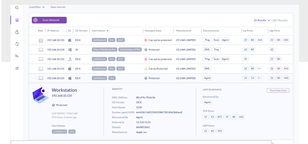

SentinelOne Ranger (IoT) – Technology Preview

March 6, 2019
By Caleb Fenton

Ranger creates visibility into your network by using distributed passive and active mapping techniques to discover running services, unmanaged devices, and vulnerabilities.

Why Does Enterprise Need This?

The number of devices running on networks is increasing as people bring their personal phones, laptops, and smart devices into the workplace. Adding to the network. All these devices are becoming increasingly intelligent and complex. This complexity can lead to bugs, and bugs can lead to vulnerabilities that network. Ranger generates this inventory automatically and maintains itself over time.

Ranger also makes it easy to find unmanaged endpoints. You want to make sure every device joining your network is protected, but this can be tricky clicks away.

How Does Ranger Work?

Ranger turns existing SentinelOne agents into a distributed sensor network which combines passive and active reconnaissance techniques to build

Since it's not enough to simply know you have a device on your network, Ranger also tries to fingerprint the operating system and the device's role. us to be very confident when we say an endpoint is unmanaged because we won't be alerting on incompatible devices such as VoIP devices, IP cam

It's well known that Firewalls and IDS systems respond poorly to normal network and vulnerability scanning attempts, and many IoT devices cannc techniques are quite good at finding all hosts on the same subnet as our agents. Second, we don't use a single endpoint to do all of the mapping — our probes are incredibly lightweight. Nmap takes 10s to 20s more traffic and Nessus requires 120s to 500s! This is because our probes are very s

What We Tried

There's no general solution for scanning networks. Each one is a unique snowflake and can be arbitrarily complex. Because of this, we wanted to tr it was key to leverage existing agent deployments. It's so hard and expensive for large enterprises to roll out a new agent, and many enterprises are

Before we had an agent built, we experimented by modifying our network to redirect all traffic through a Suricata tap. The benefit of this was that it amount of traffic was overwhelming the Suricata box, even on a small network. We could also see endpoints which talked with the internet. Ev

The next difficulty we had was deciding how to prioritize implementing passive and active network mapping techniques. There are thousands of po the most informative and implementing the protocols which were the most useful.

How Is Ranger Different?

The main difference is that we use our existing agents as sensors. This means you don't have to install yet another agent for Ranger to work.

Other products on the market require adding physical appliances to the network and directing traffic there. This can be annoying to scale especially

Some products require you to capture the traffic yourself and upload the logs to a server for processing. This is probably the easiest solution to imp have many different sites and networks, you'll have to monitor traffic at all of them.

Conclusion

Ranger gives you a window into your network, and this will be increasingly important and valuable as more devices start living on the network. And

SentinelOne Ranger is now in alpha and expected to be available to all our customers during summer 2019.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- SentinelOne's Product Journey – A Year in Review
- PowerQuery Brings New Data Analytics Capabilities to Singularity XDR
- Mobile Threat Defense | Bringing AI-Powered Endpoint Security To Your Mobile Devices
- Rapid Response with XDR One-Click Remediations
- Feature Spotlight | Introducing Singularity Dark Mode
- Introducing the New Singularity XDR Process Graph