



---

# Marketing Cybersecurity: eBook Samples



## Our Philosophy

---

At glassCanopy – we love eBooks.

They make ideal “bait” when trolling for top-of-funnel leads and create a great first impression for your brand – they also provide valuable collateral for your sales force. What’s more, eBooks can be easily chopped into SEO-optimized blog posts and provide the context needed to quickly create videos, datasheets, case studies, and other collateral.

However, to be effective, the research, writing, and overall quality of the eBooks must be top-notch. Nobody feels good about giving out their contact information in exchange for a thinly disguised sales brochure.

Many of our clients felt that no one outside their organization could write an ebook that wouldn’t come off as just marketing fluff. That was **before** they started working with glassCanopy. Quarter after quarter, we produce in-depth eBooks on technical and complicated subjects that our clients (and *their* clients and customers) love.

Here’s a taste of what we can do...

---

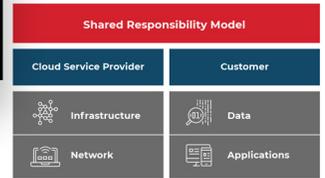
## TABLE OF CONTENTS

- 04 Introduction
- 05 Problems Lurk In the Cloud
- 06 New Threats in the Cloud
- 08 The Impact of the Shared Responsibility Security Model
- 09 Rapid Change and High-Volume Feature Releases
- 10 Cloud-Specific Threats
- 11 Access Control Issues in the Cloud
- 11 Additional Complexity and Gaps Caused by Hybrid and Multi-Cloud Architectures
- 13 How Next-Generation MDR Addresses Cloud Security Challenges
- 14 Cloud-Native
- 14 Automation and Artificial Intelligence
- 15 Continuous Security Posture Management (CSPM)
- 15 Full Response
- 17 Paladion's Next-Gen MDR: At-Asset
- 18 Applying the Power of AI and Machine Learning
- 20 High-Level Architecture
- 21 Solution Components
- 22 Threat Response
- 25 Conclusion
- 26 About Paladion



### THE IMPACT OF THE SHARED RESPONSIBILITY SECURITY MODEL

Cloud customers work within the shared responsibility security model. A CSP is responsible for securing its infrastructure and network. Their SecOps team monitors the compute, storage, and network hardware comprising the cloud platform. A customer, in turn, is responsible for their own data and application security, including patching and access control issues that arise with working in the cloud.



This shared responsibility model makes a great deal of sense. The CSP cannot be expected to know which users are authorized to use the software installed in the customer's cloud. Nor is it realistic for the CSP to remember the specifics of how the customer wants to secure its data and applications.

However, the shared responsibility model leads to a lot of problems too. At a minimum, the cloud becomes yet another digital asset SecOps has to monitor by installing cloud-based versions of on-premise SIEM systems, Intrusion Detection Systems (IDS), and other security tools.

### ACCESS CONTROL ISSUES IN THE CLOUD

Who accessed what? That's one of the most critical questions facing SecOps teams as they analyze session logs and reports.

Deciphering the access control map becomes more complicated in the cloud. Users may get in using a "side door" by accessing digital assets remotely without having to pass through the corporate network. Cloud Access Security Brokers (CASBs) can help – as can identity access systems that have been set up for cloud use.

*Using cloud deployments can inadvertently set up side-door access to critical data and systems.*

### ADDITIONAL COMPLEXITY AND GAPS CAUSED BY HYBRID AND MULTI-CLOUD ARCHITECTURES

Few organizations are one hundred percent in the public cloud. Many businesses have data across on-premise, public, and private cloud architectures. Others have applications and data that span AWS, Azure, and Google cloud. Such hybrid cloud architecture sets up a tricky security dynamic for SecOps to track by requiring many overlapping and repetitive systems for multiple cloud instances, further increasing the possibilities for human error and the need for automation.

### NEXT-GEN MDR IN ACTION

A Next-Gen MDR platform should be able to provide the detection and response service timeline depicted in the "Left-of-Hack" and "Right-of-Hack" diagram in Figure 1. The figure offers a useful way to visualize the timing of threat detection and response actions. Each of the six steps within this workflow represents processes occurring along the timeline of an attack. The "Left-of-Hack" portion includes the proactive steps taken to detect threats before they occur. The earliest form of detection is threat anticipation, followed by threat hunting, which happens closer to the time of a hack, while security monitoring serves as the detection capability occurring up to the moment of a possible compromise.

