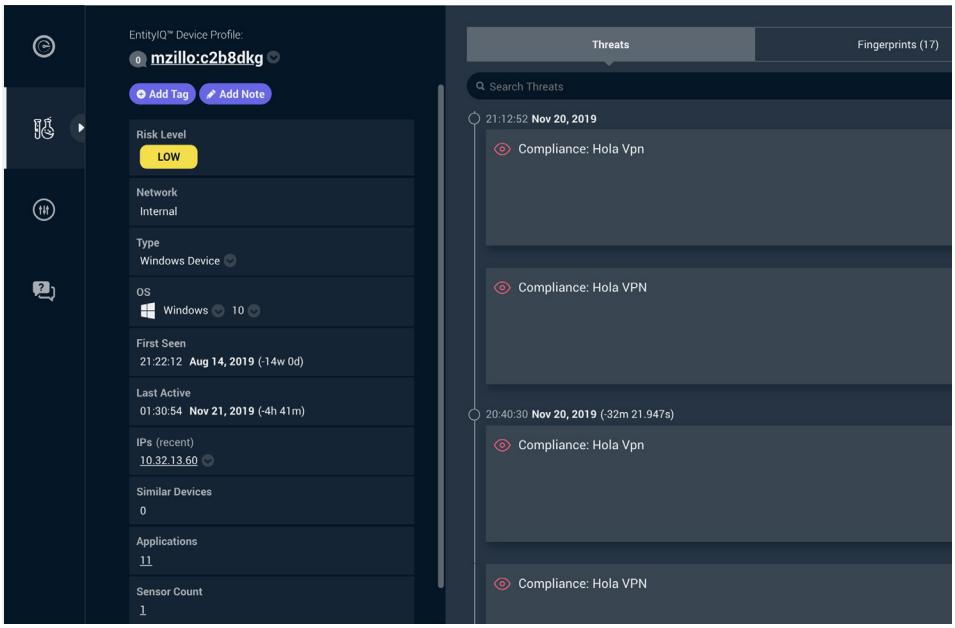
Unauthorized VPN used to hide Data Exfiltration

A senior company executive at a technology firm used a personal laptop computer to access the corporate network. Awake identified the laptop had been compromised using “free” virtual private network (VPN) software. A VPN is typically used to create a secure, encrypted connection to a network. In this case, the free software was actually setting up a peer-to-peer network that has been used by multiple threat actors as a vector for command and control, remote execution and data exfiltration. The executive unwittingly turned their computer into an “exit node” that an attacker could access. What’s more, this circumvented many of the company’s security practices in the process.

Awake highlighted that anyone else on the P2P network could use the processing power of this laptop, and any illicit activity would look like it came from the laptop owner and the company. This specific tool has been used for nefarious purposes such as human trafficking and distribution of child pornography. If an investigation were to occur, such activities could be attributed back to the executive and the company as if they had initiated them.

Awake discovered this situation through an adversarial model looking for VPNs and other remote access tools. The security team was notified, and the software was removed from the laptop.

Traditional security tools might have missed this software because it was on an unmanaged personal device. However, Awake’s network traffic analysis allowed this organization to identify the use of risky software because of the deep analysis of all traffic crossing the organization’s network.



Awake’s EntityIQ™ identifies the personal device and the timeline shows repeated use of the Hola VPN software.

Industry
High-Tech

Attacker Objective
Stealthily exfiltrate corporate data via a senior executive’s device

Awake detected this threat as:

- Risky due to the VPN software’s reputation for nefarious activities.
- Introducing unusual traffic from external sources.
- Unique to a particular device or person when compared to other similar devices or people, such as those in similar job functions.

For additional information about Awake please visit awakesecurity.com

AWAKE