

# Accelerate your SOC!

Expand visibility. Reduce alerts. Respond faster.



**Meet Sara and Jeff.** They work in the Security Operations Center (SOC) at a Fortune 500 company. Pardon their appearance. **They haven't slept much lately.**

Today's SOC operations are challenged by:



A shortage of skilled team members



A lack of visibility into enterprise infrastructure



An overwhelming amount of alerts from disparate security products

There will be **3.5 million** unfilled cybersecurity positions by 2021.<sup>1</sup>

**46 percent of organizations** use tools from more than 11 security vendors, with some using 50 or more!<sup>2</sup>

Nearly **half of the daily alerts** an organization receives go uninvestigated.<sup>3</sup>



These challenges are dramatically impacting Sara and Jeff's efficacy in the SOC, putting their organization at risk. With an ever-expanding attack surface and constantly evolving attacks, time is more critical now than ever.

The average time it takes for an organization to detect a breach is **197 days**.<sup>4</sup>

That's a dangerous amount of dwell time for attackers!

## Moving forward

SOCs must operate like well-oiled machines, seamlessly integrating security technology and threat intelligence for automated, streamlined response.



Integrated Security



Threat Intelligence



Streamlined Response



In fact, **Gartner** predicts that by 2022, 50% of all SOC's will transform into modern SOC's with integrated incident response, threat intelligence and threat hunting capabilities, up from less than 10% in 2015.<sup>5</sup>

Studies show organizations that deploy automated security technologies can save over

# \$1.5 Million

on the cost of a data breach.<sup>6</sup>

## How can Cisco help accelerate your SOC?



**Expand** visibility across your entire attack surface, including the network, endpoint, internet, and cloud.

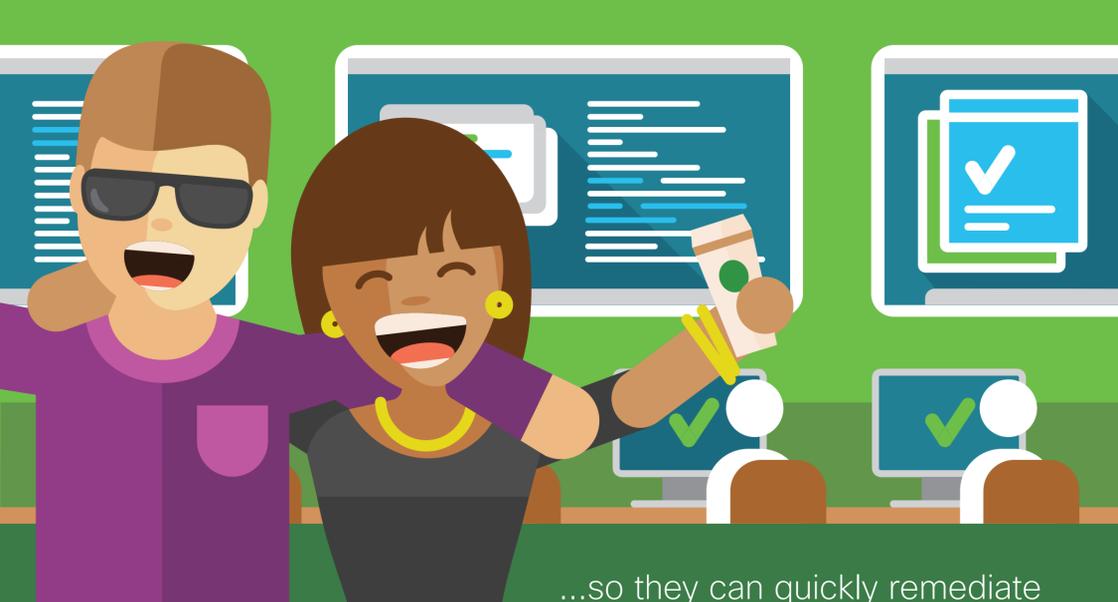


**Reduce** massive data sets to critical, high-fidelity alerts with advanced security analytics and integrated threat intelligence.



**Respond** faster to threats through simplified investigations driven by context.

With Cisco, Sara and Jeff can detect and investigate problems faster...



...so they can quickly remediate them and **move on**.

## Get started today



**Cisco AMP for Endpoints**  
Quickly discover and contain advanced malware.

Start free trial



**Cisco Threat Grid**  
Conduct in-depth malware analysis to better prioritize risks.

Start free trial



**Cisco Stealthwatch**  
Detect threats faster across the network and in public cloud infrastructure (even in encrypted traffic).

Start free trial



**Cisco Umbrella Investigate**  
Gain unique insight into attacker infrastructure.

Learn more



**Cisco Threat Response**  
Dramatically simplify security through automated integration. (Already included with several products.)

Learn more

For more information, visit [cisco.com/go/security](https://www.cisco.com/go/security).



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](https://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.