

# Red Hat Drives Security Orchestration and Automation with New Ansible Capabilities

OCT 02, 2018

*Red Hat previews Ansible Automation for enterprise security solutions, including Check Point, Splunk and Snort*

AUSTIN, Texas – ANSIBLEFEST 2018--(BUSINESS WIRE)-- Red Hat, Inc. (NYSE: RHT), the world's leading provider of open source solutions, today previewed new Ansible Automation integrations to help customers automate and orchestrate enterprise security solutions, further extending Red Hat's leadership across the IT security landscape. By automating security capabilities like enterprise firewalls, intrusion detection systems (IDS) and security information and event management (SIEM), organizations can better unify responses to cyberattacks through the coordination of multiple, disparate security solutions, helping these technologies to act as one in the face of an IT security event.

Automation is an important component of digital transformation, helping to drive efficiency, deliver value faster, and solve IT and business workflow challenges. Starting with [networks](#), Red Hat has been driving Ansible Automation into IT domains beyond operations, enabling users to more easily automate more tasks in more ways, including security tasks. Beyond the intent to enable security solution automation, Red Hat also announced [certified content](#) to help improve the reliability, consistency and veracity of content.

As IT environments become more complex, so do the security events facing enterprise IT teams. To help organizations better assess risks, remediate issues and develop compliance workflows, Ansible security automation will offer new modules to integrate and orchestrate security tasks and processes. These capabilities are designed to enable IT security teams to innovate and implement better controls that can encompass security technologies that enterprises are using with Red Hat Ansible Automation.

According to Gartner, "Security teams are suffering from staff shortages, an increase in the volume of alerts and threats, and the ever-present need to do more with less. Existing tools, such as firewalls, endpoint protection platforms (EPPs), security information and event management (SIEM), secure web gateways (SWGs) and identity proofing services (IDPSs), have not been improving the breadth and depth of their APIs. This hinders security teams from getting their tools working in concert with each other to solve problems. The "tool silo" problem is still the norm for most security teams. Threat intelligence (TI) has matured significantly and is now a front-and-center requirement to improve the context security practitioners need. It is also making many tools and processes smarter and more efficient." (*Gartner, Preparing Your Security Operations for Orchestration and Automation Tools, Anton Chuvakin, Augusto Barros, February 22, 2018*)

Through Ansible security automation, security teams can better address multiple use cases, including:

Detection and triage of suspicious activities - Ansible can automatically configure logging across enterprise firewalls and IDS to enrich the alerts received by a SIEM solution for easier event triage; for example, enabling logging or increasing log verbosity.

Threat hunting - Ansible can automatically create new IDS rules to investigate the origin of a firewall rule violation and whitelist those IP addresses recognized as non-threats.

Incident response - Ansible can automatically validate a threat by verifying an IDS rule, trigger a remediation from the SIEM solution and create new enterprise firewall rules to blacklist the source of an attack.

As part of this preview, Red Hat's Ansible security automation platform provides support for:

Check Point – Next Generation Firewall (NGFW);

Splunk – Splunk Enterprise Security (ES);

Snort

## Availability

Support for automating enterprise security solutions in Ansible is currently in tech preview and is slated to be generally available via Ansible Galaxy in early 2019.

## Supporting Quote

*Joe Fitzgerald, vice president, Management, Red Hat*

"Since Red Hat acquired Ansible in 2015, we have been working to make the automated enterprise a reality by driving Ansible into new domains and expanding automation use cases. With the new Ansible security automation capabilities, we're making it easier to manage one of enterprise IT's most complex tasks: systems security. These new modules can help users take an automation-centric approach to IT security, integrating solutions that otherwise would not work together and helping to manage and orchestrate entire security operations with a single, familiar tool."

## Additional Resources

Learn more about [Red Hat Ansible Network Automation](#)

Learn more about the [Red Hat Ansible Automation Certification Program](#)

Read more about [IT automation](#)

Learn more about [Red Hat](#)

Get more news in the [Red Hat newsroom](#)

Read the [Red Hat blog](#)

Follow [Red Hat on Twitter](#)

Join [Red Hat on Facebook](#)

Watch [Red Hat videos on YouTube](#)

Join [Red Hat on Google+](#)

Follow [Red Hat on LinkedIn](#)

About Red Hat, Inc.

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT. Learn more at <http://www.redhat.com>.

Forward-Looking Statements

Certain statements contained in this press release may constitute "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995. Forward-looking statements provide current expectations of future events based on certain assumptions and include any statement that does not directly relate to any historical or current fact. Actual results may differ materially from those indicated by such forward-looking statements as a result of various important factors, including: risks related to the ability of the Company to compete effectively; the ability to deliver and stimulate demand for new products and technological innovations on a timely basis; delays or reductions in information technology spending; the integration of acquisitions and the ability to market successfully acquired technologies and products; fluctuations in exchange rates; the effects of industry consolidation; uncertainty and adverse results in litigation and related settlements; the inability to adequately protect Company intellectual property and the potential for infringement or breach of license claims of or relating to third party intellectual property; risks related to data and information security vulnerabilities; changes in and a dependence on key personnel; the ability to meet financial and operational challenges encountered in our international operations; and ineffective management of, and control over, the Company's growth and international operations, as well as other factors contained in our most recent Quarterly Report on Form 10-Q (copies of which may be accessed through the Securities and Exchange Commission's website at <http://www.sec.gov>), including those found therein under the captions "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations". In addition to these factors, actual future performance, outcomes, and results may differ materially because of more general factors including (without limitation) general industry and market conditions and growth rates, economic and political conditions, governmental and public policy changes and the impact of natural disasters such as earthquakes and floods. The forward-looking statements included in this press release represent the Company's views as of the date of this press release and these views could change. However, while the Company may elect to update these forward-looking statements at some point in the future, the Company specifically disclaims any obligation to do so. These forward-looking statements should not be relied upon as representing the Company's views as of any date subsequent to the date of this press release.

*Red Hat, the Shadowman logo and Ansible are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the U.S. and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.*

View source version on businesswire.com: <https://www.businesswire.com/news/home/20181002005203/en/>

Red Hat, Inc.  
Kathryn Lucas, +1 703-663-1634  
[kkaplan@redhat.com](mailto:kkaplan@redhat.com)

Source: Red Hat, Inc.