The proliferation of IoT use in business, open BYOD policies, and a global remote workforce exponentially increases the quantity of unmanaged IP-enabled devices directly neighboring enterprise infrastructure. One compromised printer can become an adversary’s home base for reconnaissance, lateral movement, and a breach.

SentinelOne addresses this risk with Ranger, an integral component of our Singularity XDR Platform that turns endpoint Sentinel agents into distributed network sensors. Sentinel Rangers enable control of the enterprise network attack surface in real time by discovering, identifying, and containing any device-based threat. Your endpoints can now autonomously protect compute infrastructure from IoT attacks, compromised devices, and vulnerabilities. No hardware. No network changes. Simply enable Ranger in the endpoint policy and the Sentinel agents get it done.

**Key Benefits**

- Global networked device inventory
- Detect & alert on new devices
- Isolate device-based threats
- Hunt suspicious device activity
- Quantify exposure to Ripple20

**Challenging Problem. Minimal Friction Solution.**

Singularity Ranger is designed to add global network visibility and control in one place with minimal friction. The Ranger solution is part of our Sentinel agent. Just toggle it on. Ranger eliminates the need for additional specialty agents, SPAN and TAP ports, and network gear dedicated to network visibility. Plus forget about tedious manual traffic capture and upload for analysis. Ranger makes it automatic.

**Ranger gives exceptional visibility where we had none.**

Security Architect
Global Services, 10B - 25B USD
Proactive Attack Surface Control

SentinelOne’s Singularity platform delivers cloud managed distributed intelligence. Our differentiated endpoint protection, endpoint detection and response, cloud workload security, and IT operations capabilities consolidate multiple existing technologies into one solution. Singularity Ranger adds network and IoT control to the mix within the same agent. Ranger is designed to address customer requirements like these:

- Monitor changes to configuration management database (CMDB) in real-time
- Investigate devices and device activity
- Pivot from a suspicious device and hunt lateral movement activity
- Isolate device-based threats with 1-Click
- Identify gaps in SentinelOne deployment coverage

Rogues and Ranger® are both built into the agent. The capabilities differ based on the purchased license level. Rogues is included in the Singularity Complete and Singularity Control product bundles. Ranger is an add-on product with multiple added network visibility and control capabilities.