WMC IT Solutions AG
Kägenstrasse 10
CH-4153 Reinach BL 1
Telefon +41 61 716 11 11
Telefax +41 61 716 11 16
www.wmc.ch

Magic Quadrant for Endpoint Protection Platforms

Published: 24 January 2018 ID: G00325704
Analyst(s): Ian McShane, Avivah Litan, Eric Ouellet, Prateek Bhajanka

Summary

Endpoint protection is evolving to address more of Gartner's adaptive security architecture tasks such as hardening, investigation, incident detection, and incident response. Security and risk management leaders should ensure that their EPP vendor evolves fast enough to keep up with modern threats.

Sophos

In March 2017, Sophos acquired Invincea — a Visionary vendor in the 2017 Magic Quadrant for Endpoint Protection Platforms — giving Sophos access to its deep learning ML algorithms.
The Sophos Intercept X product, designed to protect against and recover from the malicious actions related to ransomware and exploits, proved popular with both existing Sophos Endpoint Protection customers and as an augmentation to an incumbent EPP. This momentum continued its increased brand awareness in the enterprise space.
Also included in the Intercept X purchase are Sophos' EDR-like capabilities — called Root Cause Analysis — and the ML malware detection technology from the acquisition of Invincea was added in late 2017.
Sophos' cloud-based EPP with the Intercept-X platform is a good fit for organizations that can take advantage of a cloud-based administration platform, and that value strong protection against ransomware and exploit-based attacks over advanced forensic investigation capabilities.

STRENGTHS

Intercept X clients report strong confidence in not only protecting against most ransomware, but also the ability to roll back the changes made by a ransomware process that escapes protection.
Intercept X is available as a stand-alone agent for organizations that are unable to fully migrate from their incumbent EPP vendor.
The exploit prevention capabilities focus on the tools, techniques and procedures that are common in many modern attacks, such as credential theft through Mimikatz.
The Sophos Central cloud-based administration console can also manage other aspects of the vendor's security platform, from a single console, including disk encryption, server protection, firewall, email and web gateways.
Root Cause Analysis provides a simple workflow for case management and investigation for suspicious or malicious events.
Root Cause Analysis capabilities are available to macOS, along with protection against cryptographic malware.

CAUTIONS

Although we credited Sophos for a cloud-first approach last year, it has now made parts of Intercept X available for on-premises customers. This is likely to hamper cloud adoption and extend the time that Sophos manages and maintains separate protection stacks.
Root Cause Analysis is not available in Intercept X for clients that use the on-premises version of Sophos Endpoint Protection.
Sophos' primary improvement was the integration of Invincea's deep learning technology. Beyond that, there has been little in the way of enhancements to the EDR capabilities of the Sophos Endpoint Protection platform in the last 12 months.
Sophos does not provide vulnerability reporting; rather, it relies on its mitigation and blocking technologies, so organizations will need to find other ways to prioritize their patch management program.

WMC IT Solutions AG
Kägenstrasse 10
CH-4153 Reinach BL 1
Telefon +41 61 716 11 11
Telefax +41 61 716 11 16
www.wmc.ch

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (January 2018)