SANGFOR XDDR WHITEPAPER

Why XDR is Not Enough

www.sangfor.com

SANGFOR

What is XDR? 01

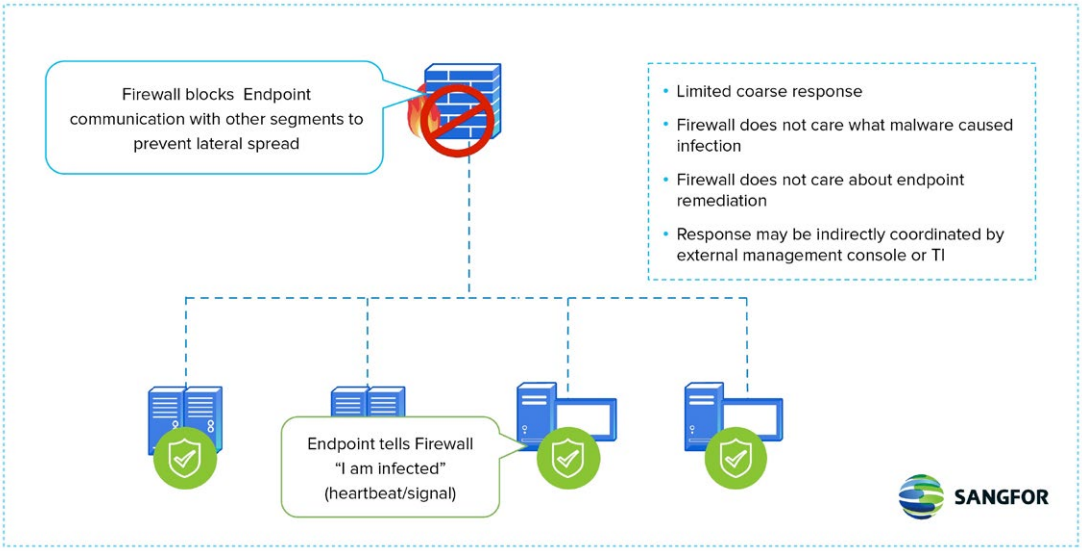
One of the latest trends in cybersecurity is Extended Detection and Response, more commonly known as XDR. Although originally defined by Palo Alto Networks as a key capability, other security vendors have released some type of XDR functionality and of course all define and approach it differently. Gartner defines XDR as "...a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components." Oddly, that sounds a lot like Security Information Event Management (SIEM) with the addition of response capability. And that is the key point. Unlike SIEM, XDR does not only identify an incident, but it also has an automated response to it.

Most vendors with XDR are promoting integrating their security products together to build a more coordinated response. The reality is most XDR tries to integrate endpoints and networks together using endpoint detection and response (EDR) and next generation network firewalls (NGFW); the idea being EDR can tell the firewall what to block, such as malware command & control (C&C) communications.

Why XDR is Not Enough 02

So, as grand as the concept of XDR is, it is rather limited for several reasons:

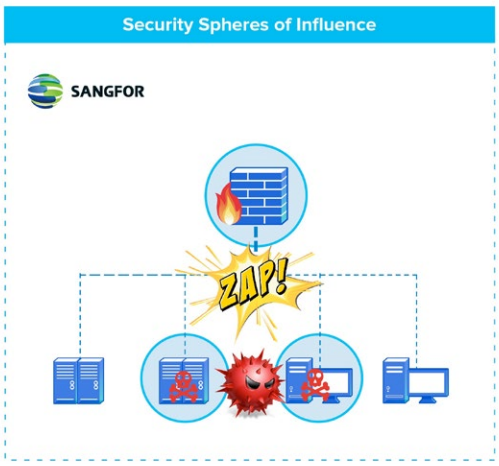
• **XDR is usually one way:** In most XDR solutions, the EDR can send information to the firewall to trigger a response but the firewall does not normally send information to the endpoint to respond to a threat. For example, and endpoint can tell the firewall it is infected by malware and the firewall can block all communications from that endpoint. But the firewall, when seeing suspicious traffic, cannot ask the endpoint to run a scan to see if it is infected.



• **XDR response is not granular:** Normally, EDR will tell the firewall that the endpoint is infected. But what malware was detected or what ports the malware uses for C&C are not communicated. So, the firewall will block all communications from the endpoint, effectively isolating it from other network segments or the internet. But that would not be good if the endpoint were an ecommerce server generating revenue.

• **Response time slowed due to indirect communications:** As exciting as integrating EDR and NGFWs together sounds, the EDR and NGFW may not directly communicate with each other. Instead, communications and response instructions are routed through a management or threat intelligence (TI) platform. This indirect communications could impact how long it takes for a response to be initiated.

• **XDR does not close gaps between products:** All security products have a sphere of influence or area domain that they protect. NGFWs protect communications between networks. EDR protects endpoint from malware. But malware is becoming more sophisticated and can exploit the gaps in coverage between networks and endpoints.

