

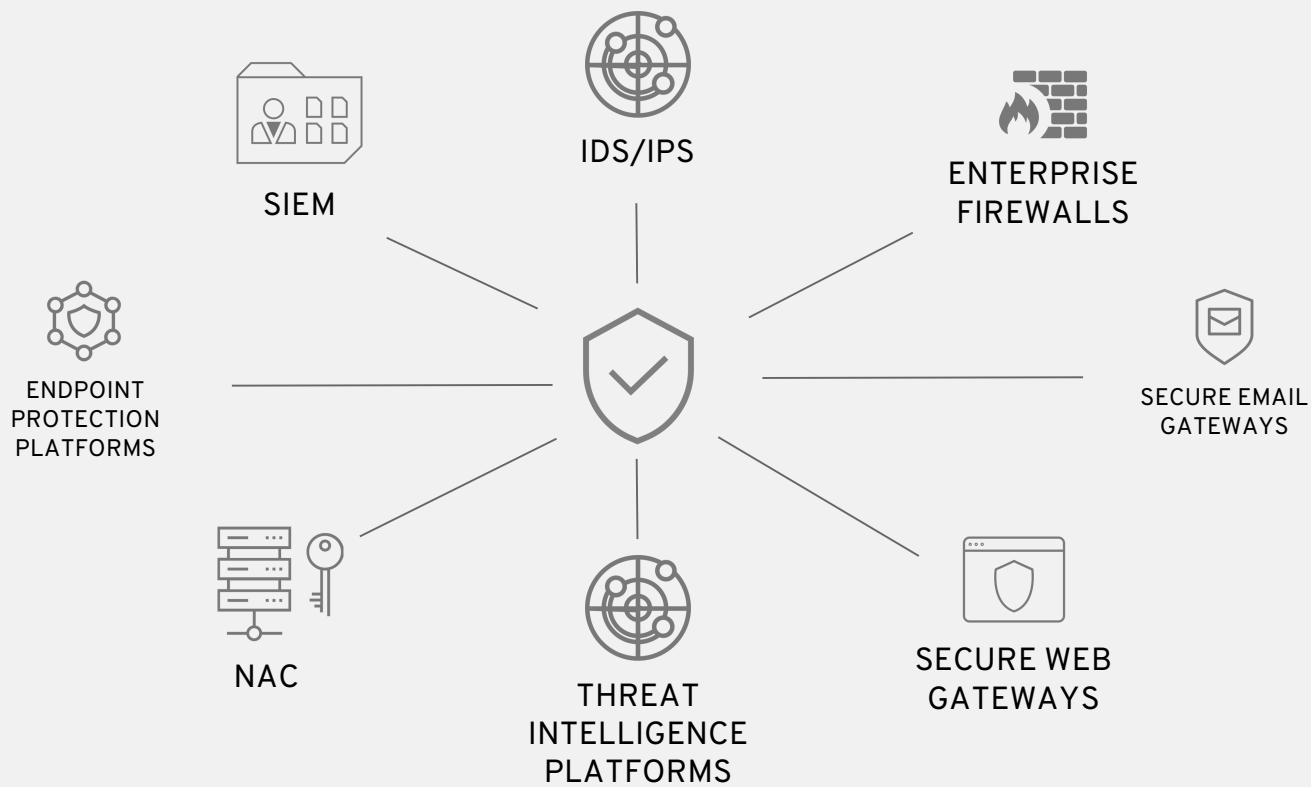
#**ANSIBLE**AUTOMATES

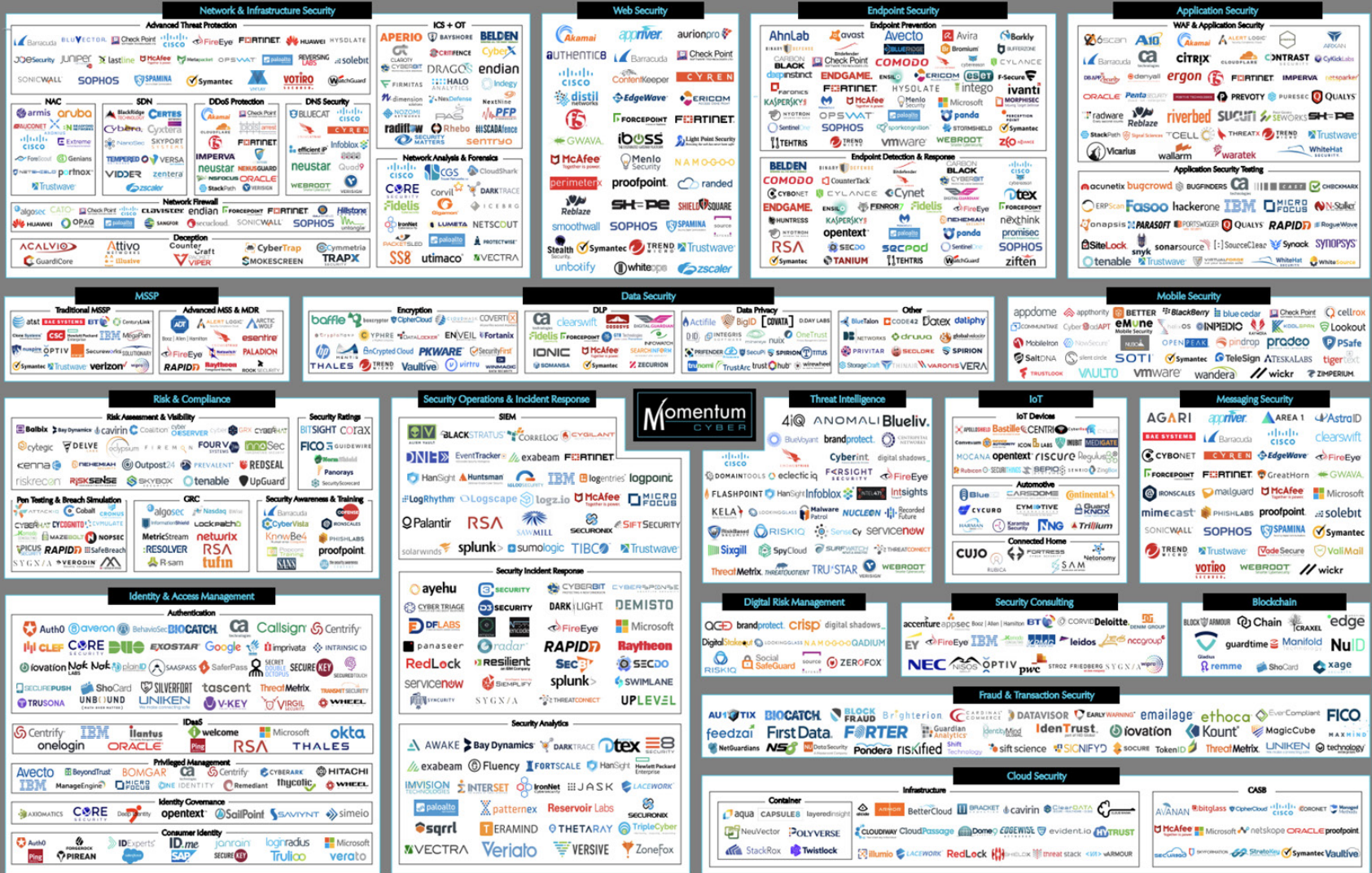
# INTRODUCING ANSIBLE SECURITY AUTOMATION

Massimo Ferrari,  
Management Strategy Director  
mferrari@redhat.com  
@crosslogic