**Left-of-Hack to Right-of-Hack Services™**

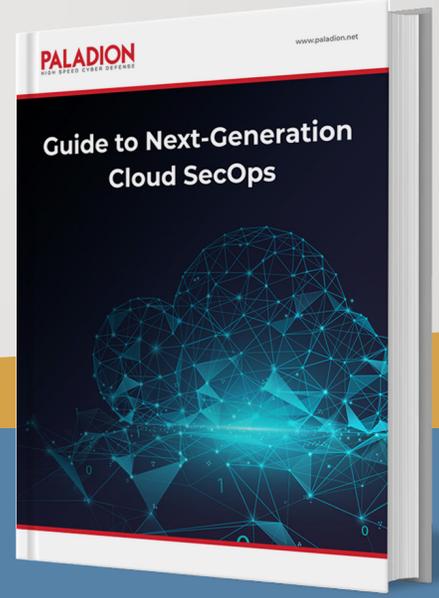
Timeline: Early (Time to Detect) | Likely Compromise | Immediate (Time to Respond) | Post-Attack (Time to Restore)

- Threat Anticipation:** Threats are identified by analyzing network traffic and logs.
- Threat Hunting:** Proactive search for threats using machine learning and manual analysis.
- Security Monitoring:** Continuous monitoring of network traffic and logs for anomalies.
- Incident Response:** Immediate action to contain and eradicate threats.
- Auto-Containment:** Automated actions to isolate affected systems.
- Response Orchestration:** Automated workflow for incident response and remediation.

Figure 1 - Threat detection and response workflow represented by proximity to the time of a compromise.

The "Right-of-Hack" includes the time-to-respond workflows, which follow a similar time-based pattern. The incident analysis takes place immediately after an attack, followed by auto-containment, and then response orchestration.

*A robust MDR solution includes both pre- and post-attack activities.*



**Client:** Paladion

**What they do:** Next-gen managed detection and response (MDR)

**Summary:** A introduction to how next-generation managed detection and response (MDR) solutions allow cloud security operations to take a proactive approach to cybersecurity.

**Want to read the entire 26-page eBook?**

**CONTACT US**

## INTRODUCTION

93 percent of all network breaches include a phishing or spear phishing attack.

For the most part, the perimeters of most vigilant organizations are reasonably tight. Firewalls are in place, servers are patched, and physical security is in place. However, email is a giant gaping hole in your network defenses.

**Email is the vector for virtually all the bad things that keep you up at night.**

What's worse is that the bad guys are using email to target every IT person's greatest weakness: their employees.

If you think that your organization is safe from email-borne attacks because you have set up Office 365 with email security packages like EOP, Proofpoint, McAfee, or Barracuda, you need to think again. These security packages will not reliably stop spear phishing or zero-day attacks.

According to a 2016 Vanson Bourne study of IT decision makers, 84 percent of organizations said a spear phishing attack successfully penetrated their organization in 2015. However, 71 percent also indicated that they already have some form of email security technology in place.



## Email security is clearly broken.

The problem is twofold:

- 1. Technology:** Most email "security" systems are really just glorified spam filters. They were designed to stop known mass email attacks. The underlying architecture of these solutions isn't suitable to catch zero-day threats or one-off spear phishing emails.
- 2. People:** Many employees will click on or respond to a well-crafted phishing or spear phishing email if it lands in their email inbox. Despite education efforts, 20 to 30 percent of recipients open standard phishing messages that arrive in their inbox and 12 to 20 percent of those click on any enclosed phishing links. These already high rates more than double when looking at spear phishing email!

We'll walk through the scope of the problem and then discuss how you can quickly close up the existing security holes in your Office 365 setup.



1. The line figures are taken from Verizon's 2016 Data Breach Report, and the higher numbers are from an August 2016 study by Friedrich-Alexander University, but many other studies show similar results.



Figure 2 - The progression of a spear phishing attack, starting with research of the target organization and identification of a specific individual inside the organization, followed by a series of emails intended to build trust with the target.

