MAPPING OUT THE CRITICAL ELEMENTS OF NEXT-GENERATION ENTERPRISE ENDPOINT PROTECTION

Before setting out to compare any two endpoint protection strategies, it's instructive to understand the key functional components required in protecting a mix of endpoint devices across today's major threat vectors, from attack inception to full containment and remediation.

From the endpoint device perspective, the threat execution lifecycle can be divided into three phases: *pre-execution, on execution and post-execution*.

PRE-EXECUTION: STATIC PREVENTION, WHITELISTING AND BLACKLISTING

Any file-based malware can be prevented from executing on a target endpoint device—provided that the attack code has been previously detected and can be identified upfront as a known threat. This is the essence of legacy antivirus software; its ability to block known threats from executing by directly matching a threat to signatures that exist within the antivirus software's management layer.

More recently, organizations have begun supplementing the shortcomings of their antivirus software by deploying whitelisting and blacklisting technology as an additional layer of protection. These techniques combine to form a brute force method of gating which applications are allowed to run on a particular endpoint device. This form of prevention is an effective means of significantly shrinking the organization's overall attack surface, and makes hackers and cybercriminals work harder (and spend more money) to penetrate the organization's IT infrastructure via the endpoint.

By today's standards, pre-execution protection should be considered table stakes for any approach to securing the endpoint.

ON EXECUTION: DYNAMIC DETECTION OF ADVANCED MALWARE AND EXPLOITS

The execution phase is where an unknown threat (often a carefully wrapped or altered variant of a known threat) escapes initial detection and begins to execute on the endpoint device. It is during execution where continuous analysis of system activity is performed in order to identify malicious behavior. Detection of advanced malware and exploits by dynamic methods was first pioneered by network-based sandbox technologies which emulate endpoints and execute suspicious content with the goal of trying to identify new, never-before-seen, threats. As new threats are detected, signatures are created and distributed to the perimeter firewall with the hopes that they can be blocked during pre-execution from that point forward.

Increasingly organizations are adding new, behavior-based endpoint security solutions to prevent advanced threats that aren't detected at the network level. These solutions focus on the real-time identification of malicious behaviors used by malware, exploits and stealthier script-based attacks. This is achieved by monitoring all system level activities from the kernel space on up, forming context to allow for the quick identification and isolation of malicious patterns that are linked to a new threat. These new solutions have proven to be more effective against advanced threats and are increasingly used as a replacement to antivirus.

It is also important to note that the depth and extensiveness of activity monitoring on the endpoint device determines the practicality of any forensics information that can be rendered. This is key ingredient to successful post-execution processes.

POST-EXECUTION: MITIGATION, REMEDIATION AND FORENSIC ANALYSIS

Once an attack successfully executes on one or more endpoints, the organization remains vulnerable until security personnel can fully mitigate it, stopping its lateral spread and eliminating it from affected devices. Many technologies today are focused on identifying and alerting to the existence of a threat. This sends incident response personnel into a scramble, armed with a combination of mitigation and forensics tools and manual procedures through which attempts at finding and quarantining infected systems are made. Sometimes, expert security consultants are called in (at a considerable expense) when internal teams need assistance with mitigation, remediating affected files, or generating and interpreting forensic data. Ultimately, the most effective response is one where attack mitigation and remediation are executed immediately, at the initial point of detection. This is validated through Gartner's Adaptive Security Architecture, and has been adopted by a few pioneers who are integrating detection, prevention and response for a more complete approach.