SentinelOne™

SentinelOne Ranger (IoT)

Autonomous Endpoint Protection That Saves You Time

WHAT IS SENTINELONE RANGER

Turning every protected endpoint into a network detection device capable of identifying and controlling every IoT and connected device on a network. Converging EPP and EDR into a proprietary single agent architecture, SentinelOne is the first and only cybersecurity vendor to expand into the IoT space with the same single codebase and deployment model.

By 2030, there are expected to be more than 125 billion connected IoT devices, many with little or no built-in security capabilities. Furthermore, the devices being added to enterprise networks grow more intelligent by the day – from TVs to toasters to wearable trackers. The result is more code running on more devices, dramatically expanding the number of potential vulnerabilities for attackers to target. 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.

SentinelOne Ranger solves this critical problem by giving machines the ability to detect 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. The technology can not only fingerprint and profile devices the SentinelOne agent discovers from enabling complete environment visibility, but can also identify if any aspect of that environment is dangerous. SentinelOne's Ranger technology is the industry's first solution that allows machines to autonomously protect and notify security teams of vulnerabilities, rogue devices, and anomalous behavior.

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!

FOR MORE INFORMATION ON SENTINELONE, VISIT WWW.SENTINELONE.COM.

SentinelOne™

www. sentinelone.com • sales@sentinelone.com

+1-855-868-3733 605 Fairchild Dr, Mountain View, CA 94043

Why Does Enterprise Need Ranger?

The number of devices running on networks is increasing as people bring their personal phones, laptops, and smart devices into the workplace. Additionally, more and more Internet of Things (IoT), Operational Technology (OT), and smart appliances are being added to the network. All these devices are becoming increasingly intelligent and complex. This complexity can lead to bugs, and bugs can lead to vulnerabilities. This means it's increasingly important for network administrators to have a way of keeping inventory of what's on their 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 with an increasing number of devices and limited IT personnel. With Ranger, a list of unmanaged endpoints is just a few 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 a map of everything on the network.

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. This means you can easily look at all of your printers, mobile devices, Linux servers, and so on. Fingerprinting also allows 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 cameras, printers, and so on.

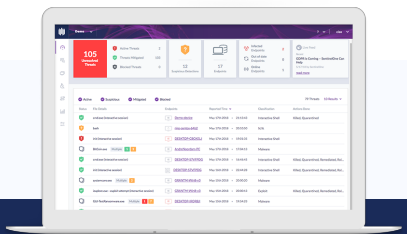
It's well known that Firewalls and IDS systems respond poorly to normal network and vulnerability scanning attempts, and many IoT devices cannot handle the strain of being scanned normally. We deal with this problem in a variety of ways. First, our passive techniques are quite good at finding all hosts on the same subnet as our agents. Second, we don't use a single endpoint to do all of the mapping — the work is intelligently divided amongst all agents. This means no one particular endpoint is noisy or suspicious. Finally, our probes are incredibly lightweight. Nmap takes 10x to 20x more traffic and Nessus requires 100x to 500x! This is because our probes are very targeted and precise.

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 for large and busy networks.

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 implement, but it puts a heavy burden on the user to collect enough information to get a clear view of the network. If you have many different sites and networks, you'll have to monitor traffic at all of them.



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

SentinelOne™

www. sentinelone.com • sales@sentinelone.com

+1-855-868-3733 605 Fairchild Dr, Mountain View, CA 94043