REPORT REPRINT

Kaspersky highlights its threat intelligence portfolio

MAY 18 2020

By Scott Crawford

The company's investment in threat research has long supported its growth as a worldwide contender in endpoint security. That research has helped build Kaspersky's threat intelligence portfolio into an important contributor to its enterprise strategy, with a set of offerings that seek to augment capabilities for security teams.

Introduction

Kaspersky has long been known as a provider of cybersecurity technologies and a recognized international contender in domains such as anti-malware and endpoint security for many years. Fueling its success in these domains, however, has been an investment in research that has built a significant body of threat intelligence for the company. Today, as Kaspersky broadened its emphasis in enterprise markets from hybrid cloud to industrial cybersecurity and the Internet of Things, it highlights its threat intelligence capability as a primary enabler of its strategy.

451 TAKE

Threat intelligence is a valued capability among enterprises, with 42% of respondents to 451 Research's 2019 Voice of the Enterprise: Information Security, Workloads & Key Projects survey reporting it as already in use, with another 15% reporting projects in pilot or proof of concept and a further 25% planning to deploy over the ensuing 24 months. Kaspersky has achieved significant penetration of global markets, which informs its visibility into geopolitical concerns as well as cybercrime – visibility that can add valuable perspective to threat intelligence, especially when other researchers often speak primarily from North America or western Europe.

With multiple offerings for access to intelligence reports and findings, analysis of samples and exposure of an organization's digital footprint, Kaspersky seeks to put this intelligence more directly to work in security operations. Recent offerings such as CyberTrace highlight this strategy to correlate internal security monitoring and alerting with external threat intelligence, to arm more responsive defense with the insight needed to detect malicious activity, respond to attacks and prioritize risks in light of real-world threats. We would expect Kaspersky to press even further into optimizing security operations, enhancing visibility and action through its combination of widely adopted technologies in multiple environments and its threat intelligence capabilities.

Context

Founded by Eugene Kaspersky and colleagues in 1997, Kaspersky began as an antivirus vendor focused, like many at that time, on the endpoint, and has since grown to become a significant global vendor of security software, operating in 200 countries and territories on six continents. Today, the company's portfolio embraces multiple aspects of security for enterprises as well as SMBs, across a wide range of IT and operational technology (OT) and the Internet of Things.

Established in Russia, the company is now administered through a holding company in the UK, with process and storage of data for North American customers now based in Switzerland. It currently employs more than 4,000 in 34 regional offices worldwide. Privately held with no outside investors, Kaspersky reported audited 2018 revenue of $706m (adjusted for foreign exchange) through both direct sales and a number of OEM relationships.

Threat intelligence gathering and analysis

A provider with a significant presence in endpoint security such as Kaspersky has many advantages others don't. Its agents often number in the millions, deployed on systems around the world in virtually any scenario, from the datacenter to end-user devices. They encounter attack tools and tactics such as malware and exploit techniques on a daily basis. They examine samples to understand threat behavior and activity, and their technology may respond with a combination of heuristics and behavioral analysis to recognize malicious patterns when previously unencountered threats emerge.

Substantial as it is, Kaspersky's endpoint presence represents only a part of its global intelligence-gathering capabilities. Web crawlers, spam traps and 'bot farms' (networks of hosts that interact in honeypot fashion with malicious automated functionality or 'bots') collect data available from attack techniques. Open source intelligence (OSINT) further contributes to inputs. The Kaspersky Cloud Infrastructure supports the gathering and analysis of all this information by human experts and AI. Human analysis is spearheaded by the company's Anti-Malware Research organization and by its Global Research and Analysis Team (GReAT), an elite group of more than 40 experienced researchers in 20 countries tracking more than 200 threat actor groups. Customers and partners can also participate in threat research through the Kaspersky Security Network, a cooperative initiative that allows participants to voluntarily submit contributions and depersonalized data for analysis and obtain findings such as threat detection and reputational analysis deployable in operations.

For the integration of its threat intelligence output with security tools and operations, Kaspersky has partnerships with several IT security and operational technology (OT) providers, including major security information and event management (SIEM) vendors, threat intelligence platforms (TIPs) and network security technologies.

Threat intelligence offerings

Kaspersky's threat intelligence output includes actionable data ranging from machine-readable information to in-depth human analysis and reports. IP reputation, malicious file and content hashes, malicious URLs, vulnerability data, passive DNS findings, command-and-control (C&C or C2) server data, structured indicators of compromise (IoCs) and a widely embraced approve list of legitimate software are among the many types of vetted data Kaspersky provides through its threat intelligence feeds. Additional insights available to premium subscribers include detailed reports on malicious file activities and behaviors, other domains and URLs associated with suspicious files or sites and DNS resolution of suspicious IP addresses. These feeds can be consumed directly by security and IT infrastructure and endpoints, as well as by security operations platforms such as SIEMs.

For enterprise security analysts, the Kaspersky Threat Intelligence Portal is a primary point of access to Kaspersky threat intelligence. With over 20 petabytes of data under management, the portal delivers access to feeds as well as reports that help organizations correlate threat intelligence findings across data sets, answer questions of relevance of findings to their organization, access detailed analysis of threat actors and tactics, understand their exposure to specific threats and act on conclusions and recommendations. Premium subscribers have access to additional details such as the functionality of specific attack tools and the relationships evidence has to other threat intelligence findings. APT Intelligence Reporting details include analysis of methods and tools used in an attack or campaign, technical detail on C&C functionality, IoCs and YARA rules for mitigating attacks. Country- and industry-specific reporting is also available.

