

# SECURITY AS A SERVICE

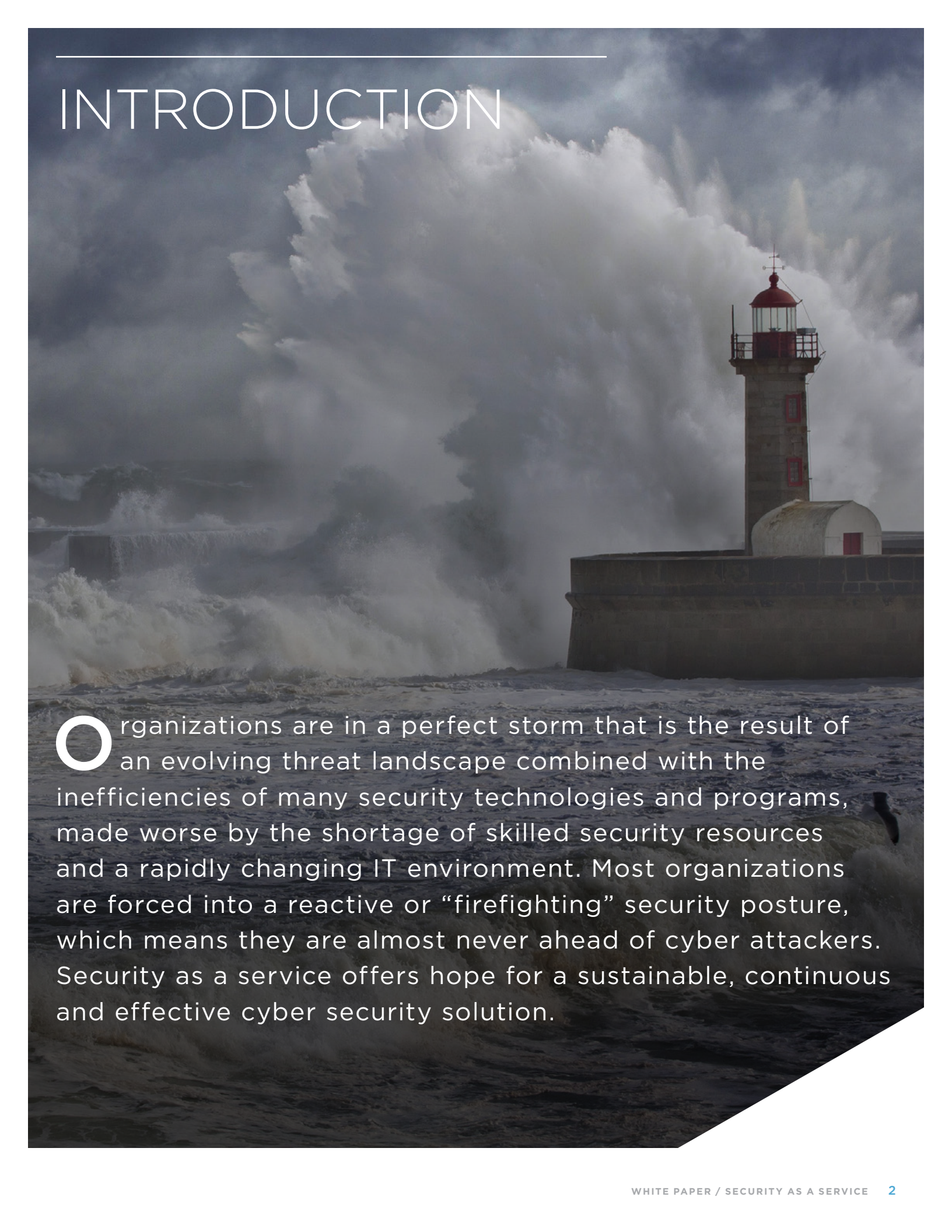
FOUR ELEMENTS OF FUTURE-PROOF SECURITY

© 2019 FireEye, Inc. All rights reserved. FireEye, the FireEye logo, and all other marks contained herein are trademarks of FireEye, Inc. or its affiliates. All other marks contained herein are the property of their respective owners. FIRE-19-0001-000001





# INTRODUCTION



Organizations are in a perfect storm that is the result of an evolving threat landscape combined with the inefficiencies of many security technologies and programs, made worse by the shortage of skilled security resources and a rapidly changing IT environment. Most organizations are forced into a reactive or “firefighting” security posture, which means they are almost never ahead of cyber attackers. Security as a service offers hope for a sustainable, continuous and effective cyber security solution.





# Current and emergent cyber security challenges

**M**ost organizations are not security companies — they are governments, financial institutions, consumer goods companies — cyber security is not their area of expertise. The security they need consumes resources that could otherwise be invested in their core interests.

