RAPID7

BUYER'S GUIDE

Security Orchestration and Automation Solutions

Understanding today's
SOAR market and offerings

TABLE OF CONTENTS

Introduction 3

So much to do, so little time and resources 3

Security Orchestration and Automation to the Rescue 4

Your Business Case for Automation 6

Eight Criteria for Evaluating Orchestration and Automation Solutions 8

Should you build your own solution instead? 9

Orchestration and Automation Made Easy 10

Next Steps 11

About Rapid7 12

Introduction

So much to do, so little time and resources

To say that today's threat landscape is challenging would be a massive understatement. Cybercriminals continue to successfully infiltrate organizations' defenses across the expanding attack surface of traditional infrastructure, cloud, mobile, and IoT devices.

While it's difficult enough to keep pace with rapidly evolving threats to protect a dynamic, perimeter-less environment, security teams today face numerous operational challenges that keep them from being as effective, accurate, and responsive as they need to be, including:

- **Disparate tools:** While there is certainly no lack of good security tools on the market, they don't all integrate with other tools or systems to centralize and share relevant, contextual data and alerts.
- **Too much data:** These individual technologies, originally purchased to meet a very specific need, now compete for the security team's time and attention, each outputting hundreds or even thousands of individual alerts per day.
- **Manual, repetitive tasks:** Searching through logs, creating help desk tickets, and organizing data via spreadsheets are examples of the time-consuming, manual tasks that burden security teams as they attempt to manage an ever-increasing workload.
- **Talent shortage:** The security workforce talent gap — which makes it difficult to hire and retain skilled staff — exacerbates the above operational challenges. In fact, eight out of 10 organizations report they are impacted by the security talent shortfall.[1]

For all these reasons, one of the fastest growing security trends right now is the adoption of security orchestration and automation solutions to help teams accomplish more, at a faster pace, and with greater accuracy. As security teams and the automation solutions to support them mature, the question is no longer whether organizations should automate at all, but when and how much.

This guide explains why security orchestration and automation are becoming increasingly essential tools to improve agility, responsiveness, accuracy, and efficiency. You'll also learn which use cases lend themselves easily to automation and the fundamental criteria you should consider when choosing a security orchestration and automation solution.

[1] "2018 Cyberthreat Defense Report," CyberEdge Group, 2018.

01 Security Orchestration and Automation to the Rescue

Security processes and playbooks often include a lengthy list of manual tasks, many of which require going from system to system to gather, collate, and analyze data and then act on that gathered intelligence. Each process can take hours (if not days or weeks) to complete, depending on the particular activity or threat.

Today's security teams don't have the luxury of time or unlimited resources. Nor can they afford to make mistakes because they are overwhelmed with data and alerts.

Speed and accuracy are now the watchwords for cybersecurity teams, and it's exactly what security orchestration and automation can provide. That's because machines have near unlimited scalability and are capable of quickly and accurately handling massive quantities of data in a fraction of the time it would take a human to gather and analyze it. This removes much of the manual effort, so your team can focus on bigger threats and more proactive security measures.

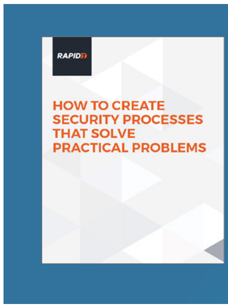
AUTOMATION IS…	AUTOMATION IS NOT…
The ability to perform security operations tasks—gathering and enriching data, analysis, vulnerability assessments, deprovisioning users, and much more—without the need for human intervention.	A replacement for humans on your security team, or an entirely hands-off approach to completing tasks. Instead, it allows you to do more with your existing staff and focus on the strategic questions, as opposed to routine, manual information gathering.

ORCHESTRATION IS…	ORCHESTRATION IS NOT…
A method of chaining tasks together to create larger processes and workflows that span tool sets. It's the connected layer that streamlines security processes and powers automation at scale to accelerate responses and save valuable time and resources.	A replacement for existing security processes or tools. Instead, it orchestrates the integration of tools and automates the execution of certain tasks within well-defined processes.

Orchestration and automation helps security teams do more by focusing on analysis and response instead of spending exorbitant amounts of time manually collecting data and performing other repetitive, lower-value tasks. But it's also now helping cybercriminals work faster and more effectively, too. If you're looking for one more reason to automate, it's this: it may soon be the only way to keep up with cybercriminals as they automate more of their malicious workload and attack tactics.