Figure 2 shows a typical progression of a spear phishing attack. The attacker's first step is to research Widget Co. to get a sense of how they can best mount a successful spear phishing attack. After cataloging the executives in the "Our Team" section of the Widget Co. website, the attackers create a cross-reference of social graphs, using Facebook and LinkedIn accounts to build lists of who knows whom inside Widget Co. Then, by piecing together the social information, the attackers are ready to go spear phishing.

The attackers find an HR employee at Widget Co. named John Smith. Posing as Mr. Smith, the hackers target Smith's Facebook friend and colleague, Jeff Jones, an HR manager at Widget Co. To build trust in the faked email address, the hacker posing as Mr. Smith sends his "friend," Mr. Jones, a note asking about the family vacation he is currently on (according to pictures posted to Facebook). If Mr. Jones responds, the hacker is off to a good start. He's successfully impersonating another Widget Co. employee and is starting to build trust in the faked email with his target. Mr. Jones replies and says he is enjoying his time away with his family. The two continue to banter about Mr. Jones' family vacation as well as things going on in the office, including the names people that have been researched and associated with the social circle.

1

## Secure's Solution

All Vade Secure email solution provides spam, graymail classification, and the most robust email security solution on the market.

**Initial Filtering:** Emails are analyzed for known phishing and malware signatures, including executable files. This quickly weeds out all spam and mass attacks.

### Anti-Malware:

- We read the code embedded not just in executable files but in Office documents, PDFs, and more.
- This in-depth proprietary defense system is bolstered by two complementary anti-virus solutions.

**URL Sandboxing:** All URLs are examined to be sure they do not link to malware, phishing sites, or any other malevolent site. Unlike most URL exploration engines, Vade Secure explores the URL both when it first comes through the system and also again whenever a user attempts to click on a link, thus defeating time-bombed URLs.

**Artificial Intelligence:** Any remaining messages are analyzed for unknown malware and phishing tactics to prevent spear phishing and zero-day attacks that would otherwise get through the filters. Our rules-based engine is based upon processing billions of emails every day, so it is constantly learning and improving.

- **Identity Verification:** Our Identity Match™ system considers hundreds of subtle technical and behavioral factors to determine if the sender is who they claim to be to protect against email imposters.

- **Domain Verification:** The sender's domain is double-checked for authenticity.

- **Content Analysis:** Vade Secure performs a deep analysis of every email to look for attempts from hackers to steal personal information. The artificial intelligence engine creates a warning if there are sensitive data requests within the email, like asking for personal information or credentials.

**Human Intelligence:** Vade Secure runs a 24/7 global threat intelligence center with email security experts. They constantly monitor the information that comes in so that we can identify new and interesting threats.

**Spam Control:** Vade Secure achieves a 99.99 percent catch rate with essentially a zero percent false-positive rate (<0.00001 percent).

**Commercial Email/Graymail Management:** Delight your customers with commercial email categorization and one-click auto-unsubscribes.

13

Vendor Comparison	Proofpoint Essential	McAfee	Vade Secure	Barracuda	EOP
<b>Known Threats</b>					
<b>Basic Signature-Based Protection for Known Threats</b>	✓	✓	✓	✓	✓
Blacklisted Spam	✓	✓	✓	✓	✓
Blacklisted Malware	✓	✓	✓	✓	✓
Blacklisted Phishing	✓	✓	✓	✓	✓
<b>Unknown Threats</b>					
<b>Zero-Day Malware/Phishing/Spam Detection</b>					
Basic Machine Learning & Heuristics	✓		✓		
Complex Reputational Analysis	✓		✓		
Advanced Artificial Intelligence Based Analysis			✓		
<b>Anti Phishing Detection and Protection</b>					
Real time URL Exploration			✓		
Time-Bombed URL Protection	✓		✓	✓	
Sensitive data request	✓		✓	✓	
Exact Spoofing Detection	✓		✓	✓	
Similar Sender Spoofing Detection	✓		✓	✓	
DKIM Sender Authentication	✓	✓	✓	✓	✓
SPF Sender Authentication	✓	✓	✓	✓	✓
<b>Convenience</b>					
Low Priority Email Classification	✓		✓		
One-Step Unsubscribe	✓		✓		
Advanced Unsubscribe	✓		✓		
Archive	✓	✓	✓	✓	✓
SMTP Retention	✓	✓	✓	✓	✓
<b>Deployment</b>					
Cloud / SaaS	✓	✓	✓	✓	✓
On premise	✓	✓	✓	✓	✓
30' installation	✓	✓	✓	✓	✓
Exchange Compatible	✓	✓	✓	✓	✓
Office 365 Compatible	✓	✓	✓	✓	✓
Google Apps Compatible	✓	✓	✓	✓	✓
Zimbra (Zimlet)	✓	✓	✓	✓	✓
cPanel Plugin	✓	✓	✓	✓	✓

