenzenlose Unternehmen von heute

ZUSAMMENFASSUNG

Der Wechsel zu einer Cloud-verwalteten Umgebung für Netzwerkservices bietet überzeugende Vorteile wie Flexibilität, Kostensenkung, verbesserte Benutzerfreundlichkeit und größere Effizienz durch optimierte Arbeitsabläufe.

Während Unternehmen ihre Umgebungen virtualisieren und den Cloud-Betrieb ermöglichen, bleiben die Herausforderungen für das Netzwerk bestehen, werden aber im gesamten Ökosystem verschärft. Dies gilt für die Netzwerkerkennung, Sichtbarkeit und Synchronisierung, hohe Verfügbarkeit und Ausfallsicherheit. Ebenso müssen Unternehmen mit Herausforderungen bei der Vereinfachung und Automatisierung von Arbeitsabläufen, der Skalierbarkeit, der Berichterstattung, der Technologieintegration und der Sicherheit rechnen, um Benutzer, Daten und Infrastruktur überall zu schützen.

Dank der marktführenden Lösungen von Infoblox für vor Ort und in der Cloud verwaltete Core-Netzwerkdienste und der Erfahrung mit hybriden DDI-Implementierungen können Sie die Transparenz, Automatisierung und Kontrolle in allen Unternehmensumgebungen vereinfachen und verbessern.

ENTERPRISE-NETWORKING FÜR DIE MODERNE BELEGSCHAFT

Mobilität, IoT und Cloud haben die Art und Weise verändert, wie Menschen sich miteinander vernetzen und geschäftlich tätig sind. Mobilgeräte sind ein wesentlicher Bestandteil des täglichen Lebens. Das Internet der Dinge (IoT) breitet sich in den Bereichen Fertigung, Transport, Energie und Einzelhandel aus. Geschäftskritische Anwendungen verlagern sich rasch auf cloudbasierte Lösungen wie Salesforce, Microsoft und Box.

In der Folge wächst die Zahl der verbundenen Geräte und Standorte, insbesondere am Netzwerkrand. Mitarbeiter und Kunden erwarten zuverlässige Konnektivität, hohe Verfügbarkeit und schnelle Reaktionszeiten. Und dadurch steigt wiederum die Nachfrage nach Lösungen, die die Verwaltung und Kontrolle von verteilten Umgebungen vereinfachen und optimieren.

WARUM ÜBER EINEN HYBRIDANSATZ NACHDENKEN?

Unternehmen verwalten ihre zentralen Netzwerkdienste traditionell über das Backhauling von DNS und DHCP in zentralen und regionalen Rechenzentren und verwenden lokale Server- oder Router-basierte DDI-Implementierungen in Zweigstellen, Remote-Standorten und verteilten Niederlassungen.

Obwohl diese Bereitstellungsmodelle nach wie vor gewisse Kostenvorteile bieten, sind sie weniger effizient, da die Anzahl der Standorte zunimmt und sich der Schwerpunkt der Aktivitäten in den Randbereich verlagert. Gleichzeitig ist die Verwendung mehrerer DNS- und DHCP-Lösungen im Rechenzentrum des Unternehmens und an entfernten Standorten umständlich, zeitaufwändig und fehleranfällig, insbesondere im großen Maßstab. Jeder Standort

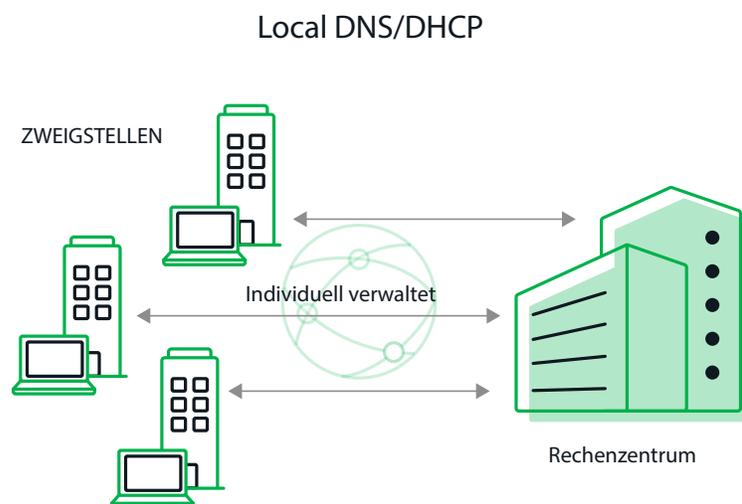


Abbildung 1: Traditionelles Modell für die Netzwerkbereitstellung

erfordert eine individuelle Verwaltung mit mehreren Tools und Prozessen für die Bereitstellung, Verwaltung und Kontrolle. Dies birgt ein erhebliches Potenzial für Unstimmigkeiten zwischen den Standorten, Ausfälle und Beeinträchtigungen der Anwendungs- und Serviceleistung.

