IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

ESET Evolves with AI, MDR, Threat Intelligence, and Integrations

May 20, 2024

By: Mark Child, Andrea Siviero

IDC's Quick Take

ESET held its annual global partner and customer conference, ESET World 2024, in Bratislava, Slovakia, May 13–15. The vendor announced a broad spectrum of new developments in its product and services portfolio, highlighted some key alliances and integrations it is building with other security and technology players, and presented its dedicated offerings for its partner channel.

Event Highlights

Although ESET has growing business in the enterprise space, it has long had a strong presence in the SMB segment, and this diverse coverage is reflected in its announcement of a new multitier structure for its managed detection and response (MDR) service. The vendor offers two versions of the service: ESET MDR for SMBs and ESET Detection & Response Ultimate for Enterprises, which can be combined with its ESET PROTECT Elite and ESET PROTECT Enterprise offerings. For SMBs that do not have their own security operations centers (SOCs) or teams of security analysts, ESET's MDR service provides threat prevention much faster than they could on their own. Enterprises that adopt the Ultimate version get additional components, such as customized malware analysis tools, as well as historical and customized threat hunting, digital forensic incident response (DFIR) assistance, and premium advanced support, which includes deployment, operation, and incident resolution.

Another of ESET's strong suits is its security research and threat intelligence. With hundreds of experienced researchers and telemetry collected from more than 110 million sensors across all global regions, the vendor works extensively analyzing malicious activity and threat trends and publishing threat reports. ESET published more than 90 reports in 2023, covering a whole range of industries, geographies, and threat actors and their campaigns. That number continues to rise in 2024, and it is out of this that the vendor has launched its ESET Threat Intelligence (TI) service, which provides in-depth technical analysis, various proprietary intelligence feeds, summaries of advanced persistent threat (APT) groups, actionable insights, reports for C-suite executives, and direct access to ESET security analysts. ESET TI can also be integrated into major security information and event management (SIEM) and security orchestration and response (SOAR) platforms, such as IBM QRadar, Anomali, openCTI, or Microsoft Azure Sentinel. The ESET TI service is available in multiple tiers to enable more flexible pricing and make it accessible even for small organizations.

As is the case with every security and technology conference these days, AI was a recurrent topic throughout the agenda, although ESET managed to avoid letting the noise drown out the core focus — keeping customers safe from cyberthreats. The vendor was also careful to present a balanced view of the benefits and threats of AI, neither overdoing the fear, uncertainty, and doubt (FUD) nor submitting to rosy-tinted optimism. ESET previewed its forthcoming chatbot-based AI Advisor, which conducts deep analysis of cyber-incidents, covering, for example, what exact techniques are used, what credential access compromises, and what level of persistence any infection has, while guiding users on

recommended responses and remediation measures. AI Advisor will enable natural language querying, significantly accelerating security analysts' investigations of suspicious activity.

Partnerships and Integrations

Enterprise security is increasingly broad and complex, and no security vendor can go it alone. Consequently, IDC is seeing considerable consolidation in the market, as well as the expansion of security ecosystems and alliances. ESET is no exception to this, with partners playing a key role in the company's success and growth. The vendor works with 100,000 partners around the globe (2,500 of which are "gold partners") and has a mixed business model across retailers, e-stores, resellers, and MSPs.

During ESET World 2024, the vendor also highlighted its recently announced technology integrations with Arctic Wolf and Elastic Security:

- ESET's Inspect module, which enables extended detection and response (XDR) within its ESET Protect Platform, has been integrated into Arctic Wolf's MDR solution. This considerably enriches the telemetry informing Arctic Wolf's platform and customers, enhancing security posture and risk mitigation capabilities. ESET Inspect will also send alerts triggered by suspicious activity on client endpoints to Arctic Wolf, prompting rapid investigation and response to contain threats.
- ESET's strategic integration with Elastic aims to provide enhanced cybersecurity analytics and visibility to customers by providing access to ESET's advanced threat intelligence feeds. Elastic customers will benefit from enhanced visibility and real-time data on indicators of compromise (IoCs), such as botnets and malicious domains, files, and URLs.

ESET World also hosted a dedicated session covering its partnership with Intel, which has ramifications for security and even sustainability. ESET has integrated Intel's Threat Detection Technology (TDT) into its endpoint protection platform, which gives it access to unique hardware telemetry and helps protect against ransomware with threat detection at the silicon level.

From a sustainability perspective, ESET has developed hybrid-aware products that can recognize which processor cores are available on Intel machines and run workloads on the most efficient options. For endpoint security, ESET hybrid-aware solutions will run noncritical tasks (e.g., certain scans that don't need to finish within a certain period) on the more efficient e-cores. This reduces energy consumption, increasing sustainability for organizations that deploy these combined solutions across their enterprise estates.

The newest development, the Intel AI PC, now has three core types: the traditional CPU and GPU and a neural processing unit (NPU). To conserve system resources and optimize performance, endpoint security solutions run a lightweight agent on the device and send back the telemetry to the cloud. Cloud backends process big workloads — because organizations don't want their user devices slowed down. The AI PC allows some of the processing to take place directly on the device, however, due to its three AI engines. This delivers:

- Extended ransomware detection capabilities
- Lower latency (because not all telemetry needs to be sent to the cloud)
- Reduced cloud costs

- Improved security (because some processing is done directly on the machine)

The development and nurturing of a solid partner ecosystem remain key for ESET, and the multiple partner-oriented initiatives in place (e.g., Partner Program, ESET Hub, Education Portal, and Partner Portal) certainly help in that direction.

IDC's Point of View

Enterprise security remains a very challenging arena. According to IDC's *European Security Technologies and Strategies Survey, 2023*, 60% of European security teams struggle to manage sprawling security estates that drain time and resources, 51% are unable to shift entrenched legacy systems, and 47% cannot balance their security priorities with the demands of their fast-moving businesses. While many of the cybersecurity behemoths continue to slug it out for market share and mindshare, and cybercriminals and nation state actors continue to develop ever more effective ways to breach company networks, ESET goes steadily about its business of developing an integrated platform of world-class security solutions backed by world-class security research.

Like many security vendors, ESET recognizes that, even with the best tools to hand, many organizations simply lack the resources to constantly fight off cyberattacks. Consequently, the vendor is also building out its MDR offerings. This does, however, bring it into a very competitive space. Nevertheless, the vendor also recognizes that two (or more) heads are better than one, and it is working hard to identify the right partners and develop integrations that strengthen its position on the market and the protection it can bring to end user organizations, directly or indirectly.

Key aspects the IDC EMEA team recommends ESET looks at to further accelerate its growth:

- Link security solutions' impacts to clear business impacts and ROI to show the business value associated with security investments.
- Develop a narrative and framework around the evolution of the office of the CISO to show how your vision and solutions align with digital business and security imperatives.
- Expand further on your AI capabilities, developing a full AI-security digital-use-cases taxonomy and road map by time horizon.
- Keep pushing on partner ecosystem growth, with a focus on building industry-specific expertise by country.
- Drive awareness around your pure-play security and research credentials. Not all organizations are content with an enterprise bucket-license default-security-tooling approach.

Subscriptions Covered:
European Security Technologies and Strategies