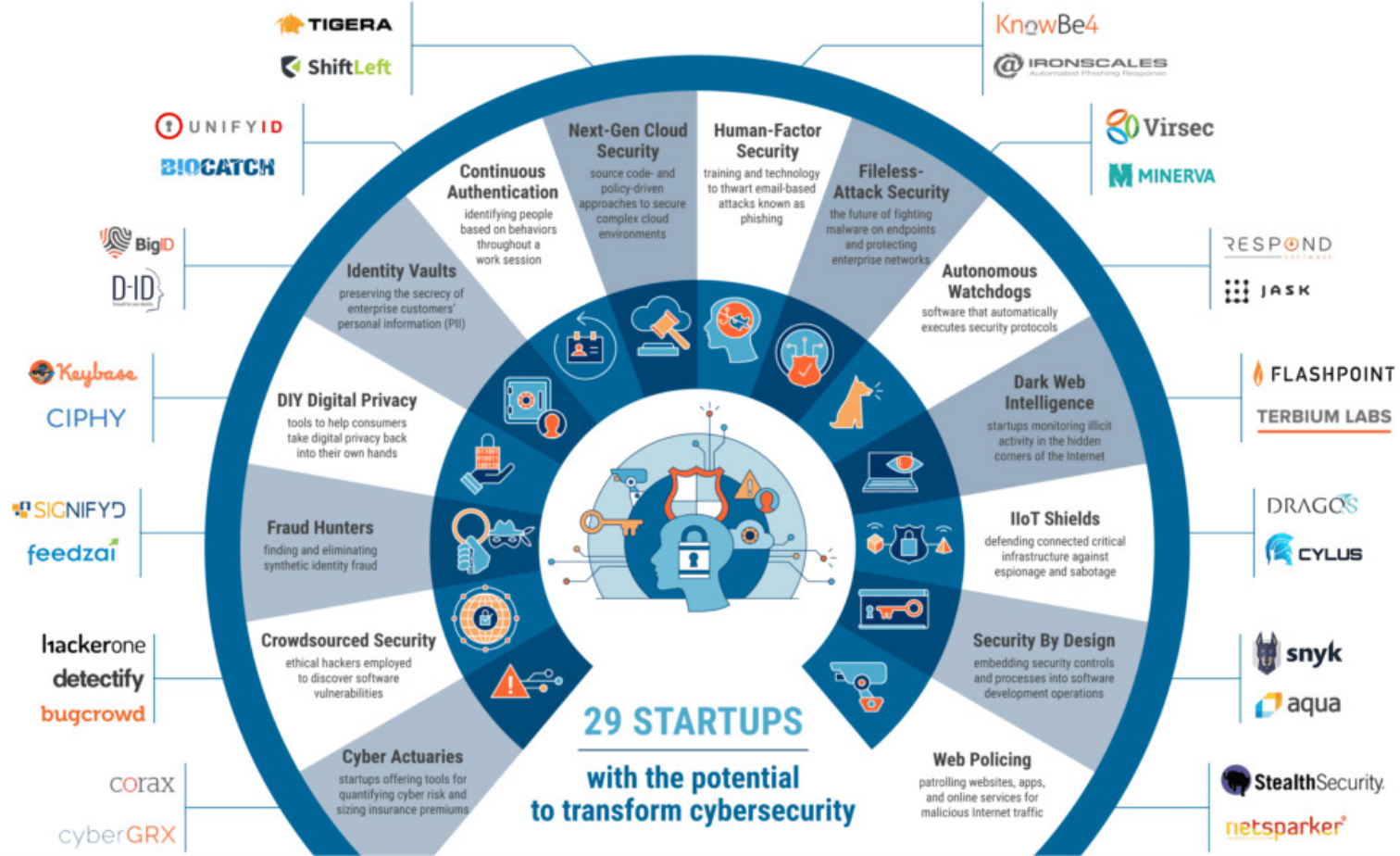


ANSIBLE





# CBINSIGHTS 2018 CYBER DEFENDERS



\$3.58bn

Funding in last year

+71.99%

YoY Funding Growth

179

Deals in last year

+26.62%

YoY Deal Growth

27

Avg Deals per Quarter

\$298.9M

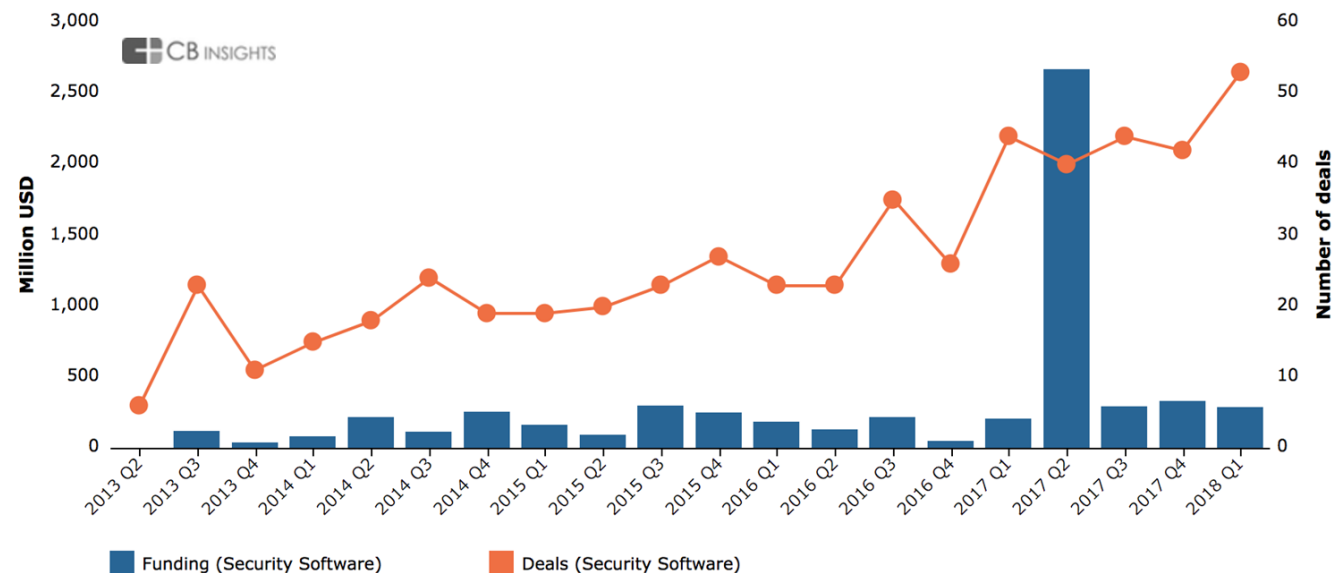
Avg Funding per Quarter

Q2'17

Biggest Quarter  
(\$ Funding)

Q1'18


Biggest Quarter  
(# of deals)






**"According to Gartner,  
worldwide spending on enterprise security  
will reach \$96.3 billion in 2018,  
an increase of 8% from 2017."**






“For one, security teams are overwhelmed.  
**The average security team typically  
examines less than 5% of the alerts  
