Infoblox

BloxOne® Endpoint for the Anywhere Workforce

Extend BloxOne Threat Defense capabilities to laptops and mobile devices everywhere

KEY CAPABILITIES

- **Secure laptops and mobile devices** operating both on and off the network

- **Block malicious QR codes** and other mobile-unique threats

- **View and control online activity** in one place for all devices regardless of their location

- **Counter advanced evasion techniques** abusing DNS to hide threats from other defenses

- **Improve SOC efficiency** with visibility, control, and automation capabilities anywhere workers need to be

- **Leverage 'Safe Search'** options to filter explicit content like pornography and violence

- **Enjoy Maximum Value with Minimal Effort, Friction or Risk** with an easy-to-deploy mobile app or ultra-thin client

Transformations Challenge Security Flexibility

Network and security architectures were forced to adapt as remote work became 'normal' and again to the growing adoption of the hybrid workplace as a long-term reality. At the same time, more work activity has been taking place on mobile devices as those platforms and apps have become more commonplace and capable. So many IT and security teams are struggling to provide the network and security services necessary to support an anywhere, anytime worker while safeguarding sensitive information and other assets.

Unfortunately, VPN and other traditional remote work solutions have failed to deliver the levels of reliability and usability necessary to maintain optimal worker productivity. One survey reported that 59% of network and security leaders could not claim VPN worked well for them.[1] As a result, organizations everywhere are searching for alternative technologies to deliver the reliable, secure, and resilient environment needed for workers to smoothly perform the full range of their responsibilities from anywhere, at any time.

Finding a Solution Within Core Network Services

Both legitimate and malicious activity depend on foundational communications technologies like IP addresses and DNS. Infoblox BloxOne Threat Defense, operating at the DNS layer, can see and detect malicious cyber activity other solutions do not and provide unique control and automation capabilities to mitigate these threats. It collects this DNS activity and can correlate it with additional security and network information to accelerate threat investigation and speed incident response for more efficient Security Operations.

As your organization adapts to important digital or workplace transformations, the BloxOne Endpoint helps ensure worker security and productivity even as where, when, and how they work changes. The consistent protection, extensive visibility, and powerful automation capabilities of the BloxOne Threat Defense solution, extended to off-network PCs and mobile devices through BloxOne Endpoint, can provide greater peace of mind to security teams regarding defensive and incident response capabilities for your anywhere workforce.

Supported Platforms/Operating Systems

The BloxOne Endpoint is available as part of the BloxOne Threat Defense 'Business Cloud' or 'Advanced' license as a single mobile app or ultra-thin client to extend visibility and control to the following platforms:

PC Platforms

Windows:
- Windows 10, 11

Apple:
- MacOS 11.0, 12.0
- Mac with Intel or Apple M1 chip

Managed Google Chromebook OS:
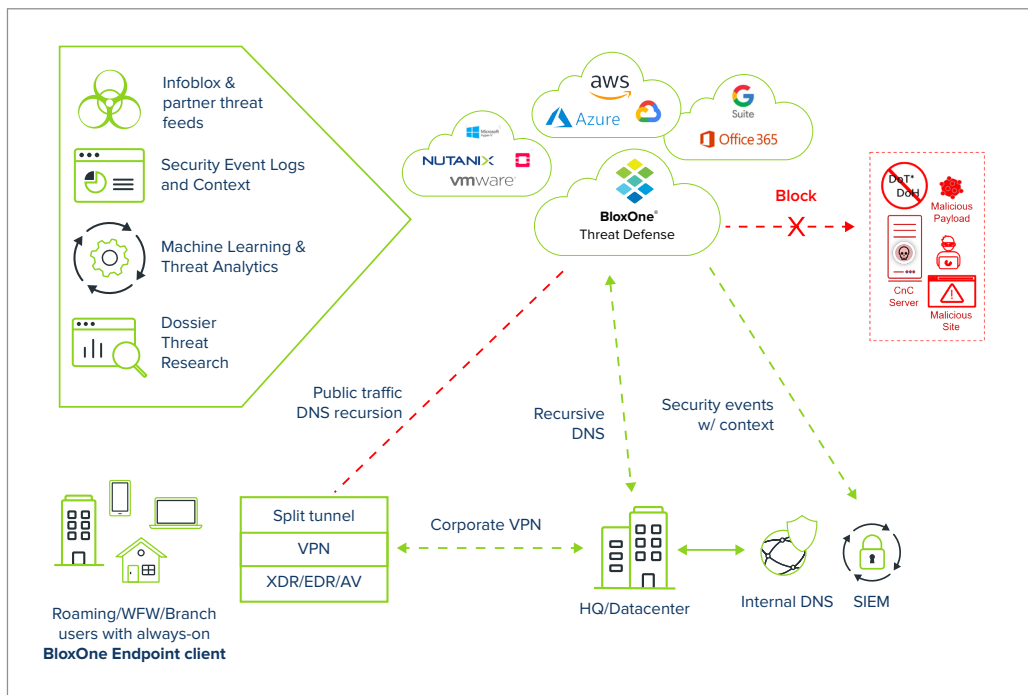- Chrome version 90 or higher

Mobile Device Platforms

iOS:
- iOS 14.X and higher

Android:
- Android 10 and higher

Part of the Overall BloxOne Threat Defense Solution:

To learn more about BloxOne Threat Defense, visit www.infoblox.com/ThreatDefense

[1] Osterman Research survey: "The Global Quest for Sustainable Work-From-Anywhere Security"; 2021, Commissioned by Infoblox