11



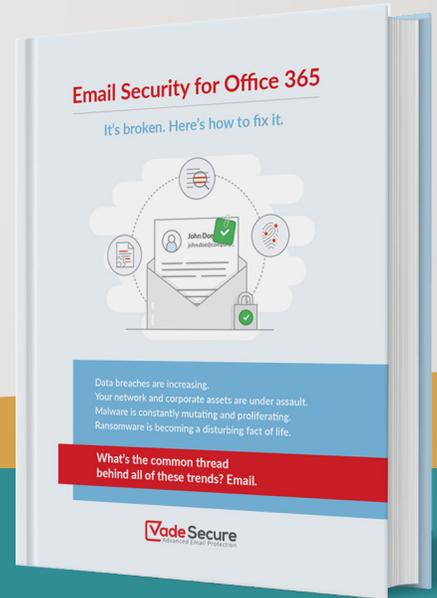
**Client:** Vade Secure



**What they do:** Predictive corporate email security



**Summary:** An introduction to the evolving email threat landscape and why you must implement advanced email security specifically for Office 365.



Want to read the entire 15-page eBook?

CONTACT US

**SWIMLANE**

## Pressures Faced by Cybersecurity Teams

Security managers work in a pressurized environment which seems to create new varieties of stress on a regular basis. The overall threat level continues to grow. Beyond that, however, the "surface area" of risk exposure expands over time. In tandem, the number of security alerts increases – creating a situation where staffers and their incident response capacity can become overwhelmed. This reality is compounded by the fact that businesses today are more reliant on IT than ever before. In many cases, IT defines the organization in strategic and operational terms. When a bank essentially becomes an IT entity that happens to lend money, for example, the stakes for cybersecurity become higher than ever.

**Increasing Attack Surface Area**

Organizations today face new types of threats. Evolving IT platforms such as IaaS and SaaS, coupled with innovations in mobile devices, conspire to increase the spectrum of risk exposure. For instance, the practice of placing data assets and applications on cloud infrastructure expands the security perimeter. The popular trend of hybrid IT, which blends on-premises and cloud infrastructure, results in more – and more diverse – systems to monitor for security incidents.

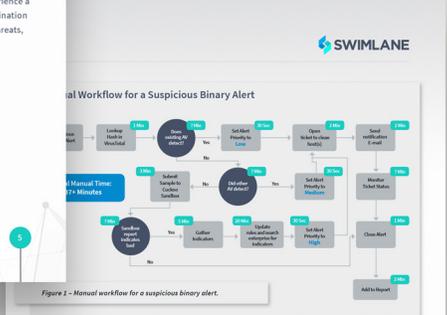
The growing use of "As-a-Service" solutions like Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) now places critical systems outside the firewall and beyond your direct control. However, data security and incident response are still your responsibilities. For example, with a SaaS solution such as Salesforce.com, an organization generally has its entire customer list in the cloud and accessible by third party entities and contract-based employees.

**SWIMLANE**

Even with security incident and event management (SIEM) tools, which are designed to correlate security data across multiple systems, there can still be a need for manual research of adjacent event data and so forth – tasks that slow down incident response and potentially overwhelm the team.

- **Staff turnover resulting in loss of institutional/tribal knowledge** – When cybersecurity staffers leave teams that operate on complex rules and informally defined workflows, incident response can only suffer. Getting a team member on-boarded and up to speed also requires an investment of time and money. When people leave, that investment is lost.
- **Compliance and regulation's effects on security policy** – New rules, driven by changing regulations, mean new headaches and more potential missed procedures.

These factors also tend to overlap. The high-turnover cybersecurity team may experience a lack of coordination between toolsets and personnel. A team that lacks good coordination between toolsets and personnel may experience inconsistent response to critical threats, and so forth.