flowing into them every day**  
(and in many cases, much less than that). ”




**“57% of respondents said the  
time to resolve an incident has increased**

**65% reported the  
severity of attacks has increased”**





“Having **insufficient skilled personnel** dedicated to cybersecurity was the second biggest barrier to cyber resilience, with only 29% having the ideal staffing level.”

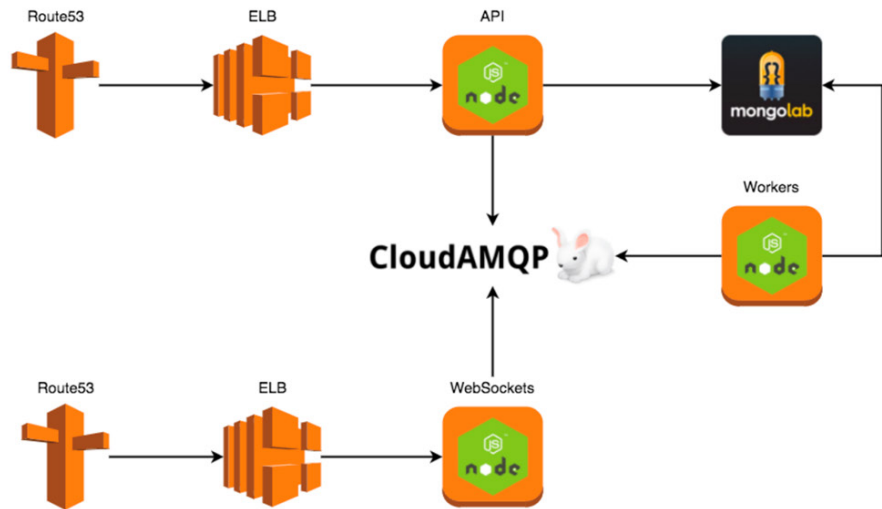


**“63% of respondents say  
their leaders understand that  
automation, machine learning,  
artificial intelligence and orchestration  
strengthens cyber resilience.”**

