Infoblox®

SOLUTION NOTE

# Enhance Visibility and Control Using BloxOne® Threat Defense and Azure Active Directory Integration

## OVERVIEW

Depending on where an organization is on its technology journey, networking and security teams often struggle to consistently manage their on-premises and multi-cloud infrastructures. The priority is often to try to find answers to the question: “How can we utilize user identity to secure and detect threats in our on-premises and multi-cloud infrastructures?”

For many years, the answer to this question was to use Active Directory, the foundation for authenticating users and applying security policies based on their permissions or access level. Active Directory is still the first choice within many organizations for storing identity information. Yet as zero trust security strategies have gained currency in today’s work-from-anywhere world, stronger security measures have become necessary. Integrating BloxOne® Threat Defense from Infoblox with your existing Active Directory implementation is the fast, effective way to extend resilient and accurate enterprise security to users and devices regardless of location.

## Challenges

The traditional notion of a perimeter is changing. Access to resources is shifting from *trust based on location in the network* – e.g. internal – to *trust based on identity, which is why today we hear a lot more about perimeterless and zero trust* frameworks. User access and authentication control is the process of determining whether an individual or a system is, in fact, who they declare they are. Digital identity management includes defining and implementing adequate authentication methods based on risk (e.g. passwords, multi-factor authentication, single-sign-on), managing incorrect access attempts, handling forgotten credential requests and ensuring that the identities are secure. Two critical factors to this process are that access be granted only to what’s needed, and that all changes are logged.

Today, many organizations struggle to secure their identity life cycle management and user access control. With inadequate or no identity management strategies in place, access and authentication processes remain manual and decentralized. It’s a situation complicated by movement to the cloud. For IT administrators with thousands of cloud applications to govern, limited visibility into user access processes makes auditing of user events and changes nearly impossible.

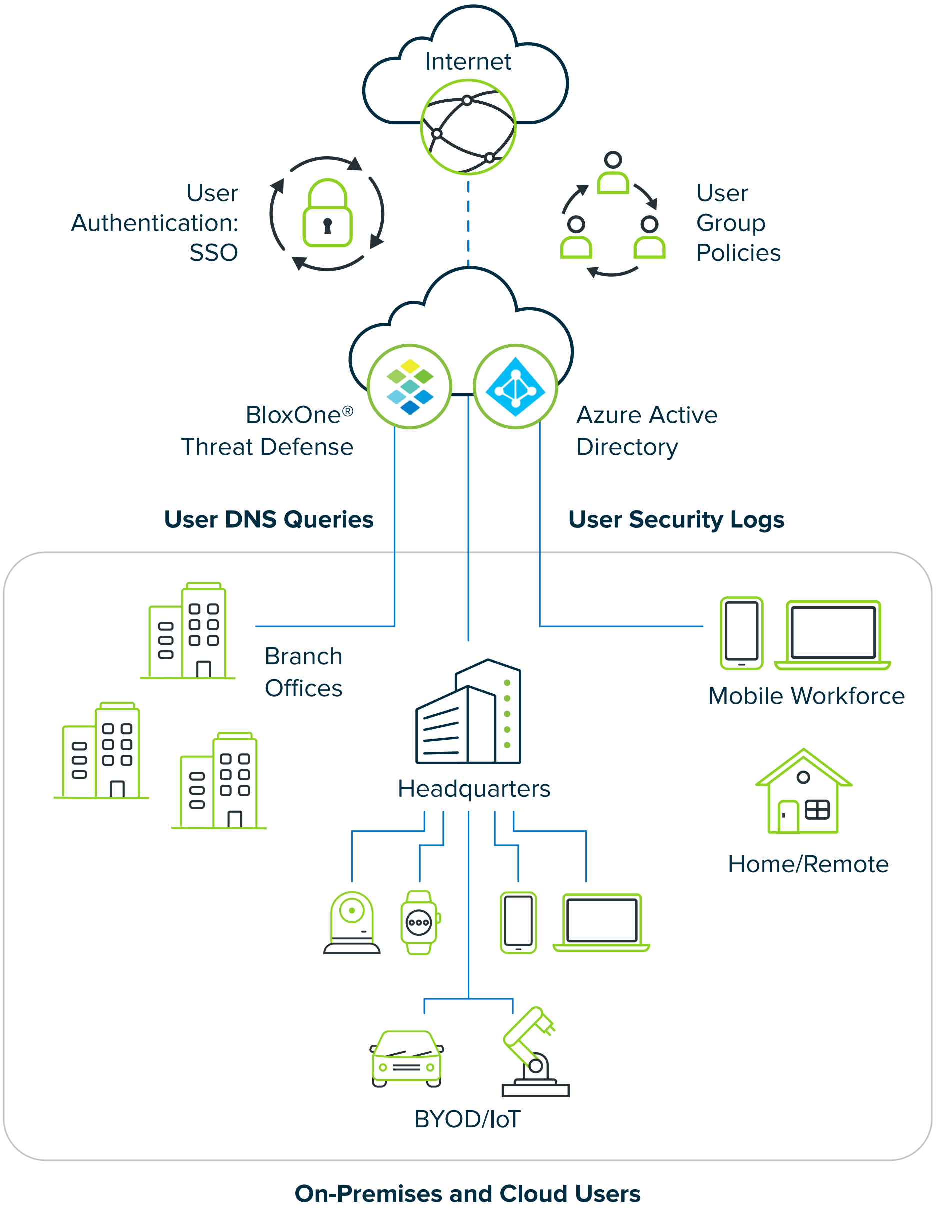
In the absence of well-defined processes, it is more likely that users may have inappropriate or excessive access to systems and services, increasing the risk of unauthorized access/use of systems and data. For instance, limited visibility into user activity can result in delays in detecting when a user accesses a bad domain or performs a malicious activity. This lack of visibility inevitably lengthens remediation because it becomes so difficult to identify compromised hosts, their location or whether the user was on-premises or on the cloud.