At the rate of ~12 alerts handled per hour, a team of 5 cybersecurity staffers can get on top of about 500 alerts per 8 hour shift. That's a lot of alerts! But, given a workload of 10,000 alerts per day, they're ignoring 95% of the alerts they receive. (Of course, ideally, there should be more than one shift running. However, only 24% of enterprises have 24x7 monitoring in place using internal resources.)

**Effects of Triage and Prioritization**

How do most teams handle this overload? They adopt a triage/prioritization approach. The team establishes parameters for which alerts will receive attention and which will be ignored. This is an understandable response to being flooded with alerts, but it's quite flawed.

**SWIMLANE**

Triage inevitably leads to missing a real attack at some point. There is no way to skip a major portion of alerts and stay in front of all valid threats. Indeed, a number of major breaches in recent years have been attributed, in retrospect, to seemingly minor alerts being overlooked.

In addition, any process that essentially turns people into machines is going to have consequences for the business. On a practical level, the speed of response is never going to be good enough. Security demands the capability of real time rapid response. The problem is that humans are incapable of 100%, always on, immediate response. On a personal level, security pros did not get into security to spend their time performing administrative tasks like cutting and pasting data. Security pros generally want to be involved in challenging security work, but the great majority of security operations in a triage environment are highly administrative. Ultimately, it's a poor use of expensive human capital.



Figure 2 – The alert triage process lets cybersecurity staffers review alerts selectively based on criteria that establish the seriousness of the threat.

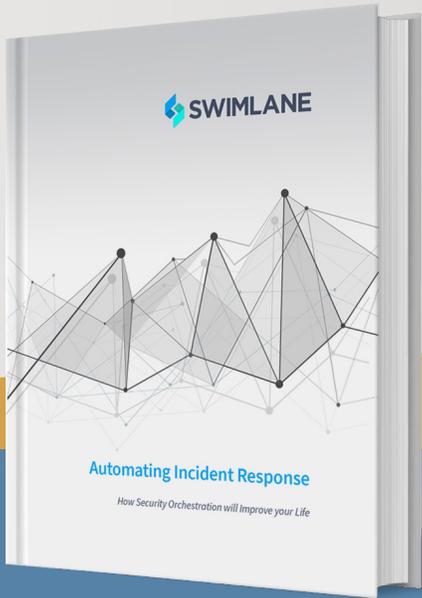
**SWIMLANE**

## About Swimlane

Swimlane automates security operations for enterprise teams

Swimlane is a security operations management platform that centralizes an organization's security alerts, automates resolution, and dynamically produces metrics-based dashboards and reports. Using software-defined security (SDSec) methods and security orchestration, Swimlane automatically responds to alerts, automates the implementation of security controls, and protects the organization from future attacks – all at machine speeds.

To arrange for a demo of the Swimlane solution or to speak with one of our security architects to see if security orchestration would be helpful to your organization, please contact us at 1.844.SWIMLANE or email us.



**Client:** Swimlane



**What they do:** Security Orchestration Automation and Response (SOAR) platform



**Summary:** An introduction on how using security orchestration to automate incident response improves security operations.

**Want to see the entire 18-page eBook?**

**CONTACT US**

## Privileged Access Management (PAM) for Healthcare

### Healthcare organizations face a unique set of IT security challenges:

- High-profile target status
- Comprehensive regulation and compliance burdens
- Large privacy responsibilities
- Rapidly evolving complications and new technologies

Of course, health IT administrators face an additional burden in the form of new technologies such as e-health initiatives, smart devices, IoT, and BYOD policies. Although IT is being held responsible for locking down this new array of possible data breaches, they often don't get that day in their actual role. What's worse, the security infrastructure that comes bundled with these new initiatives is often badly lacking and most of the data gets uploaded to the cloud by default.

Most cyber attacks involve the misappropriation of privileged credentials in some fashion. In fact, a whopping 80 percent of recent IT breaches involve the misuse of privileged credentials, according to a recent Forrester Report<sup>1</sup>. These privileged users include employees, external providers, cloud providers, automated users, and third party contractors providing application and other maintenance.

What's even more disturbing is that while the average healthcare data breach took 233 days to discover, breaches involving privileged users took 607 days. So, we probably won't know how bad 2016 really was until 2018<sup>2</sup>!

Controlling and documenting the actions of privileged accounts is central to ensuring security, achieving compliance, and protecting privacy. In this paper, we'll explore why so many healthcare organizations have adopted WALLIX for Privileged Access Management and the true security protection that it provides.

