CSO
FROM IDG
SPONSORED CONTENT

WHITE PAPER

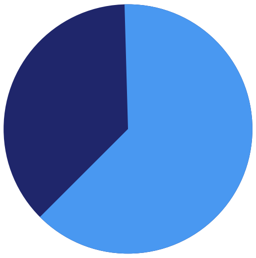
Automate and Integrate Your Security Toolset with Malwarebytes

From automation to intelligence, expand your security toolset with Malwarebytes integrations

TO SAY THAT today's security teams are overwhelmed would be an understatement. Challenged with an ongoing shortage of professionals to fill critical roles, the 2020 worldwide pandemic only made the situation worse. Security leaders were tasked with supporting widespread work from home arrangements—meaning an already large attack surface grew even larger.

In fact, IDG's 2020 Security Priorities study found 62% of security/IT executives said they expect the pandemic to impact the way their organization evaluates and responds to risks moving forward. This focus on security includes additional investment in response planning resources to address risk (38%) and updating and modernizing business continuity plans (30%). As part of these plans, organizations are actively researching and investing a variety of security solutions—and they expect to increase spending on security tools in the coming year.

But there are challenges woven into these investments. The number of platforms and tools available today to mitigate risk is dizzying. Many organizations report using more than 50 security tools, with larger enterprises often managing 100+ tools. By their very nature, a large number of tools complicates operations. And siloed tools further complicate security because they limit visibility into how they fit into an overall security playbook. What's more, a large number of security tools means some features or capabilities will inevitably overlap.



62% of security/IT executives expect the pandemic to impact their future risk response

IDG 2020 Security Priorities study

Malwarebytes

The key to solving these issues: maximizing each tool's potential with integrations. Integration between IT and security tools offers multiple benefits:

- Close the execution gap between IT policy and operations
- Blend security practices into the workflow to reduce the number of missed events and threats
- Improve response time when an organization is attacked or breached. Faster response time translates into reduced financial impact.
- Improve operational and cost efficiencies
- Eliminate redundancy in the use of toolsets, which in turn cuts costs
- Help trim time spent on routine processes, in turn freeing up security practitioners to engage in more strategic activities

The integrations between Malwarebytes' solutions and multiple industry-leading security tools can streamline an organization's active threat response, threat intelligence management, and security operations.

In this white paper, we'll illustrate how integrations with Malwarebytes solutions can address the pain points of security teams, increase efficiencies, and help minimize costs.

Active Threat Response

Active threat response is a proactive approach to detecting and mitigating the threats that challenge an organization. Time is always of the essence when it comes to detecting threats. If a bad actor executes an attack that slips past network defenses, the more time they spend undetected within corporate systems, the more damage can be done. Active threat response requires teams to use tools that help minimize dwell time, stop the spread of malware on internal systems, and prevent a negative outcome from a breach.

Use Case: Automate support ticket workflows

Security teams are inundated daily with alerts that inform them of possible infections on systems and machines on their networks. They are also inundated with other tasks and mission-critical objectives. While it would be ideal if teams could respond to tickets as soon as an alert is created, this kind of speed is impossible. It can often take days for teams to give an alert the attention it needs, and that gives malware days to spread.

Malwarebytes' integrations allow for an automated response to support tickets that speeds this process.

Example: Workflow of an automated support ticket through integration with Malwarebytes:

- A scheduled Malwarebytes scan of the user machine is initiated
- The scan returns positive identification of a high-severity threat on the user machine
- Malwarebytes sends a request to a security orchestration, automation and response (SOAR) platform to kick off the workflow and generate a support ticket. It provides all relevant information on the scan and threat discovery.
- A support ticket is created and routed immediately to the assigned security staff for review
- Security staff receives the support ticket and initiates rapid response to the discovered threat

The benefits:

With automated support for tickets, mean time to remediate (MTTR) rates are reduced significantly. Instead of a near-constant need to respond to alerts, automation allows teams to focus on more mission-critical tasks and/or higher-level work.

Automation also mitigates the potential for damage, reduces malware spread, and minimizes the impact of a possible infection or breach.

Malwarebytes' Partner integrations that can solve this use case:

ServiceNow, Cortex XSOAR, Splunk Phantom

Use Case: Proactive threat hunting

Proactive threat hunting is just as it sounds—finding a problem before it becomes a bigger problem. Anomalous behavior can be investigated and remediated before damage occurs. But, as part of this process, having a holistic view of security data is essential. Data in siloes will not provide a complete picture of potential problems on disparate parts of a network.

