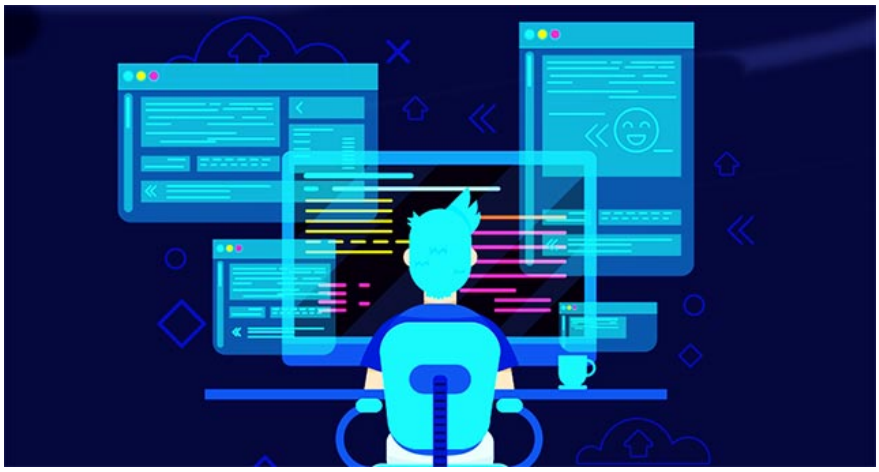
Endpoint Detection and Response threats, an emerging security technology

Endpoint Threat Detection and Response (ETDR) is a term first introduced by security expert Anton Chuvakin from Gartner in 2013 to refer to The tools mainly focus on detecting and investigating suspicious activities (as well as traces of other phenomena that don't always happen) on the server or endpoint.

Endpoint Threat Detection and Response (ETDR) is a term first introduced by security expert Anton Chuvakin from Gartner in 2013 to refer to The tools mainly focus on detecting and investigating suspicious activities (as well as traces of certain phenomena that don't happen often) on the server or endpoint. This is a relatively new type of endpoint security solution, you often find references to Endpoint Detection and Response (EDR) (often compared to threat protection). Advanced Threat Protection (ATP) when talking about overall security.



1. Fileless malware - Achilles heel of traditional antivirus software

In general, the answer 'has the most weight' for addressing the need for continuous monitoring and response to advanced threats is Endpoint detection. So what is the endpoint detection and threat response really? We will find out later.

How does ETDR work?

Basically, ETDR works by monitoring the endpoints and network events taking place in the central database, and recording all the information needed to serve the future analysis process. . In addition, on the server system, a software agent will be installed as the foundation for reporting and monitoring events.

1. Top 5 trends in endpoint security for 2018

An appropriate analytical tool will facilitate continuous monitoring and detection of abnormal signals on the network. Specifically, it helps identify tasks that can enhance overall security through alerting and deflecting common threats, and at the same time allowing users to identify risks early. in case of any attack towards the system. Being able to produce a quick response is a huge advantage at all 'fronts' when it comes to endpoint security issues, even if threats originate from an internal source in the system. network.

ETDR is not just a tool

While security researcher Anton Chuvakin introduces the term Endpoint Detection and Response to indicate tools that focus primarily on detecting and investigating suspicious activities on the system and terminology. This can also be used to describe hidden capabilities in a security tool with a much larger scope and scope of impact. For example, think of a tool that can provide application control, data encryption, device control and encryption, privileged user control, network access control, etc.

1. Learn about terminal security (endpoint security)

Anton Chuvakin has named a number of cases using the ability to display endpoints with a larger scale, that is:

1. Data search (Data search)
2. Suspect suspicious actions (Suspicious)
3. Data exploration (Data exploration)

Most endpoint detection and feedback tools solve feedback through sophisticated analysis processes, which help detect anomalies, such as unrecognized connections, or find out risk activities based on basic comparison. This process can be automated, combined with triggering alerts for immediate action or subsequent action, but many endpoint detection and feedback tools also allow security experts. conduct manual data analysis. Endpoint detection and feedback is still in its infancy, but it can be said that this technology has a complete potential to become one of the essential elements of enterprise security solutions in general and endpoint security in particular. The benefits brought about by the continuous visibility of events, unusual behavior in all data operations, detection and feedback of end points is a very urgent need for businesses - those who inherently need to be protected against ever more advanced threats.

1. What can organizations do to protect themselves from cyber attacks?