BloxOne Threat Defense

BloxOne™ Threat Defense is Infoblox's hybrid cybersecurity solution that leverages DNS as the first line of defense to detect and block cyber threats. It bundles Infoblox DNS Firewall, Infoblox Threat Insight, Infoblox Threat Intelligence Data Exchange (TIDE), and Infoblox Dossier™. The BloxOne Threat Defense solution combines Infoblox's on-prem (formerly ActiveTrust) and cloud-based (formerly ActiveTrust Cloud) security solutions into an integrated hybrid offering that provides enterprises scale, flexibility, and reliability.

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, Domain Generation Algorithms, 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.

You can deploy the BloxOne Threat Defense suite to proactively protect users everywhere: on-premise, roaming, and in remote offices or branches from cyber attacks. The solution automatically stops device communications with C&Cs/botnets and prevents DNS-based data exfiltration. It collects curated threat intelligence data and distributes the verified data to existing security infrastructure to remediate threats and prevent future attacks. It is operationally easy to use, deploy, maintain, and it enables unified policy management.

This section includes the following BloxOne documentation: