

Agile Defense simplifies security compliance with automation



Partner resources

Red Hat® Ready
Partner Program

Software and services

Red Hat Ansible®
Automation Platform
Red Hat Consulting

Red Hat Ready partner, Agile Defense, helps U.S. government customers innovate through technology. A leading information technology (IT) services business partnered with Red Hat to create a Security Technical Implementation Guide (STIG) configuration, reporting, and remediation tool. Built on Red Hat Ansible Automation Platform, Agile Defense’s DuroSuite helps customers within the U.S. Department of Defense (DoD) keep their systems secure and compliant. Red Hat technical and business experts helped Agile Defense bring DuroSuite to market faster and increase the visibility of the tool in a competitive market. With DuroSuite achieving a DoD Authority to Operate (ATO) in September 2023 and Agile Defense looking to offer an enterprise version of the tool, the built-in scalability offered by Red Hat Ansible Automation Platform will play a crucial role in supporting the growing business.



IT consulting & services

1,000 employees

Benefits

- ▶ Reduced customer time spent on audits by 98%
- ▶ Brought DuroSuite to market faster
- ▶ Achieved accreditation to open new doors in a competitive market

“Agile Defense’s key contract vehicles for pursuing opportunities, combined with Red Hat’s innovative products and emerging technologies form transformational success.”

Victoria Trunnell
Solutions Lead, Agile Defense

“Automation has become critical in enabling secure mission IT. The automation of security compliance enables risk management while reducing time to mission. Agile Defense’s security compliance tool, DuroSuite, developed with Red Hat products and technical guidance, is a critical value-add tool ensuring our nation’s most critical networks are compliant with DISA’s high cybersecurity standards.”

Rick Wagner
Agile Defense CEO

Helping U.S. Government customers avoid threats

Preventing cybercriminals from gaining unauthorized access to government systems and infrastructure has never been more pertinent. Many breaches that occur are the result of configuration errors. For the U.S. Department of Defense (DoD) and federal agencies, avoiding threats requires them to adhere to strict information, security, configuration, and compliance standards set out in the Defense Information Systems Agency’s (DISA) Security Technical Implementation Guides (STIGs).

Regular audits check for misconfigurations and other errors, yet these audits are repetitive, resource-intensive, and costly. Agencies can spend months preparing for an audit. “Our customers’ production tasks would grind to a halt ahead of an inspection while they get all their documentation in line,” said Shawn Draper, Solutions Engineer at Agile Defense. “It was a very time-consuming, manual process.” Moreover, this reactive, manual approach was leaving customers open to known vulnerabilities between checks.

Red Hat Ready partner, Agile Defense, recognized this common challenge with its U.S. Government customers. “Misconfigurations and audits are a very pervasive pain point for most of the government customers we’ve spoken to,” said Sara FitzGerald, PhD, Technical Writer at Agile Defense. A leading IT services business, which prides itself on innovation through information technology, began developing a solution. The resulting STIG automation solution performs ad hoc systems audits, optionally remediates misconfigurations, and reports on the current state of devices.

Using automation to mitigate the impact of audits

Known as Agile Defense’s [DuroSuite](#), the STIG automation solution uses Red Hat Ansible Automation Platform because of its flexible and scalable automation capabilities. “We chose Red Hat Ansible Automation Platform to tackle this problem because it can communicate with everything,” said Draper. “Network devices, Windows machines, databases, web servers...Red Hat Ansible Automation Platform can talk to them all.”

Additionally, Red Hat recently collaborated with DISA on a STIG for Red Hat Enterprise Linux® and understands the importance of creating standards for every device, OS, and software version.

DuroSuite uses Ansible Automation Platform configuration management automation capabilities to audit for open vulnerabilities. “Red Hat Ansible Automation Platform connects to devices and executes commands specified in an Ansible Playbook,” said Draper. Having identified misconfigurations automatically, DuroSuite can also automatically remediate them by following commands in a customized Ansible Playbook.

Agile Defense has built a variety of playbooks, each designed to test a different type of device. These include playbooks for Red Hat platforms, Windows devices, VMware vSphere hypervisors, Cisco routers and switches, and firewalls. Its graphical user interface (GUI) makes it easy to use, displaying audit reports, remediation results, artifacts, and other key data at the click of a button to help customers maintain compliance. DuroSuite also contains an application programming interface (API) for customers who want to access the data but not from the GUI.

“Fixing the deficiencies is only part of the battle ahead of audits,” said Draper. “DuroSuite helps with all of the paperwork too, by automatically producing all the documentation needed.” Specifically, DuroSuite uses Ansible Automation Platform to write an XML check file (viewable in DISA’s STIG Viewer) for every device on the network and vulnerability identified to present to the auditor. These artifacts produced by DuroSuite can show current-state information and demonstrate that particular security configurations have been implemented. Ansible Automation Platform also allows customers to extend the capabilities of DuroSuite to manage workflows and inventory, schedule audits, and introduce role-based access control.

Partnering to accelerate time to market

Red Hat has supported Agile Defense throughout this project. The partners’ technical teams speak at least every other week, and a named, technical, single point of contact provides support whenever the Agile Defense technical team needs it. “Our Red Hat technical contact has been a fantastic source of information,” said Draper. “He either knows or knows how to find all of the minor details you need when you’re developing this type of solution.” The Red Hat technical contact may also call upon Red Hat subject matter experts to meet with Agile Defense’s engineers to discuss customizations, deployments, scaling, enhancements, and security capabilities.