For nearly two decades, the approach to cyber security has been to add more technology to the security infrastructure. Not only has this approach failed to solve the problem — it has also made it more complex. New technology investments operate in silos and lack the integration required for intuitive and effective interoperation. The result is data overload from many different systems which each generate undifferentiated, uncorrelated alerts. Even if a system manages to detect a threat, true dangers cannot be quickly confirmed, located and identified.

And through all this, the threat landscape has continued to grow and evolve. The demands on IT departments continue to increase. Emerging computing technologies are viewed as major business enablers — as they should be. Security departments are expected to help their organizations operate securely in Internet of Things (IoT) and bring-your-own-device (BYOD) environments. As the attack surface expands, the frequency and number of attacks continues to increase and attacks have become more targeted at individuals organizations and even entire industries. The alert reactive posture that was once considered a best practice simply cannot handle the volume of alerts that security teams face.

# Threat detection is not an end goal

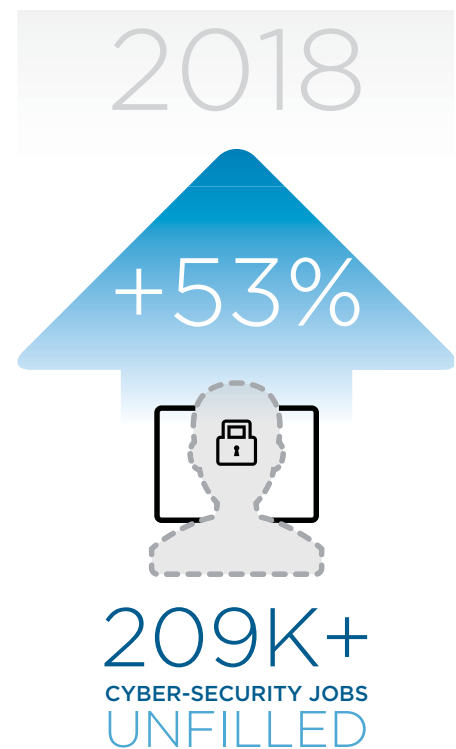
**T**raditional detection products generate high numbers of false positives and more often than not, true threats are missed entirely or buried in a sea of alerts. Most of these products lack the context to help analysts understand and help prioritize alerts.

Organizations need to go further than just threat detection. They need to be able to triage alerts and determine how to disposition them. But tools to help investigate and analyze attacks often cannot rapidly or adequately identify the motivations or methods of attackers, giving them more time to inflict damage. All of these technology shortcomings force security analysts into busywork that not only means lost productivity but increases organizational risk.



# Experienced staff are a dwindling resource

**H**iring more personnel to manage siloed security products might seem like the obvious solution. Not only is this beyond most budgets — it's often impossible, since the industry has a skills deficit. The lack of skilled resources is one of the biggest challenges plaguing the security industry. More than **209,000 U.S.-based cyber security jobs are unfilled**. That number has been steadily growing for the past five years and is expected to grow by another **53% by 2018**.<sup>1</sup> An organization cannot always expect to find a security analyst or incident responder that has experienced attacks from nation-state adversaries or major cyber crime syndicates. And if they do find such a professional, they have no assurance that they can retain that expert when demand is so high. What's worse is that many specialized security resources are often only needed for short bursts of time, making it even more difficult to justify their cost.



## Security capabilities can be extended intelligently

**M**any organizations want to build comprehensive security capabilities in house. But when they ultimately discover they can't, they sometimes decide to use a vendor, which is often construed as an outsourcing. This appears to create a 'build vs. buy' decision, but as the scope of the security problem increases and experts and expert providers become harder to find, enlightened organizations do not view the decision in such binary terms. Instead, they approach this problem as they would a logistics or financial challenge — supplementing internal experts (who deeply understand their business) with help on the commoditized low-end and specialized high-end.

*For example, every company that ships finished goods has an in-house shipping or logistics department, but they outsource truck maintenance (the low-end) to a fleet management company and complex coordination of shipping routes (the high-end) to freight-forwarders. They know that it would be inefficient to perform such tasks in house.*

<sup>1</sup> Setalvad, Ariha (March 31, 2015). "Demand to fill cybersecurity jobs booming."

## THE EMERGENCE OF

# Security as a Service

**C**omplex infrastructures, lack of expertise, the evolution of computing devices and other issues are not entirely unique to security. Attempting to solve those problems with technology, personnel and outsourcing is also common. But over time, as organizations grow and times change, they realize they cannot maintain the level of in-house security needed to maintain their defenses. The dollars needed for effective in-house security might be far better spent on their core interest to build additional revenue.

