

First Look

ESET: Making Endpoint Security Easy for MSPs

Date: December 2019 Author: Kerry Dolan, Senior IT Validation Analyst

Threat Detection and Response Challenges:¹

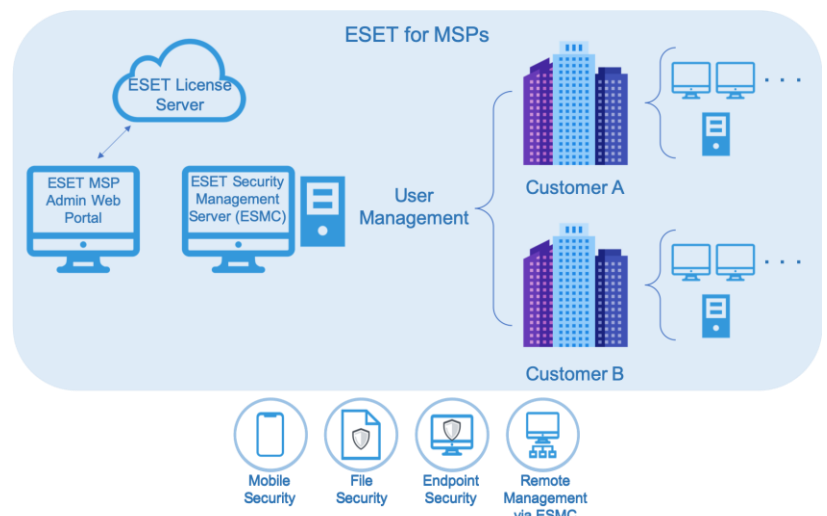
76% The percentage of respondents that find **threat detection and response more difficult** today than 2 years ago.

89% The percentage that expect to **increase spending on threat detection and response** over the next 12-18 months.

As security threats to customer endpoints proliferate and become more complex, many organizations are looking to managed service providers (MSPs) for help. Customers' manual processes are woefully inadequate; they need fast onboarding, rapid detection and response, and a sophisticated security solution that can keep up with the evolving threat landscape. In particular, SMBs are increasingly vulnerable to attacks that can be catastrophic, and many lack the resources to focus on cybersecurity. Leveraging the right MSP partner, SMBs can get high-powered cybersecurity technologies that balance quality and cost, and gain assurance of protection while they focus on their business.

ESET MSP Program

ESET provides a complete endpoint security platform that includes endpoint threat & malware protection, mobile security, file security, endpoint security, and remote management for Windows, Mac, VMware, Linux, iOS, and Android devices. ESET's security solutions use a behavior-based, multi-scanning, layered protection approach that results in a high threat detection rate and low false positives. With more than 30 years in the security business, ESET supports 400K+ businesses and 110M+ users around the world and offers full security solutions for businesses of any size.



ESET bundles a security solution for MSPs to include in their offerings, enabling complete endpoint security management for customers that includes multiple layers of detection, a real-time memory scanner, ransomware shield, exploit block, and host-based intrusion protection. MSPs can manage all customers through a single, multi-tenant management console, or leverage no-cost plug-ins to leading remote monitoring and management (RMM) providers, including ConnectWise, Datto, SolarWinds, NinjaRMM, and Kaseya. Benefits of the ESET MSP program include:

- *Flexible licensing at a flat monthly price*, to align with MSPs' service models. This eliminates up-front, multi-year licensing by individual operating system or mobile platform, which drives up cost and complexity. ESET enables MSPs to pass costs on through their offering.
- *A bundled SKU* that delivers security solutions for file servers, workstations, and mobile devices.
- *Aggregate volume pricing with discounts* on total licenses for MSP staff, regardless of how many customers they are supporting. Multiple tiers reduce the cost as MSPs build their businesses with ESET.
- *Implementation and onboarding* with an ESET engineer, and US-based support.

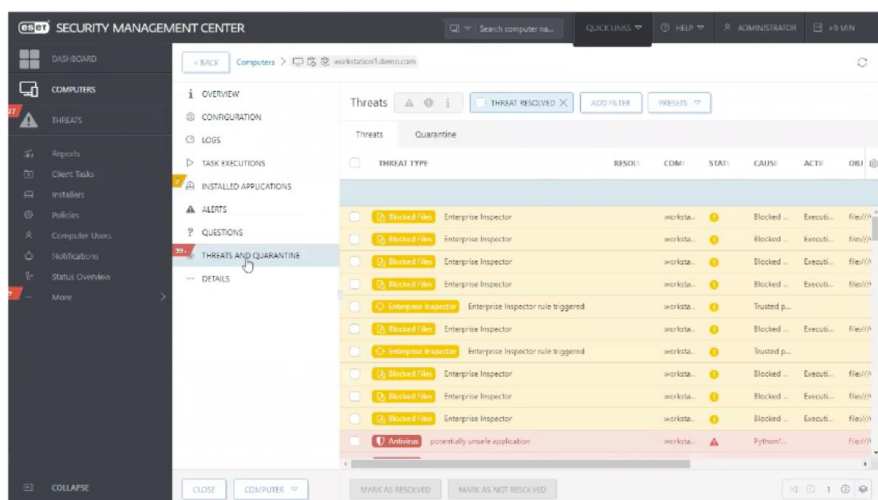
¹ Source: ESG Master Survey Results, [The Threat Detection and Response Landscape](#), April 2019.

This ESG Lab First Look was commissioned by ESET and is distributed under license from ESG.

ESG Validation Demo Highlights

- MSPs select from endpoint management options, including the ESMC or their RMM with free ESET plug-ins.
- Simple deployment options include direct from ESMC, .exe, MSI, BAT file, and more, and installers can deploy both the management component and security products.
- MSPs can create multi-tenant accounts and add licenses through the MSP Admin Portal.
- Layers of detection include web access and email filters; real-time memory scanner, ransomware shield, and exploit blocker; and host-based intrusion prevention.
- The primary detection methods use heuristics and behavior management. ESET looks at the code, rather than relying on updates or signatures; if the engine is unsure whether a threat is present, an application goes into a sandbox in the ESET kernel for monitoring.
- ESET detects threats and will quarantine and clean an infected file automatically; detailed information about the workload, OS, etc., is available.
- Unknown applications can be sent to the cloud server for scanning by neural networks, classification algorithms, or reverse engineering. Scanning is local but can use ESET’s collective research and machine learning for cloud-assisted scanning (LiveGrid).
- A customizable dashboard provides an overview of all devices with status and alerts, including tabs detailing incidents, VM details, AV & firewall threats, and more.
- MSPs can create static groups to manage customer organizations using policies. Dynamic groups are used to automate tasks by need, such as VMs that need an OS update or that are not activated with a security product.
- ESET can be configured to monitor and/or block devices (such as external drives, smart cards, mobile devices, etc.) and websites (by URL or category). Firewall network protection is also available.
- Updates to ESET are small and non-disruptive, and by default can be pulled from the nearest ESET cloud server; free caching proxies can be used if desired.

Threats and Quarantine Tab



First Impressions

As endpoint security becomes more complex, organizations are looking to MSPs for help. So, what do MSPs need? Robust security solutions that get the job done, but that are also easy to incorporate and manage.

ESG’s first impression is that ESET checks all the boxes. The product options were designed for detection and protection from malware and offer multi-layer detection using heuristics and behavior analysis. It is a lightweight solution that minimizes any disruption to user devices. ESET prides itself on making it easy for MSPs to get up and running, with a multi-tenant console or plug-ins to major RMM vendors. Bundling, pricing, and discounts are focused on helping MSPs build their businesses without additional burden. All in all, a great first impression!

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.