<sup>1</sup> Privileged Identity Management Risk, Forrester, Q3  
<sup>2</sup> <http://www.healthcareitnews.com/news/healthcare-privileged-access-management-2016-08-01>



### High-Value Targets

Patient medical records have enormous value on the dark web and black markets. As recently as 2013, medical records were generally valued at \$50 each due their value in providing critical information to enable identity theft. While the price of medical records in 2015 and 2016 have dropped (street prices down to \$1.50 - \$10 each), that's still roughly the same value as the complete profile for a stolen credit card. And medical records are generally not nearly as well protected as financial data.

Therefore, it is no surprise healthcare organizations find themselves so frequently targeted by hackers. In fact, according to HIRA Journal, 2016 saw the greatest number of self-reported healthcare data breaches of 500 records or more since records have been kept! Although the number of records exposed was down to 16.5 million, from 2015's staggering 113 million (one-third the US population), the number of entities affected rose by 20 percent.

### The #1 cause of breaches in 2016 in Healthcare? Unauthorized access.

While many sectors have seen increasing threats, the healthcare sectors in North America and Europe have seen a disproportionate increase in the numbers and sophistication of the attacks that they face. This is truly a crisis.

### A Moral Obligation

Healthcare is a business, but it's not like most businesses. The industry's "product" is the health of the patient. Human lives are at stake. Practitioners, as well as everyone in the organization who supports them, have a duty to the well-being of the patient. They also have a duty to the patient's right to privacy and need to respect the code of deontology.

*"I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."*

The modern Hippocratic Oath, generally credited to Dr. Louis Lasagna

This oath can be viewed as relevant to everyone who works in healthcare, including the IT department. It's important to not lose sight of the fact that protecting patient confidentiality is the true goal of IT security in healthcare, not just locking security compliance boxes. Robust PAM is a central element in providing true security to patients.

### A Fiduciary Duty

Patient privacy is a key business requirement as much as it is a legal and ethical mandate. Privacy issues can affect the healthcare organization's standing. Appearing lax about patient privacy can lead to costly business and reputational impacts.

<sup>2</sup> <http://www.healthcareitnews.com/news/2016/08/01/Healthcare-privileged-access-management-2016-08-01>



### Conclusion

The bottom line is that healthcare IT systems need to route all privileged access through PAM in order to ensure that this access is monitored, managed, and audited.

Healthcare organizations have a tremendous responsibility to their patients, staff, and stockholders. This responsibility is matched by the challenge of high regulatory hurdles and aggressive attackers. In order to meet these challenges, companies must invest in managing privileged accounts.

WALLIX is the ideal partner for many healthcare organizations by providing a lightweight, adaptable architecture that combines with ease of use and rapid deployment. WALLIX's proven track record in both on-premise and cloud environments shows that it can be rolled out quickly and applied broadly for both distributed and centralized healthcare organizations.

### For more information on how WALLIX can help your healthcare organization, download the following guides:

- **PAM and HIPAA Compliance**  
<http://contact.wallix.com/en-us/pam-for-healthcare-security-and-hipaa-compliance>
- **Complying with HIPAA/HITECH**  
<http://contact.wallix.com/compliance-with-hipaa-hitech>
- **PAM and PCI DSS Compliance**  
<http://contact.wallix.com/en-us/pam-and-pci-dss-compliance-assurance-with-wallix>
- **PAM and GDPR Compliance**  
<http://contact.wallix.com/en-us/pam-compliance>
- **Saint Quentin Hospital Case Study**  
<http://www.wallix.com/healthcare/>



• Privileged Access Management (PAM) for Healthcare

### How Does PAM Work?

PAM allows you to:

- Grant privileges to users only for systems on which they are authorized.
- Grant access only when it's needed and revoke access as soon as the need expires.
- Eliminate local/direct system passwords for privileged users.
- Centrally manage access over a disparate set of heterogeneous systems.
- Create an unbreakable audit trail for all privileged operations.