Außerdem sind Netzwerkinstabilität und Ausfälle kostspielig. Unabhängig davon, ob sich Unternehmen bei der Migration in die Cloud für die Beibehaltung einer herkömmlichen Architektur oder für eine vollständige Cloud-Bereitstellung entscheiden, bleibt die Notwendigkeit einer klaren Sichtbarkeit, Zuverlässigkeit, Automatisierung und Kontrolle für jede verteilte Umgebung unerlässlich – egal ob groß oder klein.

ZENTRALISIERTE SICHTBARKEIT, AUTOMATISIERUNG UND KONTROLLE FÜR DAS GRENZENLOSE UNTERNEHMEN

Seit mehr als zwei Jahrzehnten wissen Unternehmen um den Wert von Infoblox DNS, DHCP und IP Address Management (oder DDI) für einen zuverlässigen, globalen, geschäftskritischen Betrieb. Als klarer Branchenführer bietet Infoblox Unternehmen eine zuverlässige, leicht zu verwaltende Auswahl an NIOS Grid-basierten Diensten, die für Unternehmens- und regionale Rechenzentren optimiert sind. Für Unternehmen mit Cloud-Initiativen bietet Infoblox kosteneffizientes, über die Cloud verwaltetes BloxOne™ DDI für verteilte Standorte und Niederlassungen. Für alle Bereiche dazwischen bietet Infoblox ein kombiniertes hybrides Bereitstellungsmodell für umfassende Sichtbarkeit, Automatisierung und Kontrolle von Netzwerken jeder Größe vom Rechenzentrum bis zum Netzwerkrand – und das alles über eine zentrale Steuerungsebene.

Die hybride Bereitstellung beginnt mit der robusten Funktionalität und den Vorteilen von Infoblox NIOS Grid-basiertem DDI, das mit Mehrwertdiensten integriert ist, darunter Microsoft Management für Transparenz und Synchronisierung, Network Insight und Cloud-Network Automation für Erkennung und Automatisierung, DNS Traffic Control (DTC) für globalen Server-Lastausgleich sowie Reporting und Analytics für kontextbezogene Netzwerktransparenz. Offene RESTful-APIs und vorgefertigte Integrationen steigern den Geschäftswert und beschleunigen DevOps-Implementierungen. Darüber hinaus ermöglicht die zukunftssichere Architektur von BloxOne™ DDI die Optimierung von SaaS-Anwendungen und -Services sowie die lokale Ausfallsicherheit durch ein einheitliches Verwaltungsmodell. BloxOne DDI nutzt außerdem eine erweiterbare Microservices- und Container-basierte Plattform zur Vereinfachung der Bereitstellung, Rationalisierung des Betriebs und Minimierung der Gesamtbetriebskosten bei der Verwaltung von Dutzenden, Hunderten oder sogar Tausenden von verteilten Standorten und Niederlassungen.

Infoblox bietet die Möglichkeit, Angebote mit integrierter DNS-Sicherheit, Firewalls und einem umfangreichen und wachsenden Sicherheits-Ökosystem zu erweitern, um Unternehmen vor wachsenden Bedrohungen zu schützen. Zusammengenommen ermöglichen die hybriden Lösungen von Infoblox die Bereitstellung, Verwaltung und Kontrolle mehrerer Rechenzentren und weltweit verteilter Standorte von einem zentralen Standort aus. Dabei werden Investitionen geschützt, der ROI optimiert und die Skalierung für zukünftige Geschäftsanforderungen ermöglicht.