Example: How integration with Malwarebytes works for actively uncovering hidden malware:

- Data from multiple security-related tools are integrated onto a security information and event management (SIEM) platform
- A security analyst identifies an indicator of compromise (IOC) as a malicious file (MD5/SHA256)
- An analyst correlates file usage with anomalous behavior data provided by Malwarebytes Suspicious Activity running on user machines
- The analyst investigates anomalous behavior on select endpoints by initiating Malwarebytes Scan and Remediation to discover hidden malware. This initiates endpoint remediation.
- An analyst continues the threat hunt by initiating scans on all endpoints touched by the nefarious IP address, enacting remediation events when hidden malware is discovered

The benefits:

Through security data correlation and proactive threat hunting, unknown threats are discovered before they infect endpoints, and MTTR is reduced. This integration also helps prevent lateral spread and stop or significantly minimize impact.

Malwarebytes' Partner integrations that can solve this use case:

Azure Sentinel, Rapid7, Splunk, IBM QRadar

> Having a holistic view of security data is essential. Data in siloes will not provide a complete picture of potential problems on disparate parts of a network.

Threat Intelligence Management

Through threat intelligence management, security teams assemble raw data about current threats, emerging threats, and other information from a variety of sources. The data is analyzed and used in defending against potential attacks. But effectively using this data can be a challenge. There is so much of it, and it can be overwhelming to assess and analyze. Integrations with Malwarebytes can help teams maximize the impact of threat intelligence to stay one step ahead of cybercriminals.

Use Case: Correlate security data

When security teams correlate endpoint security data with other security data, such as information from the network, they can create a more complete picture of vulnerabilities. Siloed data can't offer an accurate picture of weak and vulnerable areas of internal systems. Correlated data helps establish relationships between security data sources, enabling security teams to make more informed decisions on how to protect against threats.

Example: How Malwarebytes integration verifies security incidents with multiple sources of data:

- Data from multiple security-related tools, such as network monitoring, firewall management, and endpoint security, is integrated onto a SIEM platform
- A network traffic spike from a known threat actor IP address is observed
- An analyst timeboxes the traffic event across all data sources, fearful of malware delivery on end-user machines
- The analyst monitors data from a single pane of glass, looking for anomalous or nefarious behavior indicating a security breach
- No evidence of breach is found. It is determined that the network traffic spike event is not connected to a security incident.

The benefits:

Simply put, assembling all the pieces is powerful. In a network environment, thousands of security events and bits of information are generated daily. Manual correlation is nearly impossible with today's data volumes. Data correlation helps determine relationships between events and sources of cyberthreats that in turn inform better actions and decisions.

The data is not only beneficial for risk mitigation, but also for operations and organizational considerations. Data correlation offers a "big picture" view that can help security leaders acquire information about where to invest in resources, and/or where time may be better spent by team members.

Malwarebytes' Partner integrations that can solve this use case:

IBM QRadar, Rapid7, Azure Sentinel, Splunk

Use Case: Magnify visualization of security data

Visualization brings security data from varying sources together in a cohesive way, offering a different perspective for decision-making. Teams can view information faster and more easily with graphs that identify recurring patterns, or a process diagram that shows the severity of an incident.

Through integrations with Malwarebytes, security teams can "double-click" to magnify their view of security data. They can integrate endpoint data into other IT security data sources and leverage those capabilities to visualize data, understand attack vectors, and make better security decisions in the future.

Example: How Malwarebytes integration assists with visualizing network spread of a cyberthreat:

- Data from multiple security-related tools, such as network monitoring, firewall management, endpoint security, and server data, is integrated onto a SIEM platform
- Malwarebytes Suspicious Activity alerts of a newly discovered incident on both servers and workstations, denoting possible ransomware activity
- An analyst sends Malwarebytes an action to isolate, and/or remediate and rollback via a SIEM platform
- Analysts use the log data and other security data received in a SIEM platform to trace the malware spread back to additional endpoints and servers, which are possibly compromised
- The origin of the threat is traced back to a nefarious file download by a corporate email account, identifying an additional area for security improvement

The benefits:

With data visualization, teams don't just talk about potential malicious activity—they see it. The graphic representations of patterns and behaviors provide a fresh perspective on data to improve decision-making.

Malwarebytes' Partner integrations that solve this use case:

Azure Sentinel, Splunk, IBM QRadar, Rapid7

Security Operations/Orchestration

Security operations refers to the central function within an organization that manages risk mitigation. Orchestration refers to integrating various tools to streamline the process of safeguarding the business.

Malwarebytes has several key integrations that help automate some of the most critical responsibilities in a security operations center, where teams are often short-staffed and overworked.

Use Case: Automate endpoint scanning and isolation

One of the most critical responsibilities of the security team is regularly scanning endpoints in order to identify and uncover threats and infections. This a highly repetitive process that must occur, so why not automate it?

Through integrations with Malwarebytes, automated endpoint scans from pre-scheduled events can take place, service tickets are automatically input into a SOAR platform, threat discovery is immediate, and isolation takes place quickly to minimize impact.

