5 WAYS ENDPOINT SECURITY AND NETWORK SECURITY SHOULD WORK TOGETHER

With network security, no single solution will protect against the variety of threats that organizations face. For more comprehensive protection, a combination of hardware and software provides multiple layers of security to defend the network against various threats. The time, cost and manpower required to carefully select, implement and maintain these tools is a huge investment for any organization. However, those within the network environment will not always be inside the perimeter, and the network protection capabilities will not always apply to them. If endpoints are not protected with the right security solution products, these individuals could bypass the perimeter security and introduce outside threats into the environment. The wrong endpoint security product can undo all of the work that has been done to secure the network.

Below are the five things your endpoint should do to prevent a negative impact on your network security posture:

1. **Integrate threat intelligence natively.**

   According to a recent 2016 Ponemon study, 39 percent of respondents agree that all attacks can be blocked if the organization is engaged in the sharing of threat intelligence.[1] Employing global threat intelligence expands protection capabilities beyond the known knowledge of one solution to the shared intelligence of a global community. When other members of the community encounter new and unique attacks, that information is shared so that all members can automatically detect known threats and quickly identify unknown threats.

   Both the network and the endpoint should participate in threat intelligence sharing, continuously applying growing threat intelligence across the network and endpoints into their own environments. They should also send and receive threat intelligence between each other, so that what is seen and prevented on the endpoint is also seen and prevented on the network.

[1] Source: https://media.paloaltonetworks.com/lp/ponemon/report.html

However, threat intelligence alone is not enough. The majority of organizations that subscribe to intelligence feeds are drowning in data they can't correlate or translate into actionable intelligence. Without the ability to automatically translate threat intelligence into new protections, organizations are just buying more data. The problem gets worse when there is no native integration between the components in an environment to produce and share that threat intelligence. Intelligence that is not natively integrated and cannot be translated into new protections automatically is of little use, unless you throw more people at it. The end result is merely a more people-intensive process of data analysis.

2 **Protect against known and unknown threats.**

Most traditional security products are designed to detect known threats before they enter the organization. In many cases, by the time an unknown threat has been detected, critical assets have already been compromised and detection is too little too late. Additionally, while attackers often reuse existing malware and exploit techniques, they will also make modifications to existing attacks or create entirely new attacks in order to evade detection. This leaves a whole gamut of threats undetectable by the majority of security products.

Detection and remediation on the network or on the endpoint are invariably time-consuming, people-intensive and inefficient. This is a problem that can be avoided if both the network and the endpoint can prevent known and unknown threats. Ideally, your endpoint security solution's prevention capabilities should not rely on signatures, or prior knowledge of an attack or vulnerability, and should incorporate multiple variations of analysis and prevention methods to maximize effectiveness.

3 **Be automated.**

Attackers have automation, scalability and specialized tools at their disposal. In the Ponemon 2016 Economics of a Breach survey, 68 percent of respondents said automated hacking tools make it easier for attackers to execute successful attacks.[1] An entire economy and marketplace has been created to drive the development of these tools at affordable prices.

To defend against the increasingly sophisticated attacks, organizations have point solutions that are often complex and people intensive. Seemingly insufficient, the only way to outpace the attackers is to make successful attacks more challenging and less profitable. The same survey respondents claim that 60 percent of attacks can be deterred if an attack requires an additional 40 hours to conduct[1]. The only way to achieve this in a scalable and sustainable fashion is with automated prevention.

Detection on either network or endpoint is not scalable if a security analyst must be dispatched to investigate alerts. Employing automation makes the organization a more difficult target by delaying the success of an attack, delaying the payout, and causing the attacker to move on to the next potential victim.

4 **Deliver persistent protection.**

Users are increasingly becoming more mobile, connecting to internal resources from points around the globe that are outside the organizational network perimeter. There should be the same level of protection on all endpoints, regardless of their connectivity: online or offline, on- or off-premise. Lack of persistence in these protections will lead to a compromised endpoint, and quite possibly, a compromised network, regardless of network protections already in place. Endpoint security must extend beyond the traditional network perimeter, where many cyberattacks target end users and endpoints, and where the network does not have complete visibility.

5 **Provide full visibility into activity on the network, endpoint and cloud.**

Modern attacks go through multiple steps to achieve their objectives. To successfully prevent an attack, organizations must have full visibility of all users, devices and data across the organization's network, endpoint and the cloud. This visibility is necessary to understand the context of an attack, enforce security policy across both network and endpoint, and correlate security events to improve the organization's security posture. When natively integrated threat intelligence is combined with the automated prevention of known and unknown threats to deliver persistent protection, regardless of connectivity or location, the synergistic effect can dramatically improve an organization's security posture. This will not only make your organization less appealing to opportunistic attackers, but it will also minimize the likelihood of a successful targeted attack.

Choosing the wrong endpoint security solution can leave your endpoints vulnerable to threats and impede, or undo, the significant amount of work that has gone into securing the network. Your endpoint security solution should secure all endpoints continuously, as well as add additional capabilities to other parts of the organization and bolster your network security posture overall. Palo Alto Networks® Traps™ advanced endpoint protection utilizes multi-method prevention, rather than breach detection and incident response, with purpose-built malware and exploit-prevention methods to prevent known and unknown threats. As part of the Palo Alto Networks Next-Generation Security Platform, Traps integrates with WildFire™ cloud-based threat analysis service to automatically convert threat intelligence into malware prevention, preemptively blocking threats before they can compromise an endpoint. Learn more about Traps.