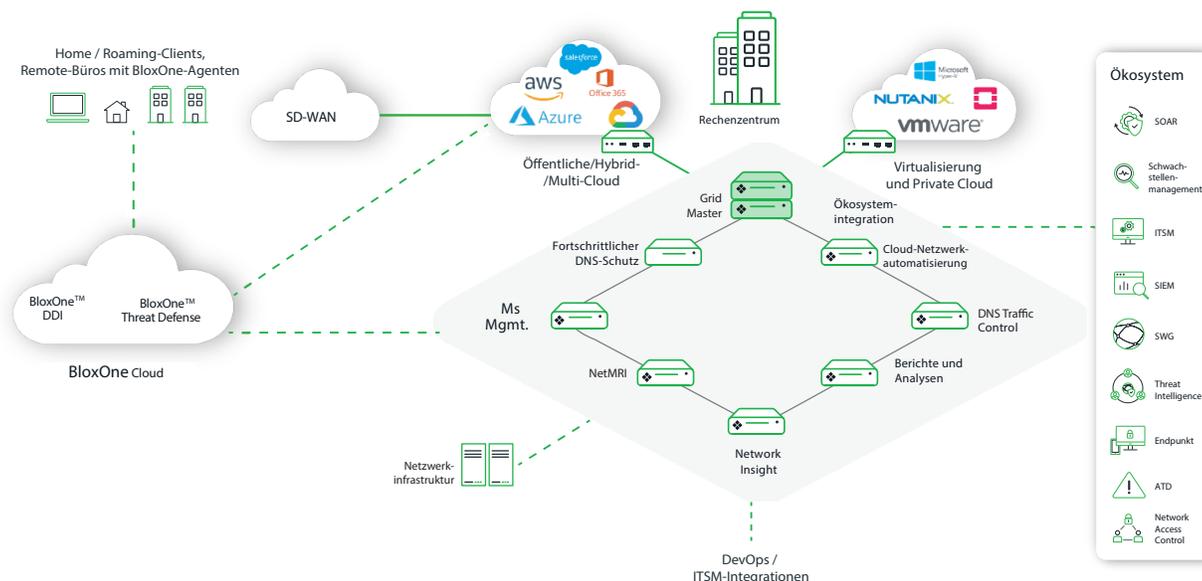


Abbildung 2: Bereitstellungsmodell für hybride Netzwerke

- **Zuverlässigkeit:** Vollständig integriertes DNS vor Ort oder in der Cloud
- **Zukunftssicher:** Cloud-verwaltete Infrastruktur bis zum Netzwerkrand
- **Resilienz:** Cloud-verwaltete Niederlassungen mit lokaler Ausfallsicherheit
- **Sicherheit:** Einheitlicher DNS-Schutz ermöglicht grundlegende Sicherheit überall
- **Automatisierung:** APIs und integrierte Vorlagen beschleunigen die Bereitstellung und optimieren die Investition
- **Kontrolle:** DNS GSLB für Traffic-Management, Disaster Recovery und Skalierbarkeit
- **Transparenz:** Zentrale Steuerungsebene mit kontextbezogenen Echtzeitdaten für schnelle Triage und Lösung

KUNDENEINBLICKE: LÖSUNG MODERNER NETZWERKHERAUSFORDERUNGEN

Globale Anwaltskanzlei: Vermeidung von Netzwerkausfällen

Die Leistung einer vollständig integrierten Lösung

Als eine global tätige Anwaltskanzlei mit mehreren Standorten weltweit mit erheblichen DNS-Stabilitätsproblemen zu kämpfen hatte, startete sie ein Projekt zur Aktualisierung ihrer Umgebung. Stakeholder aus allen Bereichen des Unternehmens wurden einbezogen, um sicherzustellen, dass die Lösung den wichtigsten Unternehmenszielen entsprach, einschließlich erweiterter Sicherheit und ihrer Cloud-First-Initiative. Die Kanzlei wollte nicht die gesamte Infrastruktur in die Cloud migrieren und entschied sich daher für eine hybride Umgebung.

Die Anwaltskanzlei entschied sich für eine Kombination aus Infoblox NIOS-basierten DDI-, BloxOne™ DDI- und BloxOne™ Threat Defense-Lösungen, um alle Anforderungen zu erfüllen. Die NIOS DDI-Lösung umfasste Advanced DNS Protection (ADP), um ihr DNS gegen DDoS-Angriffe (Distributed Denial of Service) zu schützen. Außerdem wurde DNS Traffic Control (DTC) Global Server Load Balancing für die Verwaltung des Traffics im Rechenzentrum, die Ausfallsicherheit von Anwendungen und die Skalierbarkeit eingesetzt. BloxOne DDI wurde für alle Niederlassungen gewählt, um die Bereitstellung und Verwaltung zu vereinfachen und gleichzeitig eine gleichbleibende Anwendungsleistung und lokale Ausfallsicherheit im gesamten verteilten Unternehmen zu gewährleisten.