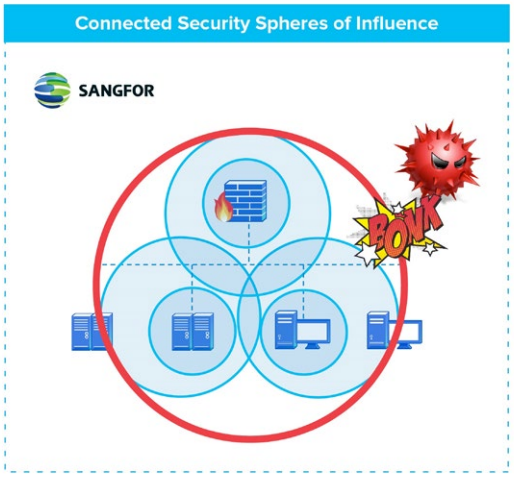


Ransomware is a prime example of malware that can defeat XDR. To date ransomware is the most successful malware to breach, infect and attack data in organizations of every kind all around the world. And every organization infected by ransomware had some type of EDR and NGFW.

The ransomware attack in Sept 2020 at Saraburi Hospital illustrates this. The attack made all online patient data unavailable and patients were asked to bring in copies of their medical records and prescriptions during treatment.

Adding Another 'D' to XDR

03

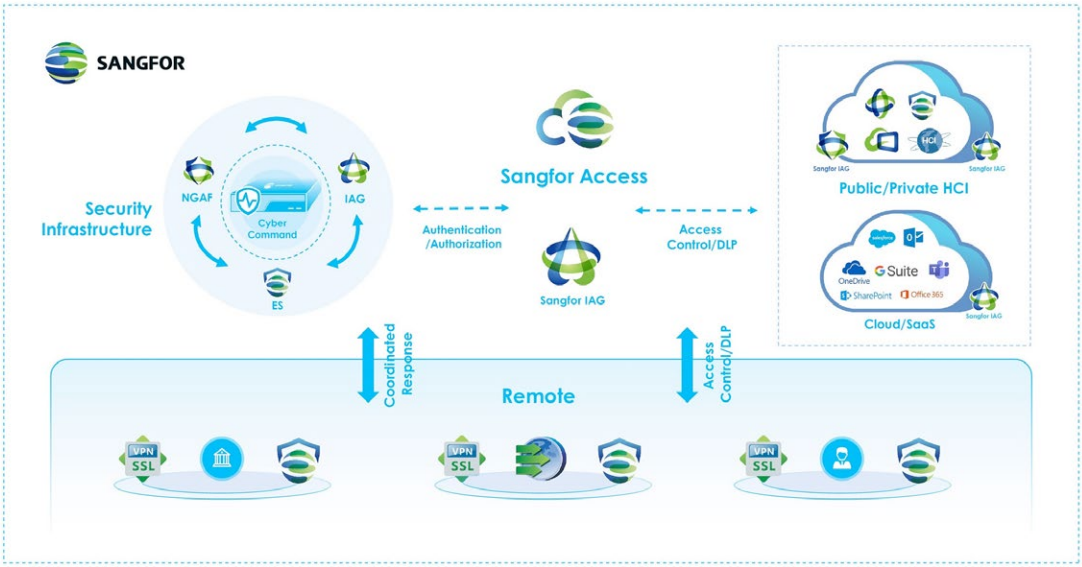


XDR as currently available is not enough. Better synergy between security products is needed to defend against upcoming AI enable malware. One way to improve synergy is to extend the spheres of influence of security products to close the gaps malware like ransomware can exploit. Enabling bi-directional direct communications between products creating closed feedback loops to better identify and more quickly defend and respond to threats is a must.

Extending the spheres of influence for all products within an organization is important as customers have security solutions from more than one vendor and many really do not integrate well on their own.

Sangfor's Award Winning XDDR Security Framework 04

Sangfor's award winning eXtended Detection, Defense & Response (XDDR) strategy has implemented direct bi-directional communications long before XDR. And bi-directional communications are not just between the Sangfor NGAF network firewall and Endpoint Secure endpoint protection, but across all Sangfor security and cloud product lines. XDDR extends threat response beyond Sangfor products using the Cyber Command threat detection platform to integrate 3rd-party products.



Cyber Command correlates SIEM events, network traffic flow data, and endpoint protection data giving a 360-degree view of threats and risks in an organization. Multiple advanced AI models, cloud sandboxing, and direct response orchestration all contribute to XDDR's enhanced ability to coordinate and automate threat response across all products integrated into XDDR delivering true layered defense-in-depth even in hybrid cloud environments.

About Sangfor Technologies 05

Sangfor Technologies is an APAC-based, global leading vendor of IT infrastructure solutions specializing in Network Security and Cloud Computing with a wide range of products & services including Next-Generation Firewall, Internet Access Gateway, Endpoint Protection, Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, SASE, SD-WAN, and many others.

Sangfor takes customers' business needs and user experience seriously, placing them at the heart of our corporate strategy. Constant innovation and commitment to creating value for our customers help them achieve sustainable growth. Established in 2000, Sangfor currently has 7,500 + employees with more than 60 branch offices globally in exciting locations like Hong Kong, Malaysia, Thailand, Indonesia, Singapore, Philippines, Vietnam, Myanmar, Pakistan, UAE, Italy, etc.

Visit us at www.sangfor.com or send us an email to marketing@sangfor.com to learn more about Sangfor's Security solutions, and let Sangfor make your IT simpler, more secure and valuable.