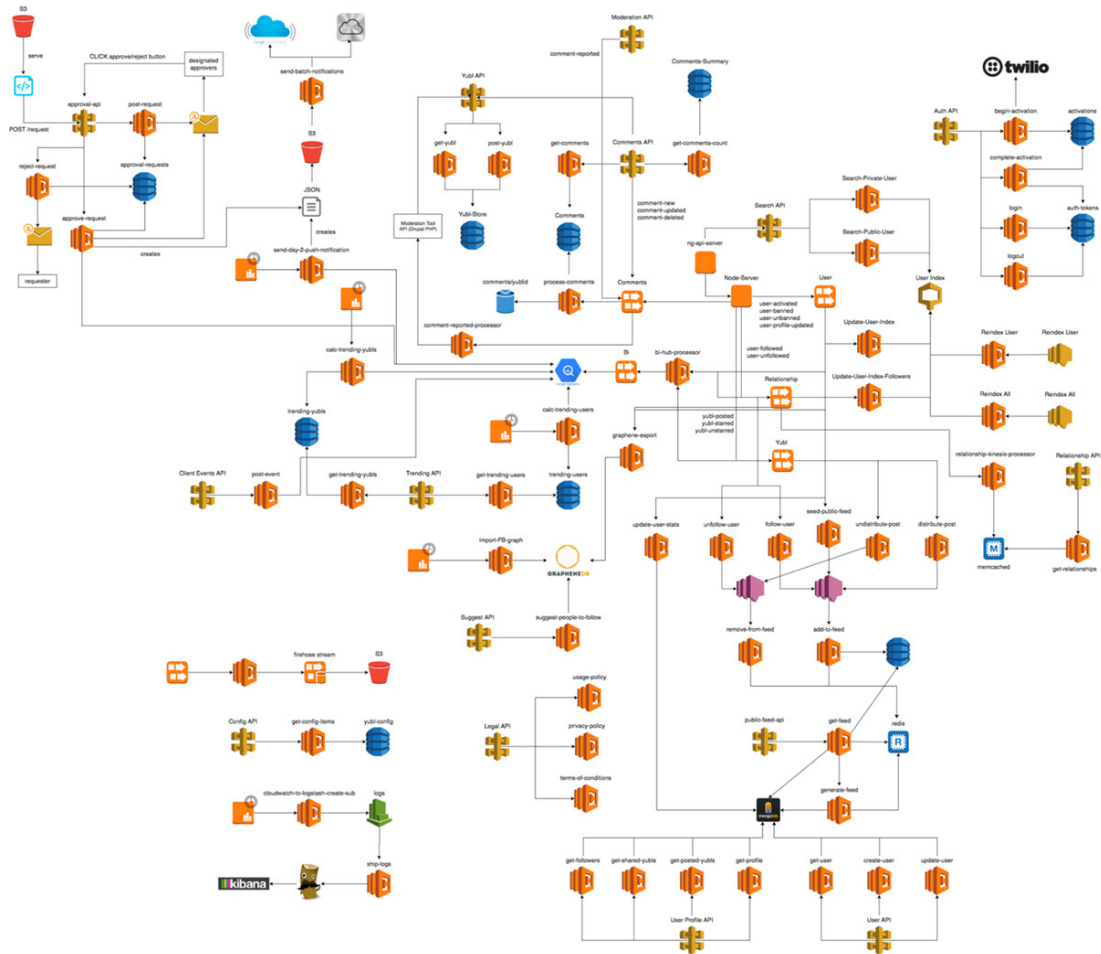


AT CLOUD SCALE  
YOU HAVE NO CHOICE BUT AUTOMATE

# REAL-WORLD CONTAINER-BASED APP IN AWS



# SAME APP, REWRITTEN AS FUNCTION-BASED AWS APP



This is just about the inherent inefficiency of  
the IT security world.

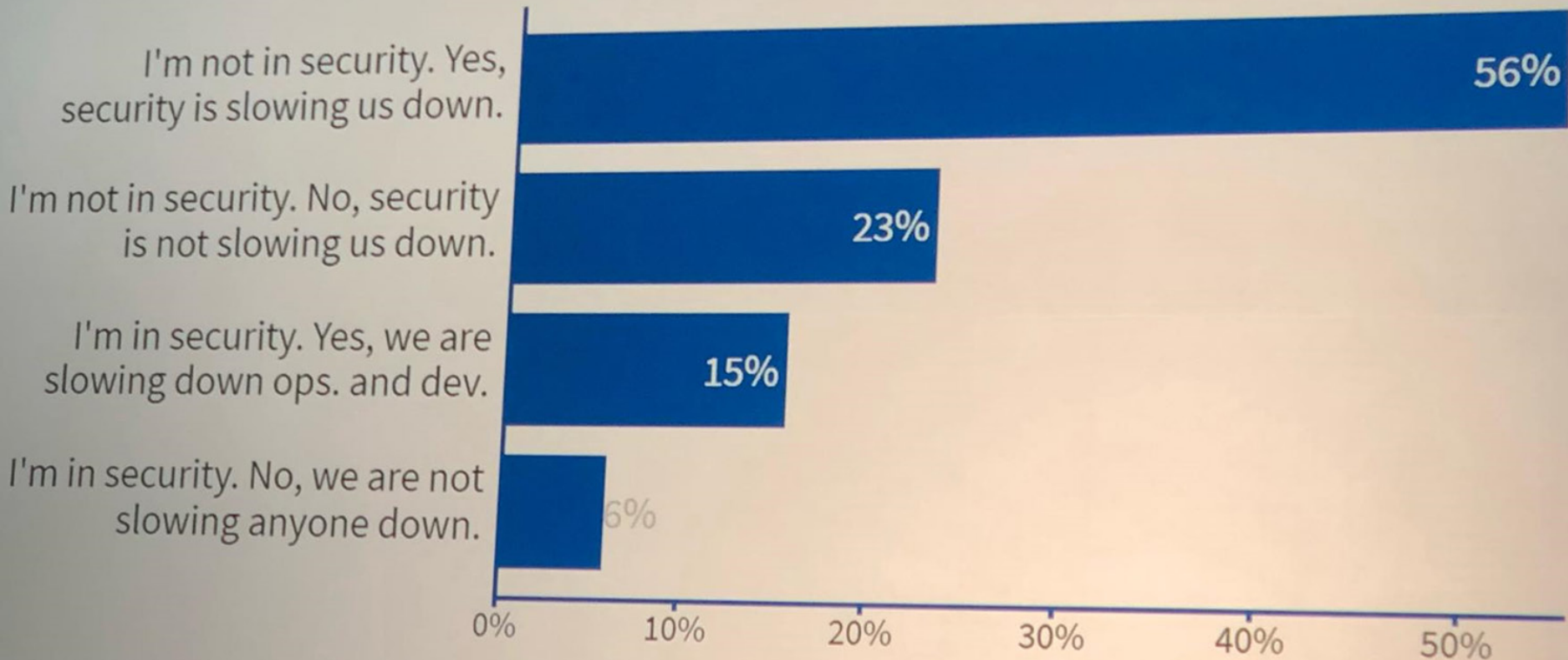
Then there are 2 new emerging aspects...






Visit [gartner.com/gpolls3](http://gartner.com/gpolls3)

Do you believe information security is slowing down agile operations and agile development?

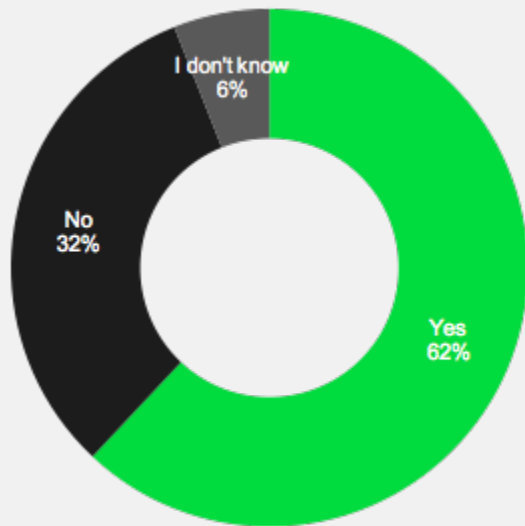






“The use of AI to automate tasks involved in carrying out cyberattacks will alleviate the existing tradeoff between the scale and efficacy of attacks. This may expand the threat associated with labor-intensive cyberattacks (such as spear phishing). We also expect novel attacks that exploit human vulnerabilities (e.g. through the use of speech synthesis for impersonation), existing software vulnerabilities (e.g. through automated hacking), or the vulnerabilities of AI systems (e.g. through adversarial examples and data poisoning)”