BloxOne Threat Defense wurde ebenfalls hinzugefügt, um den bestehenden Schutz durch ADP für DDoS zu erweitern. Darüber hinaus wurde die DNS Firewall (DNSFW) eingesetzt, um die einheitliche Sicherheitslösung zu vervollständigen. Die Automatisierung über APIs und Konfigurationsvorlagen vereinfachte die Integrationen mit den erforderlichen Lösungen für den Geschäftsbetrieb, die Fehlersuche und die Problemlösung.

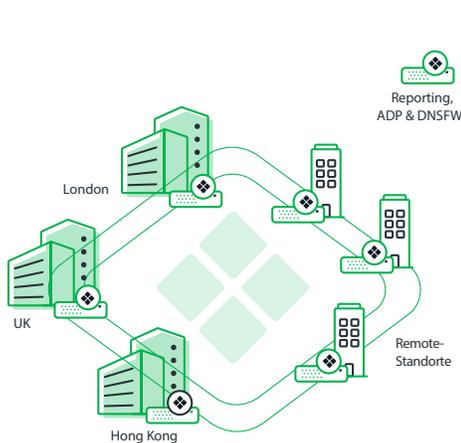


Abbildung 3: Vorher – Traditionelles DDI-Modell

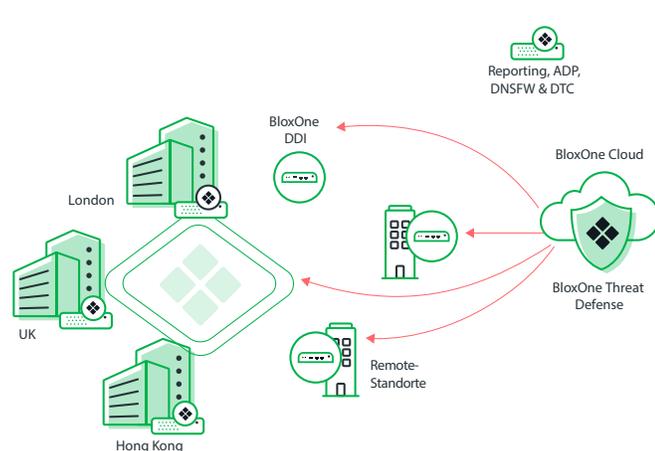


Abbildung 4: Nachher – Cloud-verwaltetes SaaS-Modell

- **Disaster Recovery:** Schnelle Rückkehr zur Normalität für die Geschäftskontinuität bei Störungen
- **Resilienz:** Cloud-verwaltete Niederlassungen mit lokaler Ausfallsicherheit
- **Sichtbarkeit:** Zentrale Steuerungsebene mit Kontextdaten in Echtzeit für ein besseres Netzwerkmanagement
- **Nachhaltigkeit:** Kostengünstigste DDI-Services für verteilte Standorte für bessere Gesamtbetriebskosten
- **Zentrale Steuerung:** Vereinfachte Bereitstellungen, verbesserte Effizienz und optimierte Abläufe
- **Automatisierung:** APIs und integrierte Vorlagen beschleunigen die Bereitstellung und optimieren die Investition

Globaler Anbieter im Gesundheitswesen: Sicherstellung der Geschäftskontinuität bei Naturkatastrophen

Disaster Recovery und Ausfallsicherheit der Standorte

Als ein Hurrikan einen wichtigen Produktionsstandort zerstörte, waren die Lieferungen, die Lieferkette, die Geschäftsabläufe und der Umsatz dieses global tätigen Anbieters von Gesundheitsprodukten weltweit beeinträchtigt. Nach der Wiederherstellung des Betriebs setzte das Unternehmen die Priorität auf die Ausweitung der IT-Aktivitäten über die traditionelle Notfallwiederherstellung hinaus, um die Ausfallsicherheit seiner Standorte und die betriebliche Kontinuität im Falle künftiger Katastrophen zu gewährleisten.

Es wurde NIOS-basiertes DDI installiert, um die Leistung und Ausfallsicherheit in den Rechenzentren des Unternehmens zu verbessern. BloxOne™ DDI wurde für verteilte Standorte gewählt, weil es die kostengünstigste Lösung pro Standort für zentrale Dienste bot und den Zugriff auf Anwendungen, die lokale Ausfallsicherheit und die Betriebskontinuität optimierte.

