infoblox.
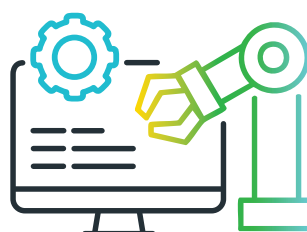
MODERNIZE MANUFACTURING OPERATIONS: OPTIMIZE NETWORKING, INCREASE PRODUCTIVITY AND SECURE DATA

SUMMARY

With Infoblox solutions, your manufacturing organization can simplify and modernize critical network services while improving security, enabling significant efficiency and productivity gains.

Infoblox solutions streamline and automate the foundational services that make modern networking possible—DNS, DHCP and IP address management (DDI). Together, our enterprise-grade DDI and comprehensive security capabilities empower you to better protect sensitive intellectual property and operational data, support compliance and effectively navigate the rapidly evolving manufacturing IT landscape.

OVERVIEW & CHALLENGES

Industry 4.0 and smart manufacturing are transforming how your organization operates, fueling the need to implement next-generation technology to create more efficient, flexible and intelligent processes to deliver better products, faster production times and less waste. Cloud-first strategies, increasing cyberthreats and rising customer expectations are accelerating this shift, exposing critical gaps in visibility, security and operational control. Hybrid and multi-cloud environments are becoming standard, yet many manufacturing organizations still rely on legacy, fragmented systems and siloed teams. Cyberattacks, such as ransomware, are increasingly—and often successfully— targeting manufacturing companies, impacting operational efficiency and causing production delays. Disjointed critical network services lead to network misconfigurations and poor asset visibility, exposing operations to pervasive threats that traditional security tools cannot detect. Lastly, aging infrastructure, rising scalability and evolving regulatory compliance requirements only add complexity.

Infoblox can help you bridge these challenging gaps. By providing unified and automated critical network services and strengthening cybersecurity posture, our solutions enable your organization to operate with greater speed, resilience and confidence to keep pace with your productivity objectives.

KEY BENEFITS FOR MANUFACTURING ORGANIZATIONS

- **Accelerate Cloud Transformation:** Centralize and automate critical network services and bolster security across hybrid and multi-cloud infrastructure.

- **Maximize Uptime and Reduce Outages:** Ensure continuous availability for all network-connected production and supply chain assets.

- **Secure Your Network and Prevent Breaches:** Proactively protect all devices (traditional, IoT and OT) to safeguard manufacturing infrastructure and sensitive data.

- **Simplify Regulatory Compliance:** Automatically assess and ensure compliance with evolving regulations, avoid legal penalties and sustain customer trust.

Challenges Manufacturing Organizations Face and the Consequences of Maintaining the Status Quo

Challenge	Description	Consequence	Description
Operational Complexity	Since 2019, hybrid cloud adoption has grown by 68% among manufacturers.[1] The management and data integration tied to these systems can create silos and operational complexity that reduce agility and cause delays.	Rising Operational Costs	In cloud environments, maintaining legacy infrastructure requires more effort and manual oversight. The cost of downtime and troubleshooting can exceed the cost of investing in automation and centralized control. IT budgets may shift from strategic projects to firefighting and patching.
Scalability and Resilience	Manufacturers need resilient, scalable network services to support growing device density, factory digitization and global operations.	Inability to Scale and Adapt	Limited scalability increases the risk of bottlenecks, downtime and delays—disrupting production and impacting customer commitments.
Cybersecurity Pressure	Because of the sensitive data they handle, manufacturing organizations face increasing risk from cyberattacks. In 2023, the manufacturing industry experienced 638 ransomware attacks globally.[2]	Increased Exposure to Threats	Without proactive measures, manufacturing organizations remain vulnerable to cyberattacks. Recovery can be costly and disruptive, and result in lasting damage to an organization's reputation and regulatory standing.
Regulatory Compliance Requirements	Manufacturing organizations must adhere to regulations, like GDPR and NIS2, and recommended standards, like IEC 62443. Ensuring compliance requires detailed logging, reporting and remaining current with evolving requirements.	Compliance Gaps	Non-compliance can lead to fines, legal penalties, loss of trust and regulatory scrutiny that can create additional reputational damage.

INFOBLOX SOLUTIONS

Infoblox solutions enable your manufacturing IT organization to meet the complexity, scale and security demands of on-premises, hybrid and multi-cloud environments. The Infoblox Universal DDI™ Product Suite combines DNS, DHCP and IPAM to simplify and automate network operations across your existing legacy and cloud-based infrastructure. By unifying these critical network services in a centralized platform, the solution eliminates manual errors, reduces provisioning delays and ensures consistent policy enforcement across distributed environments. In addition, it provides comprehensive visibility and analysis of all assets across public clouds, on-premises networks, IoT/OT devices and third-party applications, enabling teams to troubleshoot faster while avoiding resource conflicts.

infoblox.

