Red Hat® Ansible® Automation Platform is a foundation for building and operating automation across an organization. The platform includes all the tools needed to implement enterprise-wide automation

## Do you ask yourself these questions?

- Do you know your security policies are being followed at all times?
- Are you mostly dependent on human processes to insure you are compliant?
- Does the security committee push policies and IT Operations are faced with how to apply them in a heterogenous consistently changing ecosystems?
- Does it take too much time and effort to validate and report on your policies?

# Ansible Automation Platform

## Security Compliance

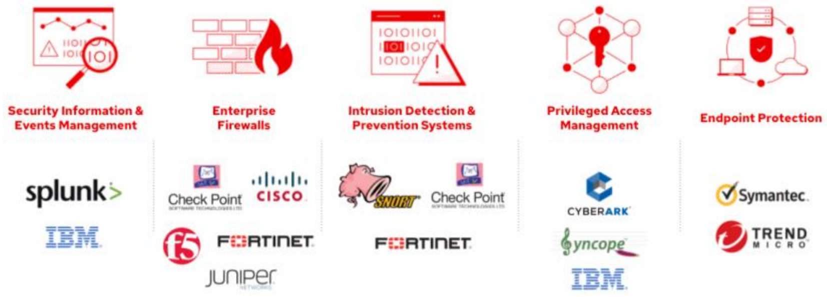
### Challenge

Today, organizations have designed good processes around security but struggle in their execution. The root cause in many cases is that humans become the bottleneck. The result is that failure can occur over time due to maintaining the compliance and configuration policies.

Along-side the execution of security processes is the reporting capability. Once more the human bottleneck hinders the speed and frequency of these reports. Furthermore, audits and audit trails are essential to standards adherence and can accelerate businesses towards their goals but again tend to be often manual in design.

Finally, you don't know what you don't know! – Major vulnerabilities are constantly coming out and it's difficult to stay ahead as it would demand checking all sectors, all of the time. Clearly, two factors are at play here – TIME and Human intervention/impact.

### Ansible Security Ecosystem



## Solution

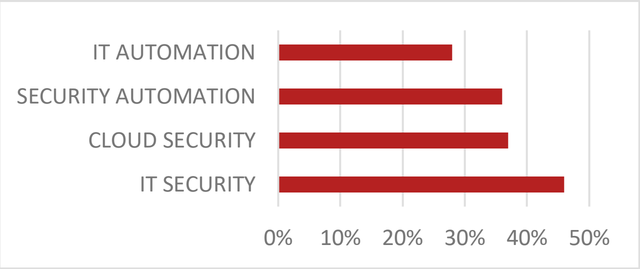
Ansible Automation Platform (AAP) ecosystem with GitOps including inventory of ALL enterprise nodes that are affected by your security policies or compliance standards.

Enable the security team (Committee) to be responsible for the security playbook(s), that will be used to maintain compliance and reporting across all assets. New Policies will be tested and reported. Current assets will be brought up to compliance with the new policies / compliance standard changes.

Existing policies and compliance standards will be consistently validated and reported on so the security responsible parties will be able to validate their policies are being implemented and staying in compliance.

What Ansible Automation Platform brings to the table is a way to add automation to ensure the policies you do choose to employ are being implemented and stay in compliance with the security teams standards. Ansible Automation Platform can not only integrate with your existing solutions but also can manage automating remediation of issues, report across your entire security ecosystem and allow you to build out custom methods of meeting your security requirements and security solutions because Ansible can maintain almost anything that has an IP address.

## Top IT Technology Funding Priority



*Statistics from – 2022 Global Tech Outlook – A Red Hat report*

## Benefit

### Enable Ansible for System Hardening

Every security department should have a hardening benchmark to which they hold their running systems. During the VM spin up lifecycle Ansible can be used for post configuration. Almost all our customers have a systems hardening step in all their configuration. Ansible is a first-class citizen in the world of configuration. Lock out certain users, tighten permissions on critical system directories etc. Red Hat has CIS benchmark systems hardening roles for rhel-7 and rhel-8.

### Audits

One of the most important pillars of Ansible Automation Platform is the auditing feature in Tower. Security teams can scan for who, what, when job templates are run. Ansible Tower produces metrics for these audits which can be exported to .csv for easy tracking.

### Reports

It's important to stay in the know with your server fleet. Using Ansible to setup reporting can be as easy as creating a playbook and taking advantage of the setup module. The setup module returns systems metrics which can be parsed for easy reading. If your organization already has a reporting tool in its security inventory like Nessus, you can still use Ansible to deploy and config the tool packages on all the supported systems.

### OS Patch Levels

Server fleet updated to the latest secure patch levels. Take advantage of OPENSCAP which automatically creates playbooks with the latest patches for security vulnerabilities. Crossvale has architected and implemented complex zero touch automation for patching server farms of 2500+ servers using Ansible Automation Platform.

## Benefit continued

### Identify & Manage Configuration Drift

Stay ahead of bad actors that can make unwanted changes on your systems. Ansible Automation Platform can perform scheduled Jobs on Ansible Tower. These Job templates run a preconfigured playbook. Ansible is idempotent, which means if something is running as intended ansible will verify it and move on to the next task. Scheduled Jobs help you identify configuration drift on your systems and rectify any damages done by a bad actor.

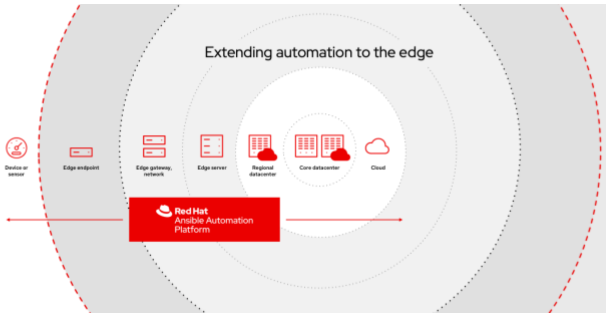
### Red Hat Certified

The modules are maintained and certified by Red Hat that integrate between your Security Automation Policies and the platforms, management consoles or nodes.
NO overhead to maintain custom written procedural scripts that break when patches are applied.

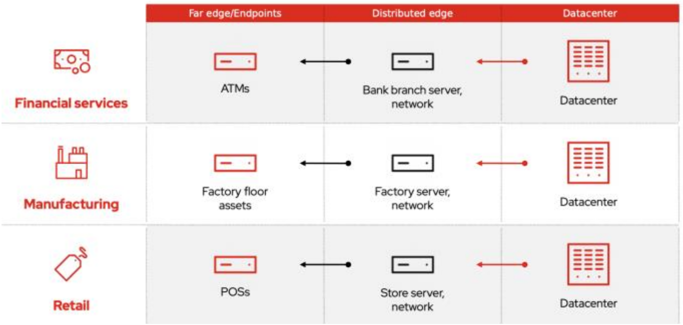
The value you gain is a standard method across your IT ecosystem to apply new policies and compliance standards and have the peace of mind that what you have said needs to be done is DONE and you have reports to VALIDATE it.

### Edge Security

Security, regulatory, and data management now extend all the way to the edge. Some small branches might not even have a rack or network closet with physical security, leaving IT devices vulnerable to tampering.



Automation solutions must include the ability to run compliance checks and remediation at scale, for thousands of devices, multiple times per day, as close to the source as possible.



## About Crossvale

For 20 years we have been helping our clients get more out of their enterprise applications and platforms. We focus on everything from Day zero, build and enablement of Container platforms, to Day one development of solutions and finally Day two operations and maintenance.