# BlackHat 2017 attendees on the chances of more attacks using AI against targets in the next year





### DeepLocker - Concealing Targeted Attacks with AI Locksmithing

Dhiling Kirat | Research Scientist - Security, IBM Research  
Jiyong Jang | Research Scientist - Security, IBM Research  
Marc Ph. Stoecklin | Principal Research Scientist - Security, IBM Research

**Location:** South Seas ABE

**Date:** Thursday, August 9 | 5:00pm-6:00pm

**Format:** 50-Minute Briefings

**Tracks:**  Malware,  Exploit Development

In this talk, we describe DeepLocker, a novel class of highly targeted and evasive attacks powered by artificial intelligence (AI). As cybercriminals increasingly weaponize AI, cyber defenders must understand the mechanisms and implications of the malicious use of AI in order to stay ahead of these threats and deploy appropriate defenses.

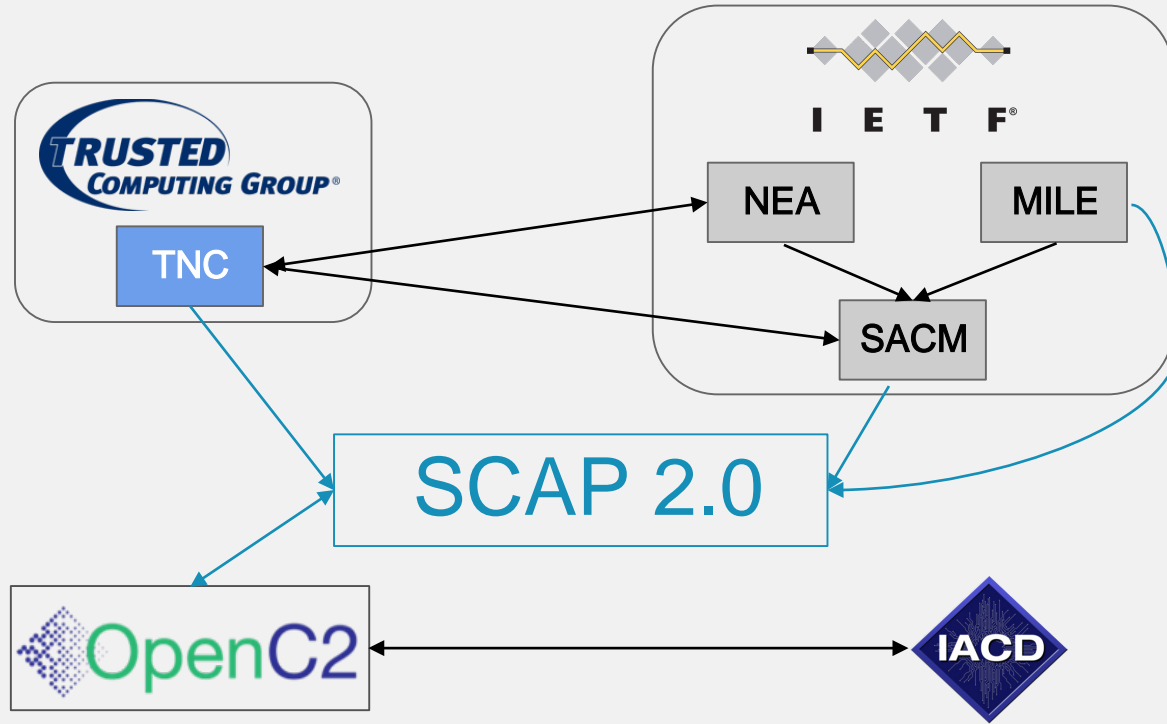
DeepLocker was developed as a proof of concept by IBM Research in order to understand how several AI and malware techniques already being seen in the wild could be combined to create a highly evasive new breed of malware, which conceals its malicious intent until it reached a specific victim. It achieves this by using a Deep Neural Network (DNN) AI-model to hide its attack payload in benign carrier applications, while the payload will only be unlocked if—and only if—the intended target is reached. DeepLocker leverages several attributes for target identification, including visual, audio, geolocation, and system-level features. In contrast to existing evasive and targeted malware, this method would make it extremely challenging to reverse engineer the benign carrier software and recover the mission-critical secrets, including the attack payload and the specifics of the target.

**WHY?**

# THERE IS NO INTEGRATION

- Proposed standards for integrations (CYBOX, OPENIOC, YARA, STIX/TAXII) are not widely adopted
  - Main proponent for integrations are security content providers
  - Automated tasks rarely involve more than two system
  - Automated remediation is not trusted
-

# CURRENT RESEARCH AND STANDARDS FOR SECURITY AUTOMATION







# AUTOMATION CAN BECOME THE LINGUA FRANCA OF IT SECURITY

**SECURITY ORCHESTRATION  
AND AUTOMATED RESPONSE  
(SOAR)  
IS BORN**



CYBERSPENSE  
ADAPTIVE SECURITY

DEMISTO

HEXADITE

 Phantom™

SWIMLANE

---

Hosted by:



**Anton Chuvakin**  
VP Distinguished  
Analyst

### Discussion Topics:

- What is SOAR
- Who should use SOAR
- How organizations are using SOAR
- The best practices in deployment and use of SOAR tools

Click "Attend" to add this webinar to your calendar.

[VIEW ALL WEBINARS](#)

## Polling Question 1

**Question: given what you know now, do you see your organization deploying a SOAR tool in the next 12 months?**

- A. Yes, a commercial tool
- B. Yes, an open source tool
- C. No, see no need or not ready
- D. No for other reasons
- E. Not sure

100  
answered

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

### How to participate in our polling

If you are in full screen mode – click Esc  
The poll question is on the "Vote" tab.  
Please click the box to make your selection.  
Upon voting you will see the results.

Thank you!



Q. Polling Question  
(please choose 1 answer)

A. Answer	<input type="checkbox"/>
B. Answer	<input type="checkbox"/>
C. Answer	<input type="checkbox"/>
D. Answer	<input type="checkbox"/>
E. Answer	<input type="checkbox"/>

**Gartner**

The first poll is open! Please provide you answer. Upon voting you will see the results.

