vmware Carbon Black FORRESTER®

Webinar Q&A

- Where do modern endpoint security suites provide visibility that traditional anti-virus (AV) products lack?
- Why should you look for a platform that integrates solutions across your security stack?
- How does next-generation anti-virus (NGAV) solve the problem of slowing down endpoints?
- Why do you need NGAV to prevent emerging attacks?
- How does NGAV solve the problem of long manual definition update processes?
- What are the benefits of a solution that uses use a single agent/console?

Chris Sherman

SENIOR ANALYST
SERVING SECURITY &
RISK PROFESSIONALS

Merrit Maxim

VP, RESEARCH DIRECTOR
SERVING SECURITY & RISK
PROFESSIONALS

Where do modern endpoint security suites provide visibility that traditional anti-virus (AV) products lack?

Traditional endpoint security products focused on detecting and blocking file-based threats before they could cause harm to a system. Over time, this clearly hasn't been enough to protect against more sophisticated, multimodal threats that easily evade signature-based protection measures. IT security professionals relying on older-generation suites generally lacked visibility into threat activity that wasn't associated with a file-based block or alert, such as enumeration of running processes, system activity, interprocess activity, and network activity. Modern suites provide visibility into each of these areas and more, with some solutions extending visibility and analysis over areas such as user behavior and device/OS configuration.

Why should you look for a platform that integrates solutions across your security stack?

Modern endpoint security suites offer integrations between endpoint, network, email, cloud, identity and access controls, and other solutions found in a typical security stack. There are several benefits to such integrations spanning policy integration, analysis, and control. Integrated policies allow for more streamlined policy management when protecting common assets/users. Risk levels are more accurately determined when analysis extends beyond just the endpoint, subsequently improving the accuracy of control measures imposed. Finally, there are several operational benefits with such an approach, such as correlating common endpoint and network traffic deemed potentially malicious in order to improve detection and remediation time.

How does next-generation anti-virus (NGAV) solve the problem of slowing down endpoints?

Whenever a new file or executable is seen, signature-based solutions (traditional AV) must check against a growing list of hashes already deemed malicious in the past. As the list of known-bad grows, efficiency goes down because the memory and compute involved in searching these very large lists of signatures grow. If a cloud lookup is involved, this can further increase the time it takes to conduct a search. In contrast, NGAV solutions go beyond signatures and machine learning to reduce or eliminate the need for time-intensive signature matching, with less dependence on a cloud connection.

Why do you need NGAV to prevent emerging attacks?

NGAV doesn't rely on prior knowledge of a specific indicator or malicious executable in order to identify and block it. As emerging attacks are less likely to have signatures, the effectiveness of traditional signature-based solutions is low for emerging threats. In the past, traditional AV would rely on heuristics and file detonation, which have proven ineffective over time. For new attacks, it's generally accepted that a combination of signatureless threat prevention and detection-oriented behavioral analysis technologies is needed for the highest level of protection against emerging attacks.

How does NGAV solve the problem of long manual definition update processes?

Traditional AV products must be constantly updated in order to give the best chance of stopping known and unknown threats. However, NGAV solutions don't require up-to-date signatures in order to provide their highest levels of potential efficacy. Instead of updating hourly or daily, NGAV solutions can adapt to new attacks dynamically and reduce the traditional AV requirement of having to complete lengthy virus definition processes. In some cases, NGAV solutions may only require monthly updates while still keeping the endpoints protected. Many solutions augment this with additional analysis capabilities both on host and/or in the cloud, but overall NGAV doesn't require as frequent updates to the client. Additional benefits can be gained when the solution is cloud-architected and new features don't require functional updates to be pushed to the client.

What are the benefits of a solution that uses use a single agent/console?

Agent fatigue is frequently cited as a top challenge for many teams. As discussed in the webinar, the average enterprise deals with around six security agents per endpoint. This has prompted many buyers to look for single-agent solutions in order to consolidate their IT and security management workflows associated with multiple agents. Having one console for multiple endpoint security functions improves the general admin experience when trying to orchestrate policies and control measures across different endpoint security functions, such as integrating threat prevention (e.g., NGAV) with threat detection (e.g., endpoint detection and response).