Durch die Kombination von Infoblox NIOS-basierten DDI- und Cloud-nativen BloxOne™ DDI-Lösungen erhielt der Anbieter die zuverlässigste und wirtschaftlichste Lösung, um die Disaster Recovery und Ausfallsicherheit seiner Standorte zu gewährleisten. Darüber hinaus erhielt er eine detaillierte Echtzeittransparenz vom Rechenzentrum bis zum Unternehmensrand sowie eine vereinfachte Verwaltung und Kontrolle bei im Vergleich zu alternativen Lösungen niedrigeren Durchschnittskosten pro eingerichtetem Standort.

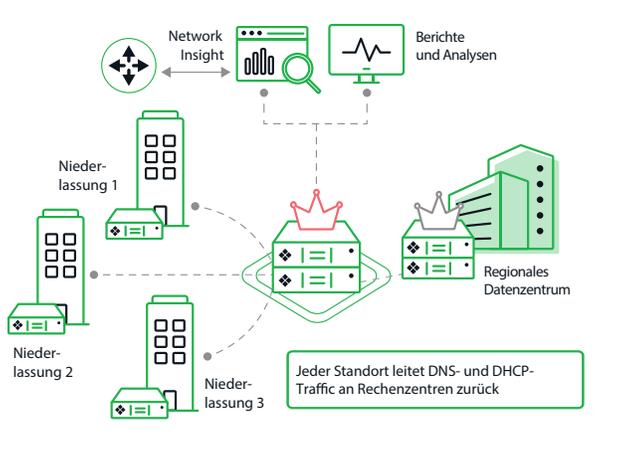


Abbildung 5: Vorher – Traditionelles DDI-Backhaul-Modell

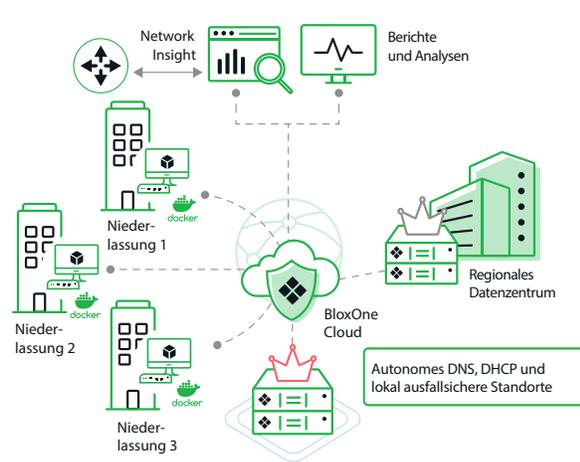


Abbildung 6: Nachher – Cloud-verwaltetes SaaS-Modell

- **Zuverlässigkeit:** Vollständig integriertes DNS vor Ort oder in der Cloud für Zuverlässigkeit rund um die Uhr
- **Sichtbarkeit:** Zentrale Steuerungsebene mit Kontextdaten in Echtzeit für ein besseres Netzwerkmanagement
- **Ausfallsicherheit:** Integrierte Disaster Recovery und Redundanz für Geschäftskontinuität
- **Kostenkontrolle:** Abonnements senken die Kosten, gewährleisten die neuesten Technologien und ermöglichen Portabilität
- **Zukunftssicher:** Eine hybride und Cloud-verwaltete Architektur lässt sich bis zum Netzwerkrand skalieren
- **Sicherheit:** Einheitlicher DNS-Schutz ermöglicht grundlegende Sicherheit überall

Globale Energie-, Öl- und Gasgesellschaft: Verbesserung von Zuverlässigkeit und Kostenmanagement

Disaster Recovery und Ausfallsicherheit der Standorte

Bei diesem globalen Energieriesen führten Fusionen, Übernahmen, globales organisches Wachstum und technologischer Wandel im Laufe der Zeit zu verschiedenen Netzwerklösungen und -umgebungen, die von Rechenzentren vor Ort bis hin zu zahlreichen Remote-Standorten mit cloudbasierten SaaS-Anwendungen reichten. Zu dieser Komplexität kam die Aufgabe hinzu, eine zuverlässige Konnektivität für Tausende von globalen Ein/Aus-Ventilen, Durchflusskontroll- und Logiksteuerungen, Telemetrieeräten und einer Vielzahl anderer benötigter Maschinen sicherzustellen. Viele Geräte mussten rund um die Uhr überwacht und gesteuert werden, weshalb Transparenz, Redundanz und Ausfallsicherheit von entscheidender Bedeutung waren. Es wurden große Anstrengungen unternommen, um die globale Infrastruktur hinsichtlich Transparenz, Agilität, Sicherheit, Leistung und Kostenmanagement zu vereinheitlichen und zu modernisieren.

