

**SOLUTION NOTE**

# INFOBLOX HYBRID SECURITY FOR PERVASIVE PROTECTION

## Strengthen and Optimize Your Security Posture from the Foundation

Digital transformation is here, and most businesses are embracing it to stay competitive and relevant to their customers. But it comes with challenges:

- Traditional security approaches no longer work in a cloud-first world.
- Massive numbers of new Internet of Things (IoT) devices are dramatically increasing the attack surface.
- SD-WAN exposes branch offices that directly connect to the Internet to security risks

Add to these issues the ever-changing cyberthreat landscape and the shortage of skilled security professionals (according to a recent ISC2 report, there is a shortage of **2.93 million** security operations personnel worldwide) and your risk of experiencing a potentially disastrous security event expand substantially. What your organization needs for effective threat defense is a solution that provides:

- Visibility into transformative network architectures like SD-WAN, cloud and IoT
- Scalability to protect against breaches and malware in a cost-effective way
- Automation to help respond faster to threats that enter the network by evading perimeter defenses
- A hybrid approach to network security that protects assets and infrastructure anywhere—on-and off-premises— and that integrates tightly with your existing on-premises ecosystems

### CHALLENGES OF A CLOUD-ONLY SECURITY ARCHITECTURE

Cloud-only security solutions:

- Make it difficult to implement threat responses in a way that completely close security gaps. For example, they can't easily share security events with on-premises cybersecurity solutions. The lack of integration results in siloed tools and increasingly costly delays at a time when network attacks are unfolding at everhigher speeds.
- Do not provide timely access to the troves of network data residing in on-premises assets that can help security teams better detect and remediate some of today's most urgent network threats.
- Are unable to ensure protection of remote offices when Internet connections go down.

### CHALLENGES OF A CLOUD-ONLY SECURITY ARCHITECTURE

With BloxOne™ Threat Defense, you get the industry's first hybrid security solution that strengthens and optimizes your security posture from the foundation across all infrastructure environments. The solution maximizes brand protection by securing your existing networks as well as digital imperatives like SD-WAN, IoT and the cloud. It powers security orchestration, automation and response (SOAR) solutions, slashes the time to investigate and remediate cyberthreats, optimizes the performance of the entire security ecosystem and reduces your total cost of enterprise threat defense.

BloxOne Threat Defense uniquely leverages the common denominator that runs your network and makes digital business possible—core network services such as DNS and IP address management. These services make the ideal foundation for security because they are ubiquitous in networks, are close to the endpoints, can accommodate **200 times** more threat indicators than traditional security technologies and are as endlessly scalable as the Internet itself.

## ADVANTAGES OF A HYBRID ARCHITECTURE FOR SECURITY

According to Comport Technology Solutions, the use of hybrid approaches that blend on-premises and cloud infrastructure will become more common because organizations want to take advantage of the cloud without giving up proximity to data residing in on-site infrastructure. For implementing security, the same argument holds true. Cloud architecture provides several advantages, such as being able to scale threat detection and handling big data analytics, while the on-premises components of a hybrid solution can unlock valuable data and context that can be leveraged for response.

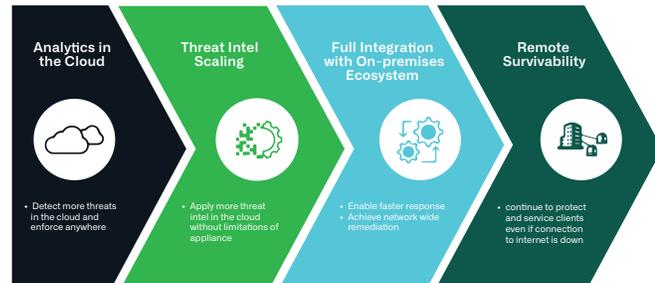


Figure 1: Advantages of Infoblox's hybrid security solution

## INFOBLOX HYBRID APPROACH TO SECURITY OFFERS YOU THE FOLLOWING ADVANTAGES

- **Analytics in the Cloud:** Certain threats like DNS data exfiltration, infiltration and tunneling can evade reputation and signature-based detection methods. To effectively detect these threats requires analytics that combine machine learning and user behavior. The cloud has greater processing capabilities to detect a wider range of threats, including data exfiltration, domain generation algorithm (DGA), fast flux, fileless malware, dictionary DGA and more. Using the hybrid model, this detection can take place in the cloud and enforcement can happen anywhere to protect headquarters, datacenters, remote offices or roaming devices.
- **Threat Intelligence Scaling:** Infoblox threat intelligence includes data from Infoblox research and third-party intelligence providers that is aggregated and curated into one platform. Your organization can apply this highly accurate, comprehensive intelligence to enforce policies on-premises or in the cloud, and automatically distribute it to the rest of the security infrastructure. Moreover, customers can harness more threat intelligence in the cloud without having to make large investments into additional security appliances in every location.
- **Powerful integrations with your security ecosystem:** The hybrid model enables full integration with on-premises Infoblox and third-party security technologies, enabling network-wide remediation and improved ROI of those technologies.
- **Remote survivability and resiliency:** With the Infoblox hybrid model, if there is ever a disruption in your Internet connectivity, the on-premises Infoblox security components will continue to secure clients in the network.

To learn more, please visit: <https://www.infoblox.com/products/bloxone-threat-defense>



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](http://www.infoblox.com)