Security orchestration and automation solutions deliver:

- Faster incident response times
- Measurable time and cost savings
- Increased accuracy across security operations
- The ability to do more with existing resources
- Fewer errors
- Improved scalability


RAPID7

HOW TO CREATE SECURITY PROCESSES THAT SOLVE PRACTICAL PROBLEMS

Looking to develop efficient security processes, but don't know where to start? Get our whitepaper, **"How to Create Security Processes That Solve Practical Problems".**

Download the whitepaper now

02 Your Business Case for Automation

Before you look for an orchestration and automation solution, a good place to start is defining the pain points your organization needs to solve. Consider the following:

- Does your security team get too many alerts to handle effectively and in a timely fashion?
- Is your team suffering from symptoms of burnout?
- Do you have trouble hiring and/or retaining security talent?
- Does your team spend an inordinate amount of time gathering and analyzing information?
- Is your mean time to respond to a threat getting worse?

Next, it's important to define your most common use cases. For example, some companies would see immediate benefits by automating the handling of malware incidents because it's the biggest problem area for them, whereas other companies would benefit by orchestrating threat hunting and data enrichment tasks to better manage an enormous and increasing volume of threats.

Knowing which use cases you can solve for with orchestration and automation and then prioritizing those that can bring immediate value will help you eliminate solutions that can't quickly solve your most pressing issues.

COMMON AUTOMATION USE CASES

USE CASE	CHALLENGES	HOW AUTOMATION HELPS
Vulnerability assessment and management	Within the first 30 days after a vulnerability is discovered, the chances it will be exploited quickly rise. Your team must act swiftly to assess systems and remediate using the appropriate process.	Orchestration and automation solutions can assist in patching serious vulnerabilities across large environments as soon as a fix is released, rapidly closing the window in which an adversary can sneak in.
Email phishing investigations	Phishing remains a top attack vector behind successful breaches. Yet investigating phishing emails involves time-consuming, manual tasks such as investigating and detonating attachments, checking URLs, and following up on suspicious requests for sensitive information.	Orchestration and automation solutions can execute tasks like these behind the scenes while your team works on the rest of the investigation and response, ensuring the situation is handled effectively and efficiently while accelerating response time. You can also automate remediation steps for when a phishing email is identified
Threat containment	When a threat is identified, containment efforts such as quarantining a device must be immediate to prevent network egress and lateral movement to other devices. At the same time, user permissions may also need to be changed to stop a compromised account from executing malicious code, stealing data, or bringing down the site or application.	Orchestration and automation solutions can easily and rapidly quarantine a device. You can automate disabling user accounts the moment a trigger event is detected, such as escalation of privileges to admin, or when malware is detected. You can also accelerate endpoint remediation by automatically monitoring and killing processes, as well as tracking file permissions and changes.