This has seen the rise of the “as-a-service” model in a variety of other domains ranging from customer relationship management to human resource automation. Security is ripe for this disruption. Adopting as-a-service models enables organizations to offload specific functions, such as those that can be automated by an experienced service provider or those that are so specialized that a partner should be left to perform them at scale. As-a-service providers focus on delivering key capabilities to customers while maintaining the latest and greatest hardware, software and experts dedicated to those capabilities. The best security teams seek out and take advantage of the reach and expertise of a service provider who can ensure the best possible defense, leaving their organization free to focus on its core interest.

Some providers have used the security-as-a-service terminology to describe any security function delivered from the cloud, but this is a narrow definition. Cloud is just a form factor — not every organization would adopt it. Security as a service is also not just synonymous with outsourcing. Organizations should retain ownership and control of critical security functions.

Security as a service is a flexibly deployed combination of technology, intelligence and expertise that provides organizations with situational awareness of the threats that they face and the ability to easily manage the prioritized actions for their security program. The resultant proactive posture enables organizations to anticipate and prepare for threats that target them. In-house security teams can shift their focus from security to risk management, which helps increase organizational agility with a clear understanding of risks and mitigation strategies.







THE ESSENCE OF

# Security as a Service

**S**ecurity as a service generally promises simpler yet more effective cyber security for organizations. To a skeptical reader that might sound like the panacea offered by every security company's marketing team. However, we can clearly identify four capabilities that distinguish genuine security as a service from partial or incomplete solutions that fail to address organizational security challenges.

## EXPERTISE ON DEMAND

Core security-as-a-service offerings should include professionals such as forward deployed threat intelligence analysts, experienced incident responders, security operations analysts and risk managers. “On-demand” availability means that organizations should be able to access such experts exactly when needed, within the context of their current situation. Examples where organizations might need help include getting answers to questions about alerts, analyzing malware or being able to delegate and access all the capabilities of a security operations center.

## FAST, FLEXIBLE DEPLOYMENT

Like other as-a-service solutions, security as a service must be quick to deploy — organizations should be able to be up and running in a matter of hours. In addition to deployment speed, flexibility includes aspects of elasticity and visibility.

Elasticity requires that organizations be able to match their needs (based on their security maturity) with provider capabilities. Deployment form factors, including on premise, cloud-based, hardware, software, self-service and fully managed, must be selectable. Pricing would ideally be subscription- or use-driven to favorably conform to security consumption. This would allow organizations to increase and reduce spend as needed, based on actual service usage.

Visibility into your security operations — an awareness of what security activities you conduct, and how you conduct them — keeps your security program under your control, whether you use a partner’s expertise or your own.

## ANSWERS NOT ALERTS

Security-as-a-service solutions should eliminate the pain organizations feel from the alert overload generated by conventional security products — especially since most of those alerts are unreliable. To achieve this, the solution must offer high fidelity detection with low false positives. Then, by applying intelligence, analytics and expertise, the solution must dramatically reduce the volume of alerts that require human attention. Finally, all alerts must include some context so that they can be correctly prioritized and understood so organizations can respond to them quickly and correctly. Intelligence and context may be derived from forward-deployed intelligence operatives or even gathered from a community of organizations that share similar target traits. The goal is to sidestep millions of time-wasting alerts and identify and resolve the most critical alerts as fast as possible.

## EFFICIENT INTEROPERABILITY

Security-as-a-service solutions must take advantage of existing customer security investments — expecting a customer to replace years of past investment is not reasonable. Ideally, the solution must increase the effectiveness of existing with intelligence, analytics and expertise. The solution must be open, with APIs, integrations and the ability to connect to the existing security infrastructure. This should help simplify processes, automate actions and eliminate human error. Taken together, all these benefits should enable organizations to go beyond mundane alert management and triage and instead focus on higher value defensive efforts including advanced practices, such as hunting for malicious activity in their environment.

---

Visibility into your security operations keeps your security program under your control, whether you use a partner’s expertise or your own.

---





# Availability of complete security-as-a-service solutions

**B**uilding or buying adequate defenses against modern computing threats requires years of research and development, engineering and forward-deployed intelligence resources. There are very few viable options for meeting the new cyber threat landscape head on and overcoming today's sophisticated attacks.

Security as a service is a financially and operationally manageable option, but the term is not firmly and universally defined. Smart organizations will discover a significant payoff to researching providers, evaluating offerings and determining the correct level of service they need with respect to expertise on demand, flexibility, answers over alerts and efficient interoperability. Security as a service should be expected to deliver the security capability and scalability critical to sustaining the well-being of your organization.

[Learn more](#) about Security as a Service.

---

**FireEye, Inc.**  
1440 McCarthy Blvd. Milpitas, CA 95035  
408.321.6300 / 877.FIREEYE (347.3393) / [info@FireEye.com](mailto:info@FireEye.com)

[\*\*www.FireEye.com\*\*](http://www.FireEye.com)

© 2016 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc.  
All other brands, products, or service names are or may be trademarks  
or service marks of their respective owners. WP.SAAS.EN-US.092016