Example: How Malwarebytes helps automate the manual process of endpoint scanning:

- Data from multiple security-related tools are integrated onto a SOAR platform
- A SOAR platform identifies an incident and automatically orchestrates Malwarebytes Isolation to limit the spread of a possible infection
- SOAR playbooks initiate an endpoint scan and remediation. The scan positively identifies the piece of malware on the machine, and updates the support ticket with this information.
- Remediation occurs, successful removal of malware is confirmed, and the support ticket is automatically updated with this information on a SOAR platform
- A SOAR platform updates the incident and a security analyst is notified of the events. The analyst can perform additional actions to remove isolation on the endpoint if required.

The benefits:

Automating endpoint scans reduces response time, minimizes threat dwell time and impact, and eliminates the hands-on process required if teams scan manually. By automating this critical process, security systems can regularly detect anomalies or other nefarious activity.

Malwarebytes' Partner integrations that solve this use case:

ServiceNow, Splunk Phantom, Cortex XSOAR, ForeScout

Use Case: Orchestrate security software installation

In environments where security and IT teams work separately, software installation is sometimes a challenge. If IT owns the endpoint, for example, it is often necessary to obtain their assistance with certain installations. With Malwarebytes integration, however, security teams can skip this manual, time-consuming process if a security problem is identified on an endpoint.

Example: How Malwarebytes integration expedites an endpoint security software installation and scan:

- User submits support ticket, reporting excessive pop-up windows and other nuisance activities
- A ticket is logged in a SOAR platform and reviewed by a security analyst
- The analyst classifies the issue as malware, and initiates Malwarebytes Breach Remediation (MBBR) through a SOAR platform
- A SOAR platform automatically copies the MBBR package on the user machine, scans the endpoint, sends back positive identification of malware, and then remediates the malware Successful remediation is reported by MBBR and the support ticket is updated
- MBBR deletes itself from the user machine and the problem is resolved

The benefits:

When a threat is detected, teams can execute a scan, perform remediation, and remove the software without jumping through hoops. This integration removes time-consuming steps with IT and eliminates the manual processes for distributing security software.

Malwarebytes' Partner integrations that can solve this use case:

BigFix, Microsoft SCCM, Forescout, Splunk Phantom, ServiceNow

Cyberattacks are non-stop, and cybercriminals are constantly innovating and evolving their techniques. Siloed data, inefficient operations, and manual processes alone are no longer effective in securing the enterprise. Breaches and security incidents are expensive, and high-impact incidents may require C-level response. Security teams must ensure their tools work together for the most efficient and proactive level of risk mitigation. Simply put, integrations are key to maximizing your security toolset in today's digital environment.

Expanding attack surfaces and inefficient use of security solutions can expose businesses to cyberthreats. Contact Malwarebytes to learn how to streamline your security toolset.

For more information visit Malwarebytes.com/integrations

Malwarebytes Integrations in Action

ServiceNow—ServiceNow is a SOAR platform provider offering technical management support, such as IT service management and help desk functionality, for large enterprise IT operations. The company's core business revolves around the management of "incident, problem, and change" IT operational events.

The integrations between Malwarebytes and ServiceNow streamlines incident response processes and reduces a security team's MTTR. Teams also gain an enhanced view of an organization's security posture with security incidents in ServiceNow that are generated on events triggered by Malwarebytes.

How the integration works: Through integration with Malwarebytes Cloud, the incident is found and quarantined. Data is sent to ServiceNow to generate a ticket. ServiceNow checks the risk score and severity and initiates Malwarebytes for remediation for other endpoints. Lastly, Malwarebytes initiates a scan and removal of malware on endpoints.

Splunk—Malwarebytes endpoint security bidirectional integration (Incident Response, Endpoint Protection, and Endpoint Detection and Response) is compatible with Splunk Enterprise Security. Integration with Malwarebytes allows teams to add endpoint intelligence to Splunk and programmatically or manually query comprehensive threat intelligence. Data from multiple security-related tools are integrated onto a SIEM platform for better decision-making. This provides comprehensive threat hunting and analysis across the enterprise.

Security teams can consolidate and analyze threat data and automate remediation of infected endpoints faster without impacting end-user productivity.

How the integration works: Malwarebytes sends security telemetry and associated asset data. Splunk analyzes the endpoint data with other data sources in Splunk Enterprise/Cloud and Malwarebytes receives the detection notification.

Cortex XSOAR—Cortex XSOAR, a Security Orchestration, Automation & Response (SOAR) technology by Palo Alto Networks, enables security responders to collaboratively investigate threats and suspicious activity and close Malwarebytes incidents in the Cortex XSOAR war room.

How the integration works: The tool generates Cortex XSOAR incidents using Malwarebytes real-time protection events and Suspicious Activity monitoring. It integrates Malwarebytes sub-playbooks into existing Cortex XSOAR orchestration playbooks. This allows teams to automate up to 95% of all response actions requiring human review and enables security teams to focus on high-priority tasks.

For more information visit Malwarebytes.com/integrations

Malwarebytes