USE CASE	CHALLENGES	HOW AUTOMATION HELPS
Provisioning and deprovisioning users	While inarguably important to your company's security posture, provisioning and deprovisioning accounts can be error-prone and time-consuming because they are typically manual tasks.	Orchestration and automation solutions that integrate with third-party vendors let you set up workflows to take specific, automatic actions on users and assets when triggered. You can quickly automate the addition or removal of users to keep systems and information within your organization secure and available to only the appropriate users.
Security alert enrichment	Many security teams face nonstop alerts, dealing with hundreds or thousands of false positives every day. Manually handling a data tsunami daily reduces your odds of being able to identify and respond to the ones that are actual threats.	Orchestration and automation solutions can help you accelerate detection by enriching the quality of the security alerts you receive and automatically weeding out many false positives, leaving your team with more time and greater context to tackle the actual threats.
Compromised credentials containment	Managing employee permissions is an ongoing challenge that carries significant risk, particularly for users with a variety of permissions across systems. In the event of a compromise, your team must respond rapidly to prevent data loss.	With the right solution, you can automate the containment of compromised credentials to immediately protect systems and data within your organization when an incident occurs.
Privilege escalation investigations	Privilege escalations are often an early indicator of a threat or an attacker in your environment. When a user elevates privileges, it should be manually reviewed to ensure that this access is appropriate. However, data gathering is manual and time consuming, leading to potential errors.	You can automate investigations, from triage through response, to validate that a user is who they say they are and that the user should have escalated access. Automation can help you improve accuracy as well as response time, which is critical to detecting an attacker in your environment as early as possible.
Incident detection and response	Even the best teams need to maximize efficiency and speed when detecting and responding to security threats. Massive quantities of data and multiple, siloed systems result in additional work and manual, repetitive steps, slowing investigations and mitigation.	Use orchestration and automation to integrate with your existing response tools and cloud services to contain threats stemming from both assets and users, and automate case management with your IT team's existing ticketing tools.
Threat hunting	Threat hunting can be extremely time-consuming and requires a high skill level to be most effective. It's difficult for teams to free up resources for extended periods of time to hunt.	Automate threat hunting processes and enrichment to identify suspicious malware and domains, and other indicators, lowering the barrier to hunting and freeing up your team to tackle critical challenges.
Security team communications	Many security teams use communication tools such as Slack as a hub for tracking incident management. This streamlined communication lets teams know the moment an issue arises so that they can respond faster and work more collaboratively.	Orchestration brings together your tools, and automation enables seamless workflows between them. Automation can take the alerts that come in from your security tools and delegate tasks from Slack back to your tools, making data flow bi-directional. You can trigger workflows when alerts are received to create new service or help desk tickets, kick off investigation and enrichment tasks, and more.

03 Eight Criteria for Evaluating Orchestration and Automation Solutions

Orchestration and automation solutions have evolved dramatically in just the past few years. While any solution you consider should offer the core orchestration and automation capabilities needed to support your use cases, there are important differences among solutions and vendors that can significantly impact your outcomes.

The following eight criteria can help you narrow the field and focus on the solutions that will deliver the most value in the easiest and quickest way possible, while delivering the flexibility and innovation you need to effectively handle future changes to your security tools and the threat landscape.

1 LITTLE TO NO CODING REQUIRED

Despite its proven benefits, many companies have hesitated to take advantage of security automation. Why? A primary reason has been the significant skills and resources required to write (and maintain) the code needed to create and automate workflows. Today, the top orchestration and automation solutions require little to no coding, allowing your team to begin using them quickly, without a major investment in coding efforts.

LOOK FOR a solution that lets you do both. It should come with a robust set of pre-built workflows for common use cases, enabling you to easily connect your technology stack and automate across your security and IT processes. You should also be able to create your own workflows or customize pre-built ones without having to code. However, in the event you need further customization, the solution should also offer the ability to work directly in the code as well.

2 EASY INTEGRATION WITH YOUR TECHNOLOGY STACK

Be sure the solution you choose has the right third-party integrations and plugins for your specific use cases (that's why it's important to define what they are before evaluating options) and technology stack. Without an easy way to integrate, you risk adding yet another silo to your security toolset instead of a way to orchestrate actions across all of your tools.

LOOK FOR a solution that offers a robust library of integrations, plugins, and workflows that supports your current environment andgives you a path to the future as well, as you upgrade or swap out various tools in your stack.

3 EXTENSIBILITY

What if a new tool comes out or you want to use a tool in a different way? Many solutions on the market require paid professional services or engineering work to build support for new integrations. Ask the vendors you are evaluating how easy it will be for you and your team to add new integrations or use cases.

LOOK FOR a software-as-a-service solution to eliminate the need to deploy and maintain software and the supporting infrastructure on-premises. In addition, a solution with pre-built workflows and integrations accelerates time-to-value as you don't have to wait for custom coding to happen before you start seeing benefits.

4 RAPID TIME-TO-VALUE

When evaluating orchestration and automation solutions, it's important to understand how long it will take your team to completely deploy the solution and begin seeing benefits. Consider the time and investment in both human and infrastructure resources. Are there any additional steps or costs required to get the new solution up and running?

LOOK FOR a software-as-a-service solution to eliminate the need to deploy and maintain software and the supporting infrastructure on-premises. In addition, a solution with pre-built workflows and integrations accelerates time-to-value as you don't have to wait for custom coding to happen before you start seeing benefits.

5 HUMAN DECISION POINTS

While orchestration and automation can handle many of the tasks within your security workflows, it's important to be able to define and enable tasks within automated workflows that require expert human insight, such as drawing conclusions and making rational judgement calls.

