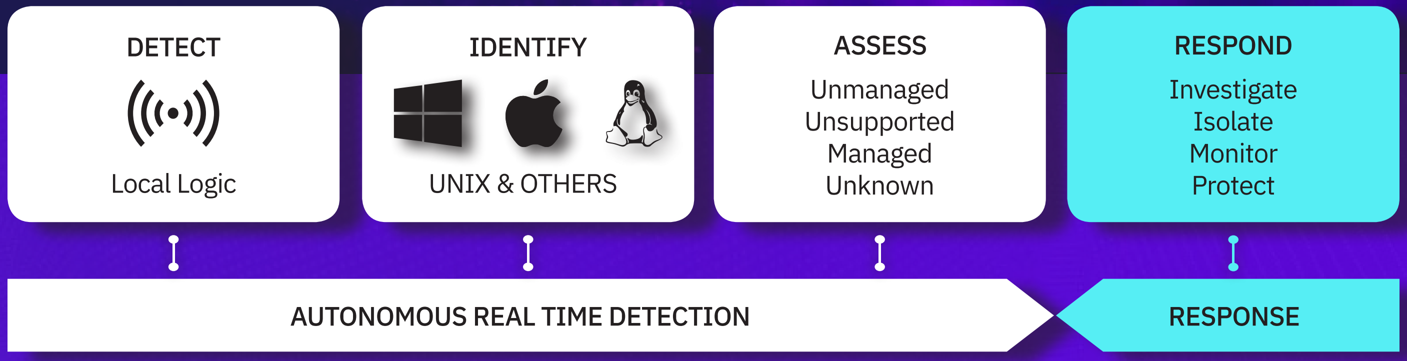
SentinelOne™

SentinelOne Ranger

IoT Detection and Response

Introducing the industry's first solution that turns every protected endpoint into a network of sensors, capable of identifying and defending against any IoT and connected device threat. Endpoints can now autonomously protect each other against vulnerabilities, rogue devices, and anomalous behaviour across your network.

Ranger IoT Detection & Response How it Works


DETECT

Local Logic

IDENTIFY

UNIX & OTHERS

ASSESS

Unmanaged
Unsupported
Managed
Unknown

RESPOND

Investigate
Isolate
Monitor
Protect

AUTONOMOUS REAL TIME DETECTION

RESPONSE

Critical Challenge

IoT devices, smart devices and industrial control, delivers business growth and profitability, but there is no real way to secure them using traditional means. The increasing demands of employees, customers and suppliers to access your network and data from smart devices plus the need for this data to be at the edge of networks is exponentially increasing the potential impact. These devices often fly under the radar of your traditional control, device security, vulnerability management and IT hygiene.

These always-on devices can result in attackers having 24x7 ability to gain a foothold, conduct reconnaissance and move laterally within your network. The speed and ease with which these devices can be connected is what makes them a major, often hidden, security hazard offering significant vulnerabilities ripe for exploiting.

Currently, enterprise security teams lack the ability to deploy software onto these fragmented devices, resulting in a complete lack of environmental awareness and ability to take accurate network inventory. Gaining this awareness and inventory through manual processes is simply impossible.

Innovative Solution

SentinelOne Ranger solves this critical problem by giving your machines the ability to discover and protect other machines, enabling them to become environmentally aware and fend off attacks from one another, without human intervention.

Using AI to monitor and control access to every IoT device, SentinelOne allows machines to solve a problem that has been previously impossible to address at scale. Our technology enables complete environment visibility by fingerprinting and profiling devices that it discovers. SentinelOne's Ranger is the industry's first solution that allows machines to autonomously protect and notify security teams of vulnerabilities, rogue devices, and anomalous behaviour.

Endpoint, network and application risk management from one cloud console

KEY BENEFITS

- Automatically generate and maintain live device asset inventory
- Ensure every device joining your network is protected with a few clicks
- Fingerprint operating systems and device configuration
- No additional agents to install
- No physical network appliances or redirecting traffic
- No manual traffic capture or upload of logs for processing

3 Options aligned to your needs

Know your network, investigate unmanaged devices, and hunt rogue devices.

	Core + Ranger*	Control + Ranger	Complete + Ranger
Hunt Rogue Devices in Deep Visibility			✓
Investigate Network Activity in Deep Visibility			✓
Reduce Attack Surface with Device & Firewall Controls		✓	✓
Isolate Rogue Devices from Managed Network		✓	✓
Manage IT Hygiene with Enterprise Inventory		✓	✓
Know Your Network from your SentinelOne cloud console	✓	✓	✓
Gain Visibility Enterprise-wide from Intelligent Scanning	✓	✓	✓
Discover IoT & Rogue Devices cloud delivered from SentinelOne	✓	✓	✓

OUR MISSION

Our mission is to enable enterprises to most effectively and efficiently manage risk. We implicitly acknowledge that security teams have to do more with fewer people while constantly stay ahead of the evolving threat landscape. These realities define our design principles; we're just getting started transforming endpoint security and beyond!

READY FOR A DEMO? Visit the SentinelOne website for more details.