Traditional security measures are insufficient against today's evolving malware and AI-driven threats. Most tools detect and respond reactively, only after a breach occurs. Infoblox Threat Defense™ uses industry-leading DNS threat intelligence and algorithmic detection to preemptively block devices from accessing malicious domains, proactively safeguarding manufacturing operations against cyberattacks. These capabilities integrate with existing security ecosystem tools, such as security information event management (SIEM) platforms, improving visibility and accelerating response times.

Infoblox Universal DDI and Threat Defense empower your IT teams to streamline operations and strengthen cyber resilience. Moreover, they simplify the work involved in meeting compliance requirements, including GDPR, NIS2 and industry-specific standards. Among these, IEC 62443 is becoming increasingly prevalent in manufacturing organizations as cybersecurity threats to industrial control systems (ICS) and OT environments grow more sophisticated. With flexible deployment models, built-in automation and extensive API support, Infoblox enables your manufacturing organization to move faster, scale efficiently and stay ahead of operational and regulatory risk.

KEY USE CASES

Infoblox solutions support several high-impact use cases that help manufacturing organizations modernize infrastructure, improve operational resilience and strengthen their security posture. These scenarios reflect the specific demands manufacturing organizations face in scaling operations, protecting intellectual property and enabling modern production environments.

Supporting Network Services Transformation: Infoblox enables manufacturing organizations to modernize aging and siloed infrastructure by centralizing DNS, DHCP and IPAM through its enterprise-grade DDI platform. These services are delivered consistently across on-premises, hybrid and multi-cloud environments, replacing manual, error-prone processes with automated workflows tailored to the needs of factory floor and enterprise environments. Infoblox supports extensive API integration, helping to unify systems and tools while accelerating network provisioning. The result is a more agile, secure and scalable network foundation that reduces operational costs and enables faster service deployment.

Minimizing IP Address Conflicts: With the explosion of connected devices—traditional, IoT, OT, robotics and ICS—Infoblox automatically detects and resolves IP address conflicts before they disrupt services. Real-time alerts, centralized IP address tracking and historical data analysis give teams the visibility needed to manage network changes and prevent conflicts and misconfigurations proactively. Automating IPAM helps manufacturing organizations avoid costly outages, reduce troubleshooting time and free up resources for higher-value initiatives, especially in dynamic, multi-cloud environments.

Facilitating Business Continuity and Disaster Recovery: Infoblox ensures local survivability and continuous network operations during outages through local DNS caching, resilient architecture and automated failover processes. This helps manufacturing organizations maintain critical network services, protect against security vulnerabilities and reduce dependency on central infrastructure, ensuring operational continuity and the sustained uptime of production environments.

Simplifying Network Consolidation Due to Mergers and Acquisitions: Infoblox's centralized DDI solutions facilitate the seamless integration of disparate networks during mergers and acquisitions. Enhanced visibility, automated processes and robust security features help manufacturing organizations manage expanded network infrastructures, reduce operational complexity and protect against potential threats and vulnerabilities.

Preemptive Protection from Ransomware and Data Breaches: Threat Defense leverages DNS threat intelligence to detect and block malicious domains early in the attack cycle, disrupting ransomware and preventing data breaches. Proactive detection, automated response and comprehensive visibility into DNS traffic help manufacturing organizations maintain regulatory compliance requirements and protect sensitive intellectual property, engineering data and production workflows from disruption.

CONCLUSION

As a competitive manufacturing enterprise, your organization understands the need to modernize infrastructure while navigating increased operational demands, heightened cyber risk and evolving compliance requirements. Achieving these goals requires evolving your underlying network to increase agility, visibility and resiliency in dynamic production environments. Infoblox solutions make that evolution possible through a unified approach to critical network services and Protective DNS security. They empower your teams to centralize and automate DDI across all environments, reduce complexity, scale operations faster and protect critical production systems, data and supply chains.

Modernize your network foundation and secure your production environments with united networking and security from Infoblox.

WHY MANUFACTURING ORGANIZATIONS CHOOSE INFOBLOX

- **Hybrid and Multi-Cloud Ready:** Ensure consistent critical network services across on-premises and multi-cloud environments.

- **Protective DNS:** Detect and block threats like ransomware preemptively with algorithmic protections and DNS-centric threat intelligence.

- **Complete Infrastructure Visibility:** Monitor IP activity, DNS traffic and connected devices from a single console.

- **Built-In Resilience:** Ensure business continuity during outages with local caching and automated failover.

- **Streamlined Automation:** Reduce manual work and accelerate provisioning with API-driven orchestration.

- **Compliance Confidence:** Support evolving regulations through granular logging, policy enforcement and reporting.

---

[1] 6 Compelling Stats on Hybrid Cloud Boosting Manufacturing Innovation,
     Number Analytics, March 27, 2025.
[2] Global sectors most targeted by industrial ransomware attacks 2023, Statista, February 2024.

---

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com