Eine NIOS-basierte DDI-Lösung mit physischen, virtuellen und cloudbasierten Appliances der nächsten Generation bildete im Rechenzentrum die Grundlage für zuverlässige, vereinfachte Kernnetzwerke, Sicherheit und Cloud-Mehrwertdienste. Anschließend wurde BloxOne™ DDI für eine zentralisierte Sichtbarkeit, Verwaltung und Kontrolle eingesetzt. Außerdem wurden SaaS-Anwendungen und -Dienste optimiert und die Ausfallsicherheit lokaler Standorte durch Hunderte kleiner, mittlerer und großer virtueller Appliances in den Rechenzentren des Unternehmens, in den Niederlassungen und an Remote-Standorten gewährleistet. Darüber hinaus wurde BloxOne™ Threat Defense integriert, um DNS-basierten globalen Schutz, Echtzeit-Analysen, Ökosystem-Integrationen und kontextbezogene Einblicke zur Förderung von Big Data-Analysen zu bieten.

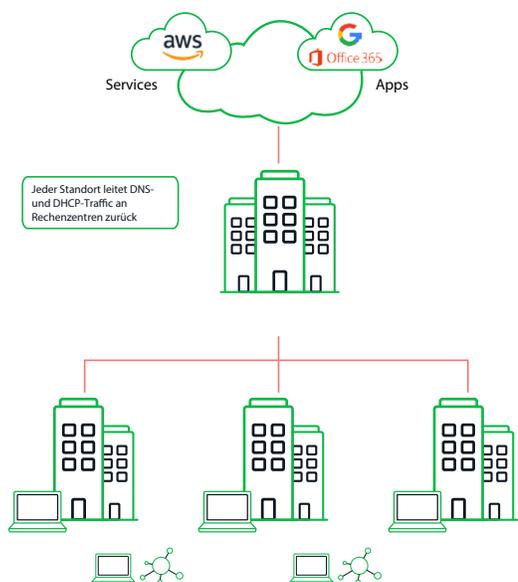


Abbildung 7: Vorher – Traditionelles DDI-Backhaul-Modell

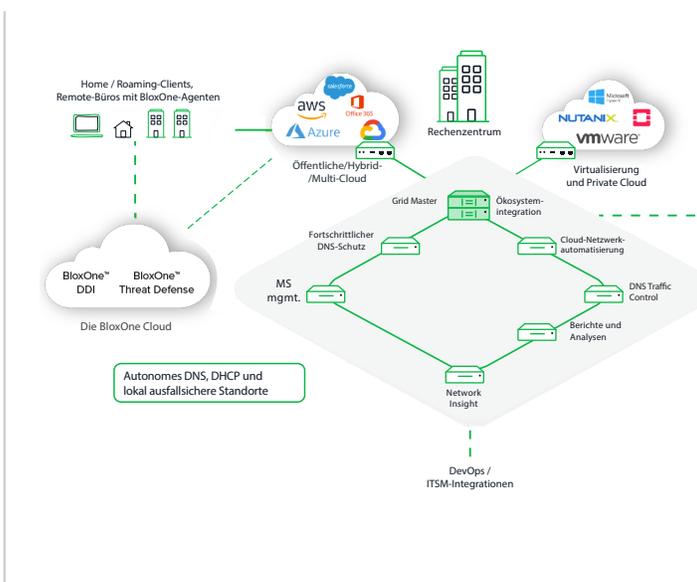


Abbildung 8: Nachher – Hybrides DDI-Cloud-Managed-Modell

Infoblox bietet marktführende hybride Lösungen für On-Premises- und Cloud-verwaltete zentrale Netzwerkdienste. Wenn es für Sie an der Zeit ist, die Kontrolle, Automatisierung und Sicherheit in Ihren Unternehmensumgebungen zu vereinfachen und zu verbessern, kontaktieren Sie unser Account-Team für weitere Informationen. Oder [testen Sie DDI im Rahmen einer kostenlosen Evaluierung](#).



Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Hauptsitz der Gesellschaft
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

