# Infoblox Unveils Simplified Security Platform to Detect and Stop Threats in Today's Borderless Networks

*BloxOne Threat Defense is the industry's first hybrid DNS security solution enabling enterprises to strengthen and optimize their cybersecurity posture from the foundation up*

**SANTA CLARA, Calif., May 30, 2019 —** Infoblox Inc., the leader in Secure Cloud-Managed Network Services, today announced BloxOne Threat Defense, the industry's first hybrid security offering that leverages DNS as the first line of defense to detect and block today's sophisticated cyberthreats. With a scalable hybrid architecture, BloxOne Threat Defense secures enterprises' existing networks as well as digital transformations like cloud, IoT and SD-WAN deployments. It makes an organization's threat analysts more productive and reduces the total cost of enterprise threat defense. Formerly known as Active Trust Cloud, this enhanced solution reduces incident response time by providing actionable intelligence to the organization's security stack, including SOAR (Security Orchestration Automation Response), and by automating action using extensive ecosystem integrations.

Despite organizations utilizing multiple security tools in their stack, only a minimal number of alerts (about 4%) are investigated because they are short staffed. According to the Ponemon Institute, data breaches can take enterprises an average of 196 days to identify, resulting in a loss of $3.6 million per year and impacting brand reputation. Everyday CISOs are challenged to do more with less, simplify their security architecture, improve compliance and ensure protection for their data.

Enterprises require a scalable, simple, and foundational security solution that can catch threats in today's dynamic networks. DNS, critical to the fabric of the internet and any IP based communication, is also the least common denominator that can serve as the perfect foundation for security because it is ubiquitous in networks, is needed for connectivity and can scale to the size of the Internet. BloxOne Threat Defense presents a hybrid deployment that ensures enterprise networks will be protected at anytime, anywhere, leveraging the infrastructure organizations already own - DNS.

Organizations such as Bank Audi s.a.e. need to able to monitor mobile and roaming users connecting to their networks. "Our hybrid DNS security solution from Infoblox allows our team to easily monitor recursive DNS traffic for on-prem or remote users through a single pane of glass," said Moustafa Marzouk, head of IT infrastructure and support at Bank Audi s.a.e. "This allows us to automatically detect and respond to threats in real-time. Now our team can easily integrate with our existing security tools, manage the network from one platform and scale for future growth and innovation."

BloxOne Threat Defense uses highly accurate threat intelligence and machine learning based analytics to detect modern malware, ransomware, phishing, exploit kits, DNS-based data exfiltration, DGA, DNS Messenger, fast-flux attacks and more. In addition, the hybrid approach allows organizations to use the cloud to detect more threats, while providing deep visibility and full integration with the on-premises ecosystem. It also provides resiliency and redundancy.

"The traditional security model is inadequate for today's organizations, especially as they continue to adopt digital transformation technologies like SD WAN, IoT, and cloud," said Kanaiya Vasani, executive vice president of products and corporate development at Infoblox. "With BloxOne Threat Defense, Infoblox is providing customers with a solution that protects everywhere, deploys anywhere, and integrates with the rest of the security stack that is already in place, providing a more optimized and streamlined security posture. Organizations can worry less about silos created by managing multiple security solutions and instead make their security stack work as one fabric."

With BloxOne Threat Defense, Infoblox has further optimized its ActiveTrust Suite, helping customers reduce the total cost of threat defense by:

- **Offloading strained perimeter defenses, like Next Gen Firewalls, IPS and Web Proxies:** Reducing the amount of malicious traffic sent to these solutions by utilizing already-available DNS servers as the first line of defense

- **Reducing incident response time by up to two-thirds:** Automate responses when malicious behavior is detected, block cyberthreats and provide data for the rest of the ecosystem to investigate and remediate.
- **Power SOAR/SIEM platforms and Prioritize response**: Leverage DNS, DHCP and IPAM data in SOAR/SIEM platforms to understand criticality of threats and to prioritize responses accordingly
- **Make threat analysts three times more productive:** Empower security analysts to make quick and accurate decisions while reducing human error with automated threat investigation, insights into related threats, and bad actor and geographical information

To learn more about the BloxOne Threat Defense solution, visit:
https://www.infoblox.com/products/bloxone-threat-defense/

**About Infoblox**
Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability, and automation to cloud and hybrid systems, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500. Learn more at https://www.infoblox.com

**Company Contact:**
Infoblox
Rainer Süßmeier
c/o Regus Munich City
Landsberger Str. 155
80687 München
http://www.infoblox.com