Online training through the Red Hat Online Partner Enablement Network (OPEN) helped Agile Defense increase productivity. “The Red Hat training was a great foundation for learning Red Hat Ansible Automation Platform and understanding how it functions and how the language works,” said Draper. “It was very thorough, very helpful, taking you from setting up Red Hat Ansible Automation Platform through to building playbooks.” The training included self-paced online modules, slides, videos, and a lab component. The lab environment was set up for attendees in the Red Hat Product Demo System (RHPDS), the same system Red Hat uses internally to connect to and practice using Red Hat Ansible Automation Platform.

Agile Defense also meets every other week with a Red Hat Solution Architect from [Red Hat Consulting](#). During these meetings, the dedicated Red Hat expert provides guidance on moving more processes to Ansible Automation Platform. “This support is instrumental in our partnership,” said Victoria Trunnell, Solutions Lead at Agile Defense. “If we have any questions, we can reach out at any time, and we hear back; we don’t have to wait until this meeting.”

The Red Hat team also helped Agile Defense achieve a DoD Authority to Operate (ATO) for DuroSuite in September 2023, opening the door to additional opportunities with government entities. Red Hat is also helping to promote DuroSuite, mentioning it to Red Hat customers at opportune moments.

Accelerating value from a critical compliance tool

Reduced customer time spent on audits by 98%

The proactive monitoring of an agency’s security posture that DuroSuite provides is critical to maintaining readiness in the face of cyber threats. Historically, this monitoring has been resource-intensive and required additional software on endpoint devices. By using Ansible Automation Platform to scan for open vulnerabilities, Agile Defense’s DuroSuite saves Agile Defense’s government customers a considerable amount of time.

“DuroSuite saved one of our customers around 98% in terms of person-hours,” said FitzGerald. “They no longer need to manually click boxes and enter information in an XML tool for every device on their network.”

DuroSuite also ensures consistency across devices. “One of the great things about automation is that it does the same thing every time,” said Draper.

Brought DuroSuite to market faster

In combination with support from the technical contact, the Red Hat OPEN training helped Agile Defense bring DuroSuite to market faster. “I went through the Red Hat training in about a week, and it probably saved me three or four months of reading documentation and struggling to get started with Red Hat Ansible Automation Platform,” said Draper.

“The training was like a springboard that allowed us to quickly make a product that works. And just having our Red Hat contact available to act as a sounding board and help us work through the challenges we encountered with using the tool was invaluable.”

Opened new doors in a competitive market

Red Hat played an instrumental role in helping Agile Defense achieve the DuroSuite ATO, which has opened many new doors. Achieving an ATO is a significant step for Agile Defense because DoD does not allow its customers to use any tools that don’t have it—meaning DoD customers would not be interested in talking with Agile Defense about DuroSuite.

To achieve the ATO, Agile Defense had to prove DuroSuite’s compliance with STIGs at three levels: the application itself, its database, and its Red Hat foundation. “Building our solution on Red Hat Automation Platform was a huge help because it has already been vetted and has an ATO,” said Trunnell.

Security never stays still; new compliance requirements come out every few months in the form of STIGs. Agile Defense must stay compliant with these as part of the ATO. The Red Hat team shares vital insight into the STIGs with Agile Defense so the company can stay ahead of any future compliance requirements.

Enhanced value for customers by building on a successful partnership

With positive feedback from customers on DuroSuite and a lot of excitement from potential customers, Agile Defense is expanding its catalog of audited devices. “We’re always developing new Ansible Playbooks to audit and remediate the next big thing,” said Draper.

Agile Defense is even looking into how it can leverage additional Ansible Automation Platform features, specifically its built-in scalability, as it investigates offering an enterprise version of DuroSuite. The company is also exploring making DuroSuite available on the Red Hat Marketplace.

The partners will continue working closely together not only at a technical level but also at a business level, following potential leads and new opportunities. “We appreciate the support and the dedication that the Red Hat account teams have provided our company,” said Trunnell. “Our partnership with Red Hat is perfect. Agile Defense’s key contract vehicles for pursuing opportunities, combined with Red Hat’s innovative products and emerging technologies form transformational success.”

Ansible Automation Platform makes Agile Defense more competitive. “Red Hat Ansible Automation Platform is a very powerful configuration tool,” concluded FitzGerald. “It gives us an edge in an emerging market.”

About Agile Defense LLC

Headquartered in Reston, VA, [Agile Defense](#) is an end-to-end enterprise IT solutions provider, delivering leading-edge digital transformation solutions at scale. The company solves its customers’ critical challenges by leveraging a customized combination of advanced technology capabilities and tools including Cloud Services, DevSecOps, Cybersecurity, and AI / Automation. With approximately 1,000 engineers and subject matter experts, Agile Defense has been critical in enabling IT transformations of large-scale, high-profile mission-essential programs, including multi-environment upgrade projects and complex cloud-based initiatives. For more information, visit [www.agile-defense.com](#).



About Red Hat Innovators in the Open

Innovation is the core of open source. Red Hat customers use open source technologies to change not only their own organizations, but also entire industries and markets. Red Hat Innovators in the Open proudly showcases how our customers use enterprise open source solutions to solve their toughest business challenges. Want to share your story? [Learn more](#).



About Red Hat

Red Hat is the world’s leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. [A trusted adviser to the Fortune 500](#), Red Hat provides [award-winning](#) support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

f [facebook.com/redhatinc](#)
t [@RedHat](#)
in [linkedin.com/company/red-hat](#)

North America
1 888 REDHAT1
[www.redhat.com](#)

**Europe, Middle East,
and Africa**
00800 7334 2835
[europe@redhat.com](#)

Asia Pacific
+65 6490 4200
[apac@redhat.com](#)

Latin America
+54 11 4329 7300
[info-latam@redhat.com](#)