Close

Ask a question

Attachments

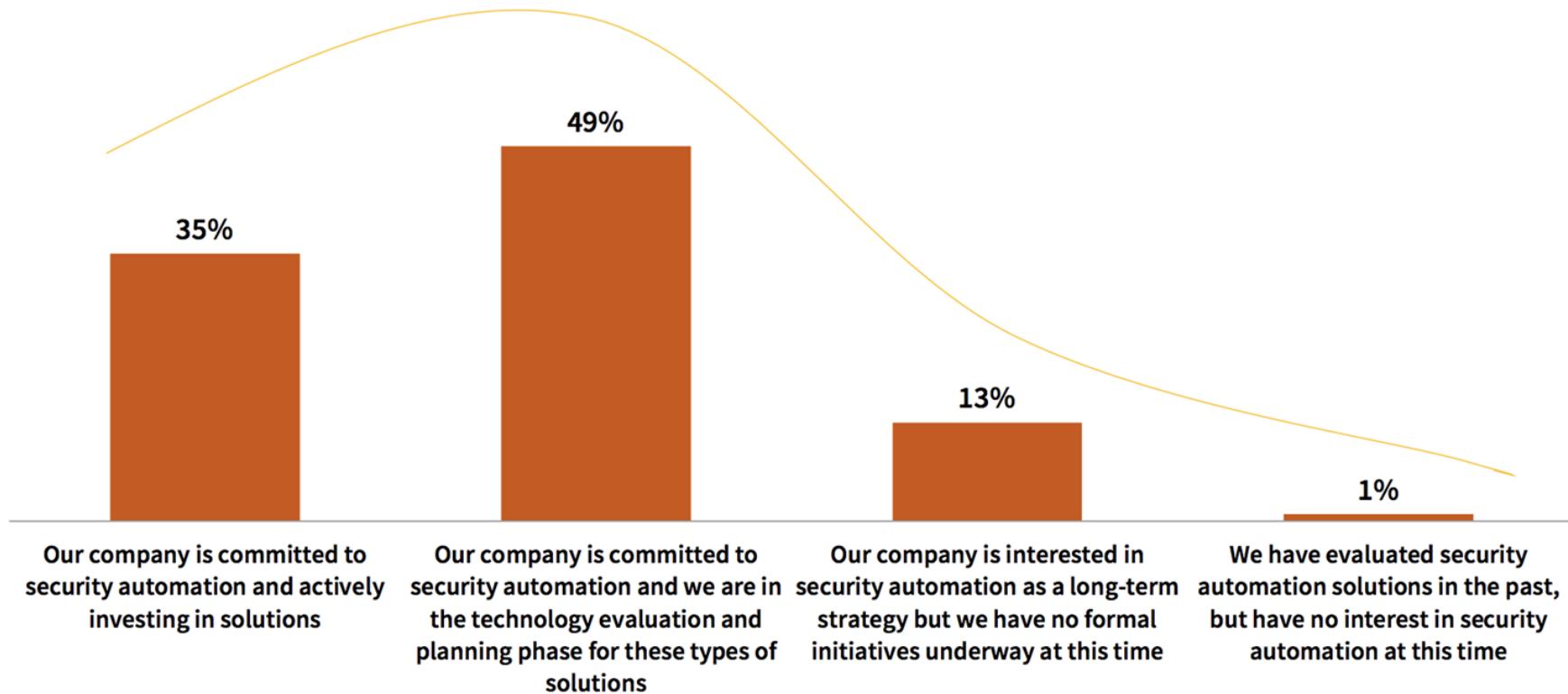
**Vote**


Rate this

Details

**Q**(1 of 1) Given what you know now, do you see your organization deploying a SOAR tool in the next 12 months?







“Early SOAR tools **assumed that every tool user is both a security expert and a skilled Python developer**, but fortunately those times are over. However, even today Python is useful for customizing playbooks of several of the popular SOAR tools, such as Phantom, Demisto and Swimlane. .. Vendors make it sound that integrating a SOAR tool with an SIEM or EDR tool is truly point-and-click. It may be, in some specific cases, but **clients report that in most cases these just don't work as expected** and an expert is needed to refine and fix it.”

Anton Chuvakin  
VP Distinguished Analyst

Augusto Barros  
Research Director

## Top open source projects

VS Code, React, and Tensorflow once again top our list of open source projects by contributor count. New to the list are projects that manage containerized applications, share Azure documentation, and consolidate TypeScript type definitions: Kubernetes, Azure Docs, and DefinitelyTyped. \*

	Contributors
1 <u><a href="#">Microsoft/vscode</a></u>	19k
2 <u><a href="#">facebook/react-native</a></u>	10k
3 <u><a href="#">tensorflow/tensorflow</a></u>	9.3k
4 <u><a href="#">angular/angular-cli</a></u>	8.8k
5 <u><a href="#">MicrosoftDocs/azure-docs</a></u>	7.8k
6 <u><a href="#">angular/angular</a></u>	7.6k
7 <u><a href="#">ansible/ansible</a></u>	7.5k
8 <u><a href="#">kubernetes/kubernetes</a></u>	6.5k
9 <u><a href="#">npm/npm</a></u>	6.1k
10 <u><a href="#">DefinitelyTyped/DefinitelyTyped</a></u>	6.0k

96M  
PROJECTS



# INTRODUCING ANSIBLE SECURITY AUTOMATION

# WHAT IS IT?

Ansible is Red Hat's enterprise automation platform to automate the provisioning and configuration of modern enterprise IT environments, from compute resources, like VMs and containers, to networks, all the way to the application layer.

**Ansible Security Automation** is a supported set of Ansible modules, roles and playbooks designed to unify the security response to cyberattacks in a new way  
- by orchestrating the activity of multiple classes of security solutions that wouldn't normally integrate with each other.

---

# WHAT DOES IT DO?

Through Ansible Security Automation, IT organizations can address multiple popular use cases:

- For **detection and triage of suspicious activities**, for example, Ansible can automatically enable logging or increase the log verbosity across enterprise firewalls and IDS to enrich the alerts received by a SIEM for an easier triage.
- For **threat hunting**, for example, 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.
- For **incident response**, for example, 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.