Functionality supported by the Kaspersky Threat Intelligence Portal includes the Kaspersky Cloud Sandbox, which enables customers to upload suspicious content for analysis via a web interface. Findings reveal sample behavior and actions initiated by an attack, such as opening additional connections or initiating C&C channels and identifying possible threat actors associated. Premium

access includes the ability to integrate security tools directly via RESTful API, default and advanced settings to optimize performance, intuitive reporting and visualizations, and in-depth analysis of complex or advanced attacks through workflows provided to better manage incidents and handle more complex investigations.

Relevance and actionability are two keywords often used in describing the evolution of threat intelligence in recent years, and two Kaspersky offerings in particular – Kaspersky Digital Footprint Intelligence and Kaspersky CyberTrace – highlight these values.

Kaspersky Digital Footprint Intelligence shows organizations how their information assets – from brand presence and integrity and public information to intellectual property and sensitive data – can introduce exposures to the threat landscape. Through this offering, Kaspersky assesses an organization's digital presence, from online infrastructure and domains to visible corporate content, and correlates findings to its body of threat and vulnerability intelligence. It can identify attacker activity associated with such exposures, from attacks detected against customer assets to information leaks and unauthorized or unintended exposure through social media.

Kaspersky CyberTrace seeks to answer a central question of security operations teams: Do detected events in security monitoring and alerting correspond to known attacker activity? Answers are vital, since they directly indicate the nature of detected actions, and how high a priority they should be given in escalation, response and threat mitigation.

CyberTrace matches log data with evidence in threat intelligence feeds to help security operations centers (SOCs) in a number of ways. It provides connectors for direct integration with many popular SIEM systems, offers a web interface for data visualization and access to findings and is also available in a stand-alone mode for parsing logs and inputs from a variety of security infrastructure and tools. It provides context to tier 1 SOC analysts to help them identify higher-priority events. For escalation, it offers on-demand lookup of indicators for more in-depth investigation. Advanced filtering of feeds enables security teams to tailor correlations to their specific requirements, with bulk scanning of logs supported, and findings exportable to common data formats such as CSV files for ingestion by other systems. Feed usage statistics help organizations better manage their threat intelligence investment. These capabilities help boost SOC analyst expertise while optimizing processes and reducing workloads for data correlation and event management.

Customers can access Kaspersky threat intelligence in a variety of ways. Customers can use their own browser, without any requirement for additional software or browser plugins of any kind, to access the Kaspersky Threat Intelligence Portal. For customers who value insight into threat indicators that are often present in web pages from any source, those with an active subscription to the Kaspersky Threat Intelligence Portal can use a Kaspersky browser plugin for Google Chrome that reveals that context in any visited web page. Customers can also integrate with Kaspersky threat intelligence via API, and use certificate-based, client-side HTTPS authentication and authorization to download and update purchased threat intelligence feeds.

Competition

Threat intelligence is a unique segment of information security. For one thing, competitors may often cooperate and even partner with each other, particularly on the integration of threat intelligence from multiple sources into proprietary tools. This reflects another distinctive aspect: threat intelligence consumers often value differing perspectives from multiple sources, even if those sources sometimes overlap in terms of coverage. In Kaspersky's case, it can bring a multinational perspective from outside North America.

Kaspersky thus competes with other leading security portfolio vendors in many business and enterprise markets, such as McAfee and Symantec (now a part of Broadcom) in North America, BitDefender, ESET and Sophos in Europe and Trend Micro in the APAC region (although all these competitors have a global presence). Worldwide, Microsoft has expanded its presence in enterprise security. Other players in markets such as network security or SIEM also offer threat intelligence capabilities, as with Cisco's Talos group, IBM's X-Force and Palo Alto Networks' Unit 42. At the same time, however, Kaspersky also partners with many of these companies to offer threat intelligence integration with their products. Additional partners include TIP providers such as AlienVault (now part of AT&T) and its Open Threat Exchange (OTX), Anomali, Arctic Security, EclecticIQ, ThreatConnect, ThreatQ and the MISP open source TIP.

More direct contenders in various aspects of threat intelligence per se include FireEye, particularly since its acquisitions of iSIGHT Partners and Mandiant, as well as CrowdStrike, Flashpoint, Group-IB, Intel 471, LookingGlass, Recorded Future, SecureWorks, Team Cymru, Verint and Webroot. 'Dark web' visibility is an emphasis of those such as DarkOwl and Sixgill.

Global systems integrators with threat intelligence offerings include Accenture (which acquired iDEFENSE in 2017), BAE Systems, Booz Allen Hamilton, Deloitte, NTT and PwC. Carriers with threat intelligence offerings in addition to AT&T include CenturyLink and Verizon. Digital Shadows, Proofpoint and ZeroFox are among those specializing in visibility into an organization's digital footprint as an aspect of the market. A large number of boutique firms further contribute to one of the most fragmented segments of information security, itself one of the most prolific markets in technology in terms of number of vendors.

SWOT Analysis

STRENGTHS

Kaspersky has strong foundations in threat research that inform its expertise, as well as a differentiating perspective as a multinational vendor. Customers in many regions could find this perspective to be a welcome alternative, particularly to providers with a distinctly North American point of view.

WEAKNESSES

Kaspersky is currently unable to sell into US government agencies, but the company claims year-over-year growth in North American threat-intelligence sales regardless.

OPPORTUNITIES

Kaspersky has the opportunity not only to integrate its threat intelligence capabilities with its own broad portfolio as well as with partner offerings, but to differentiate these capabilities based on its global view of threat insight.

THREATS

The offerings of threat intelligence providers often overlap, which can make differentiation challenging. Kaspersky compensates with its distinctive global perspective but faces significant competition from other multinational providers.