**Reference**[**https://www.infosecurity-magazine.com/opinions/active-passive-scanning/**](https://www.infosecurity-magazine.com/opinions/active-passive-scanning/)

**Advantages and Disadvantages of Active vs. Passive Scanning in IT and OT Environments**



[Chris Sherry](https://www.infosecurity-magazine.com/profile/chris-sherry/) Regional Vice President EMEA, Forescout

The bringing together of IT and OT on business networks is often promoted as a key part of the digital transformation process. Remote maintenance, faster production cycles, shorter supply chains and, above all, quicker progression from prototype development through to end-product production are just some of the advantages.

Couple this with the introduction of 5G, and production processes will be faster and more interconnected than ever before.

However, along with its numerous benefits, connecting IT and OT technology can also have its drawbacks, especially when considering cybersecurity and fail-safety. The result of more connected devices is that there is also a higher volume of access points to the network and therefore more potential attack vectors for bad actors. There are numerous technologies that detect dangers in OT networks, but many fail because they cannot keep up with the ongoing push from OT engineers' to achieve the most uninterrupted operation.

In the worst-case scenario, the supposed ‘defenses’ can even create further risks. The question, therefore, must be: how can companies effectively scan for security risks across their network and what technologies can enable this? The primary two methods for scanning for dangers to security integrity of a network are active and passive scanning, but the two have vital differences. These can be the defining factor between being victim to a cyber-attack and identifying a threat quickly enough to secure a network.

**Threats for industrial control systems like EKANS, Industroyer and others**  
Before exploring the different types of scanning, it is important to understand why organizations need to scan the OT environment in the first place. A recently discovered Trojan horse that targets exactly these environments is [EKANS](https://malware.wikia.org/wiki/Ekans). It is specifically designed for industrial control systems and their software and hardware, which is used in all areas of the industrial landscape - from oil refineries to power grids and production plants.

Similar to other ransom demands, EKANS encrypts data and displays a note to the victims requesting payment for the release, but EKANS can do much more: it is designed to terminate 64 different software processes on the victims' computers. Among them are many that are specific to industrial control systems. It can then encrypt the data with which these control system programs interact.

Compared to other malware designed specifically for industrial sabotage, this is a major blow to software used to monitor critical infrastructure, such as the valves and drivers on an oil rig. This can have dangerous consequences.  If, for example, remote monitoring is no longer possible, machines could be permanently damaged in the event of a malfunction, resulting not only in high costs but also in environmental hazards.

Several years ago the[Industroyer](https://en.wikipedia.org/wiki/Industroyer) ransomware was discovered, which also targets these machines. In order to detect such dangers quickly and to initiate countermeasures, it is therefore pivotal to carry out both passive and active scanning in OT environments to limit these dangers and identify them as soon as possible.

**What is active scanning?**  
Active scanning of an environment, whether IT or OT, is one of the most important measures in cybersecurity. It is especially important to get an overview of the ongoing processes and to check the "health" of online systems. Important information can often only be found out through active requests and cannot be found in normal data traffic or automatically transmitted sent by the system.

Active scanning works by sending test traffic into the network and querying individual endpoints. Active monitoring can be very effective in collecting basic profile information such as device name, IP address, NetFlow or Syslog data, as well as more detailed configuration information such as make and model, firmware versions, installed software/versions and operating system patch levels.

By sending packets directly to endpoints, active scanning can accelerate data collection. However, this increases the risk of malfunctioning endpoints by sending incompatible queries or saturating smaller networks with high volumes of traffic. Furthermore, active scanning does not normally monitor the network 24 hours a day, so it may not detect temporary endpoints or listen-only devices.

Disadvantages of active scanning arise more often when applied to OT environments. These systems, especially the control software, are often not prepared to perform their tasks while receiving and returning traffic. The danger that the controllers become overloaded with signals and no longer know what their actual task is.

Many of these systems are proprietary and therefore react more sensitively to external influences. For this reason, passive scans are more likely to be the go-to scanning method performed in OT environments.

**What is passive scanning?**  
A passive scan silently analyses network traffic to identify endpoints and traffic patterns. It does not generate additional network traffic and carries almost no risk of disrupting critical processes by interacting directly with the endpoints.

However, passive monitoring may require more time to collect asset data because it must wait for network traffic to or from each asset to generate a complete profile. In some cases, not all areas of the network are available, which can limit the ability to passively monitor traffic across the entire OT environment.

Nevertheless, active scans should be performed from time to time. Certain preparations must be made, however, to avoid failures or even physical damage to ICSs. Such scans are best performed when the machinery and production lines are at a standstill. This is because even if only latency periods occur, there is no guarantee that other problems will not.

Solutions for detecting and monitoring OT environments now combine both active and passive scanning technologies. They allow OT teams to achieve greater transparency in their ICS environments. They enable them to use the right approach for each subsystem.

The solutions must also ensure that the risk of interruption is reduced to zero if possible. One example of such a risk is an endpoint malfunction caused by passive monitoring of the network. However, a countermeasure to this and other similar issues is that passive scanning has the ability to limit the number of simultaneous queries to avoid overloading lower bandwidth OT networks.

**Winning combination**  
More and more IT organizations have to face the challenge of securing not only the IT environment but also the industrial internet of things. Utilizing both active and passive scanning together is important to gain an overview of the processes in the OT environments and to stop threats such as EKANS or Industroyer at an early stage.

With this, it is important to be aware of the consequences of the different types of scanning in order to make the most informed decision of which to use and when.

Active scanning should therefore only be carried out temporarily or in an extreme case to avoid production downtimes or disruptions. Passive scanning offers a lower chance of disruption but does not provide the same results. For this reason, companies need solutions that combine both and have enough experience with OT environments to know when best to use each.