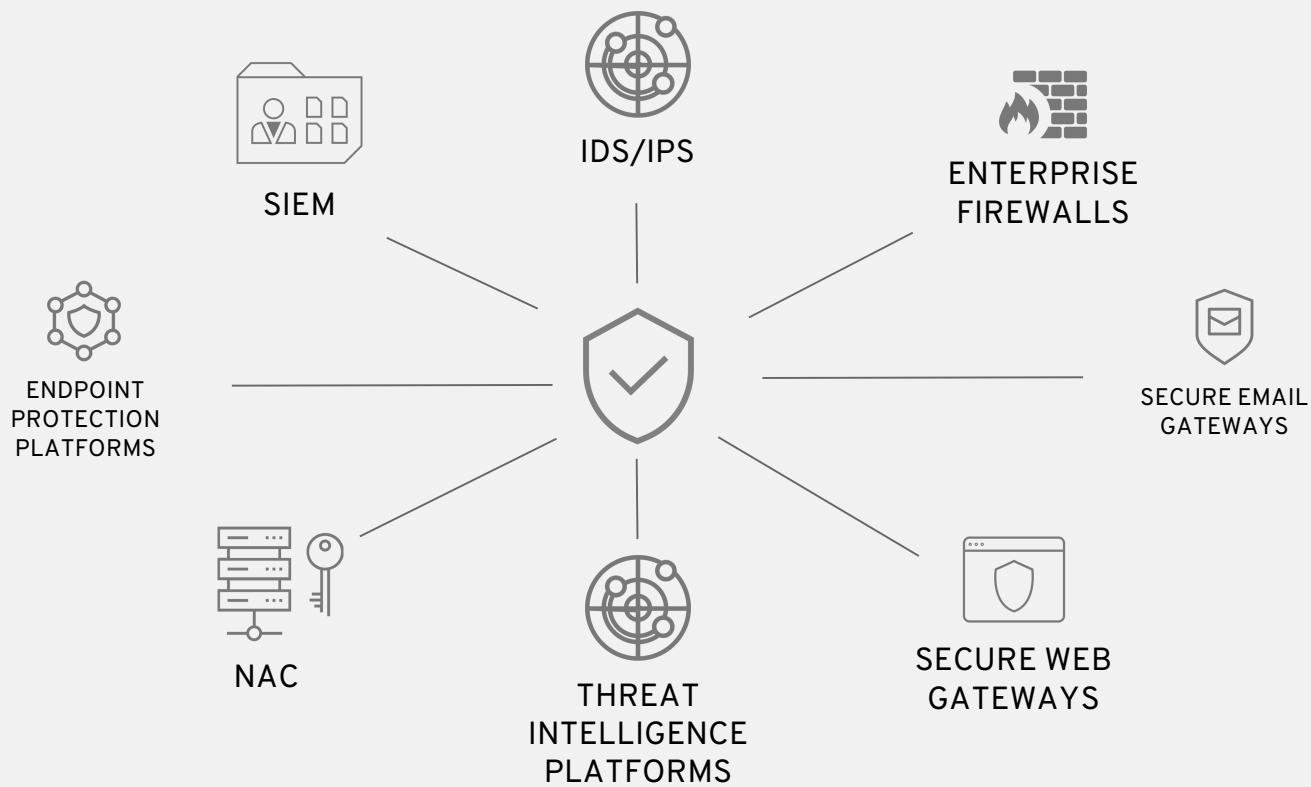
In technology preview, Red Hat's Ansible security automation platform provides support for:

- **Check Point** – Next Generation Firewall (NGFW);
  - **Splunk** – Splunk Security Enterprise (SE);
  - **Snort**
-

# WHO IS IT FOR?

Ansible Security Automation extends the Ansible agentless, modular and easy to use enterprise automation platform to support the following industry constituencies:

- **End-user organizations' security teams** in charge of Security Operations Centres (SOCs)
  - **Managed security service providers (MSSPs)** responsible for the governance of thousands of enterprise security solutions across their whole customer base
  - **Security ISVs** offering security orchestration and automation (SOAR) solutions currently using custom-made automation frameworks
-



splunk>



SIEM



IDS/IPS



Check Point  
SOFTWARE TECHNOLOGIES LTD.