LOOK FOR a solution that gives you the ability to add human decision points anywhere in the automation workflow, which empowers your team to provide expert insight when responding to critical security threats.

6 FLEXIBILITY AND CONTROL

Depending on your use cases, you may not want to automate all the tasks in a process or workflow. For instance, you may want to avoid automation for tasks that are highly sensitive or require reason beyond what a machine can correlate. What you need is the ability to determine which parts or tasks would deliver the greatest benefit if you automated them, with complete control over what your security team continues to do. Some solutions don't allow for human intervention at points that you define, requiring you to automate some tasks that you feel are better handled by your team.

LOOK FOR a solution that gives you complete control over which tasks to automate within your workflows, with designated decision points for input where it's most critical.

7 PREDICTABLE COST

Does the vendor charge a set fee per workflow, or is it based on usage? Usage can be difficult to anticipate and budget for, as some vendors charge per user, per site, or even per number of API calls. For every vendor you evaluate, it's important to understand how many users, sites, and workflows are included in the price and if there are any overage fees that you need to take into consideration as well.

LOOK FOR a pricing model that offers unlimited seats, API calls, and so on without overage fees. That way, your security team isn't discouraged from taking advantage of all the benefits of orchestration and automation.

8 PACE OF INNOVATION

Can the vendor keep pace with new attack methods, evolving threat landscapes, and advances in security technology? The pace and quality of innovation can reveal a great deal about the commitment of the vendor to the solution and to the customers of the solution. If the vendor is continuously releasing new features and prioritizing popular customer requests, that's a positive sign that it'll continue to meet your needs in the years to come.

LOOK FOR a vendor that can describe exactly how the product team receives customer requests and how those requests are prioritized on the product roadmap. If relevant, ask how quickly the vendor plans to add support for integrations not currently available for your environment.

Should you build your own solution instead?

Do you have the resources internally to write, test, and maintain custom code? If so, you may be able to create a custom automation solution in-house or with the help of consultants. Before you decide, consider the following:

- Scope: Are you orchestrating and automating one simple process or an entire system? How long are you willing to wait for the automation to be ready to use?
- Resources: How many programmers will you need? Will you need to hire consultants?
- Environment: How many tools do you have? Do these tools have flexible APIs? What languages do they use? Which automation languages playnicely with your current tools?
- Budget: Based on scope, resources, and environment, what will the total cost of your project be to your organization?
- Maintenance: What will it cost to maintain the automation when new processes or tools are introduced or when scalability becomes a concern?

04 | Orchestration and Automation Made Easy

To do more with less, accelerate your security processes, and automate your most important use cases, Rapid7 offers a suite of solutions on its Insight platform:

insightConnect

Rapid7's orchestration and automation solution accelerates and streamlines time-intensive processes—no coding necessary. With 200+ plugins to connect your tools and easily customizable connect-and-go workflows, you'll free up your team to tackle other challenges, while still leveraging their expertise when it's most critical.

insightVM

Rapid7's vulnerability assessment solution includes built-in automation workflows, including automation-assisted patching to assign and track remediation duties across teams, and automated containment to automaticallyimplement temporary (or permanent) compensating controls via your network access control (NAC) systems, firewalls, and endpoint detection and response (EDR) tools.

insightIDR

Rapid7's threat-focused SIEM solution includes built-in automation workflows for containment, such as disabling users and quarantining assets with Active Directory or Okta, and case management for streamlined incident response processes between teams.

Top three questions to ask vendors before you buy

1. How easy is it to adopt your solution?
2. How will your solution empower our team to save time and resources and produce a measurable return on investment?
3. Will your solution scale with my organization's needs?

Proof Point:

Using orchestration and automation capabilities, we've seen customers reduce average response time from 30 minutes to 5 minutes, which equates to approximately 83 percent of time saved per alert.

Next steps

If your security team is struggling to keep up with data, alerts, systems, and repetitive processes, it's time to orchestrate and automate. When you choose the right solution for your use cases, you'll accelerate your security operations as well as your time-to-value,plus free up your staff to work on the most critical issues.

To see what automation could look like in your environment, visit rapid7.com/try/automation to start a free trial or contact our team to request a demo.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on Twitter.

To learn more about Rapid7 or get involved in our threat research,

visit www.rapid7.com.