Such incidents can result in malicious code being executed or different types of malware interrupting a host's command-and-control server. These types of incidents can compromise privileged accounts, making it easy for the threat vector to gain access to systems and data.

## BloxOne Threat Defense Integration with Azure Active Directory for Better Visibility and Control

Infoblox's joint integration with Azure Active Directory is an effective solution to these challenges. BloxOne Threat Defense from Infoblox seamlessly integrates with Azure Active Directory,  the industry's leading cloud-based identity and access management service. This joint solution makes it possible to authenticate employees using single sign-on (SSO) to login into the BloxOne platform, and provides the capability to create user group policies for Azure Active Directory users that are accessing the internet.

BloxOne Threat Defense integrates Azure Active Directory as an Identity Provider (IdP) to control access to on-premises and cloud network resources through single sign-on. It also provides a unified view of all the users within an organization through Infoblox's BloxOne Cloud Services Portal (CSP).



## Benefits

### Username Identification and Security Policy Management

Connect with Azure Active Directory using SAML 2.0 or OpenID Connect to securely send and receive user authorization credentials, associating users with their network activity. Assign security policies to user groups, restricting access to specific content or blocking access to the open Internet.

### DNS Security and Content Filtering

Centrally manage all aspects of DNS, fortifying security and mitigating evolving threats. With the joint solution, you can support single sign-on authentication of users within Azure Active Directory to access the DNS system. This step allows correlation of DNS queries to a specific username within Azure Active Directory, giving administrators a valuable mechanism for keeping unauthorized users off the network. You'll also gain the flexibility to create custom user group security policies to implement content filtering and block malicious sites to lower the risk of compromise to your organization's network.

### Threat Detection and Remediation

Gain the ability to detect and block malicious user activity with a shortening in remediation timelines by identifying compromised users faster. The security logs and DNS activity reports generated by BloxOne Threat Defense help security team members to achieve superior user control and visibility. The ability to access DNS queries generated by a user, and any security events that were triggered, assists team members in viewing and understanding which user was involved in case of a security event.

## Conclusion

In response to the rising prevalence of cyber threats, and the escalation of cyber risk, many organizations are continuing to focus their efforts on improving essential security controls on their on-premises and cloud infrastructures. With better visibility and control, organizations can more effectively protect their users and networks from cybersecurity threats. The BloxOne Threat Defense joint integration with Azure Active Directory offers superior visibility to detect and block threats, and it helps network and security team members to employ user activity data efficiently to protect users from cybersecurity attacks.

Infoblox

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

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

+1.408.986.4000 | info@infoblox.com | www.infoblox.com