ENTERPRISE  
FIREWALLS



SECURE EMAIL  
GATEWAYS



SECURE WEB  
GATEWAYS



THREAT  
INTELLIGENCE  
PLATFORMS



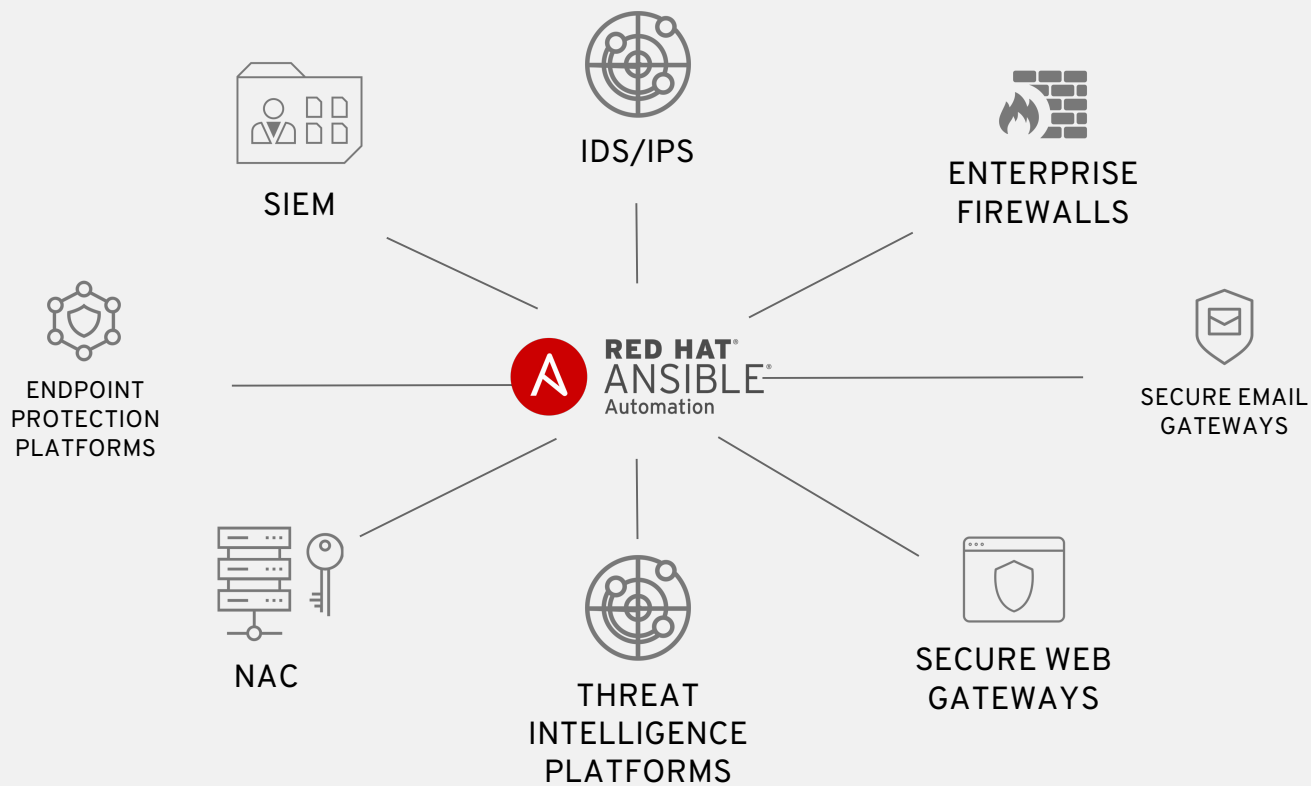
NAC



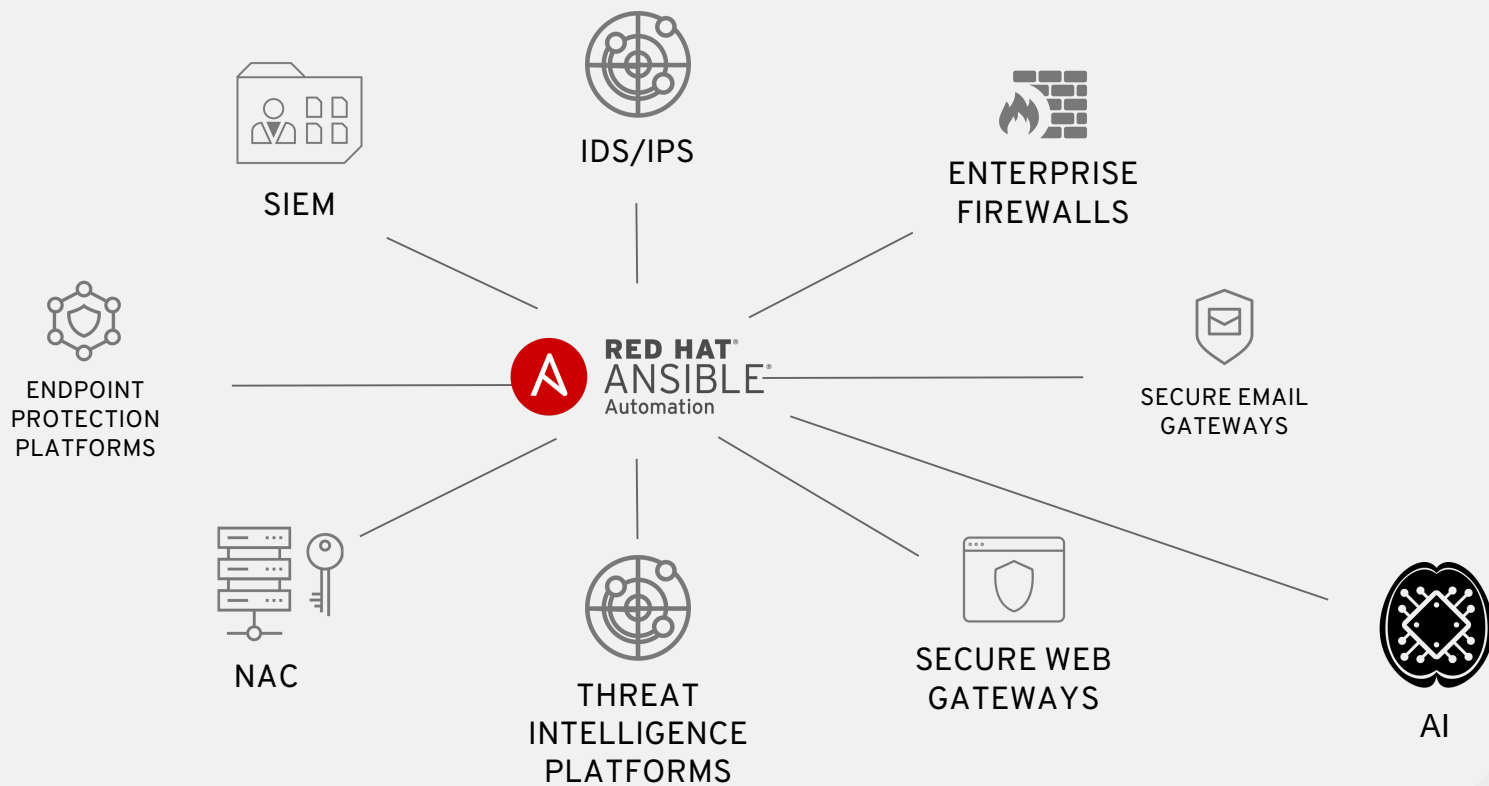
ENDPOINT  
PROTECTION  
PLATFORMS



RED HAT  
ANSIBLE®  
Automation







# HOW DO WE GET THERE?

- **Reconsider automation as a strategic defense, not just another tactical tool**
- Discover what automation tools are the most used in your org, and why
- Assess selected tools' capability to mitigate risks of automation
- Include automation software as target for pen-testing
- Pilot automated host and network security for non-critical applications
- Evaluate feasibility of centralized automation and lock down of platforms against rogue scripting
- Let your automation vendor know what security tools you are using, and how you'd like them to interact with each other
- **Pressure security vendors to start integrating with automation tools**

# This Japanese AI security camera shows the future of surveillance will be automated

By James Vincent | @jjvincent | Jun 26, 2018, 7:31am EDT

f   SHARE





#ANSIBLEAUTOMATES



redhat.

ANSIBLE