### Components of a PAM Solution

Privileged Account Management solutions vary, but most offer the following components:

- **Access Managers** – Govern access to privileged accounts with a single point of policy definition and policy enforcement for privileged account management. A super admin can add/modify/delete privileged user accounts on the access manager in a centralized system, thus greatly improving efficiency and effective compliance levels. Privileged users request access to all systems through the access manager.
- **Password Vaults** – Keep passwords in a secure and certified "vault." All system access is via the password vault. Thus, users never have direct access to root passwords.
- **Session Managers** – Track all actions taken during a privileged account session for future review and auditing. Further, some systems can prevent malicious or unauthorized actions and/or alert super admins if suspicious activity is detected.

The WALLIX Bastion reference architecture, showing how its three software components (Access Manager, Session Manager and Password Manager) work together to deliver efficient, cost-effective PAM.

### OFFICES & LOCAL REPRESENTATIONS

**WALLIX FRANCE** (VVO)  
 100 rue de Valenciennes 75013 Paris  
 France  
 Tel: +33 (0)1 42 42 42 42  
 Fax: +33 (0)1 42 42 42 42  
 Email: [france@wallix.com](mailto:france@wallix.com)

**WALLIX UK**  
 100 rue de Valenciennes 75013 Paris  
 France  
 Tel: +33 (0)1 42 42 42 42  
 Fax: +33 (0)1 42 42 42 42  
 Email: [uk@wallix.com](mailto:uk@wallix.com)

**WALLIX GERMANY**  
 100 rue de Valenciennes 75013 Paris  
 France  
 Tel: +33 (0)1 42 42 42 42  
 Fax: +33 (0)1 42 42 42 42  
 Email: [germany@wallix.com](mailto:germany@wallix.com)

**WALLIX USA** (PAC)  
 100 rue de Valenciennes 75013 Paris  
 France  
 Tel: +33 (0)1 42 42 42 42  
 Fax: +33 (0)1 42 42 42 42  
 Email: [usa@wallix.com](mailto:usa@wallix.com)

**WALLIX RUSSIA & CIS**  
 100 rue de Valenciennes 75013 Paris  
 France  
 Tel: +33 (0)1 42 42 42 42  
 Fax: +33 (0)1 42 42 42 42  
 Email: [russia@wallix.com](mailto:russia@wallix.com)

**WALLIX ASIA PACIFIC**  
 100 rue de Valenciennes 75013 Paris  
 France  
 Tel: +33 (0)1 42 42 42 42  
 Fax: +33 (0)1 42 42 42 42  
 Email: [asia@wallix.com](mailto:asia@wallix.com)

**WALLIX AFRICA**  
 100 rue de Valenciennes 75013 Paris  
 France  
 Tel: +33 (0)1 42 42 42 42  
 Fax: +33 (0)1 42 42 42 42  
 Email: [afrika@wallix.com](mailto:afrika@wallix.com)

[www.wallix.com](http://www.wallix.com)



**Client:** WALLIX



**What they do:** Privileged Access Management (PAM) software



**Summary:** An overview of the unique cyber threats that face healthcare organizations and why implementing a privileged access management solution is critical to protect healthcare IT systems.

Want to see the entire 10-page eBook?

CONTACT US



## Solution: How Swimlane Applets and Applications are up to the challenge

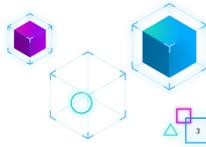
### Security orchestration, automation and response

A security orchestration, automation and response (SOAR) solution like Swimlane automates manual and time-consuming security management tasks. Additionally, SOAR centralizes security operations by orchestrating incident response playbooks and workflows across multiple specialized security tools and related infrastructure. A security analyst empowered by SOAR can use a single console to monitor, investigate and respond to the outputs of SIEMs, EDRs, anti-malware, sandboxing, threat intelligence and other security technologies.

SOAR enables SecOps teams to automate existing alert responses by modeling and orchestrating the workflow steps tied to virtually any use case. For example, an incident response process might call for a suspicious binary to be manually entered into a system such as VirusTotal for inspection. The SOAR solution handles the VirusTotal step on its own, automatically submitting the binary and collecting the results in a matter of seconds.

**SOAR solutions allow SecOps teams to automate and orchestrate operational tasks and existing alert responses.**

By automating and orchestrating time-consuming and repetitive tasks, such as opening and updating trouble tickets in systems including Jira or Remedy, creating reports, logging into multiple systems, entering incident information, and sending email alerts, SOAR significantly speeds up threat management and incident response processes.



SWIMLANE

### Swimlane Applications

Applications within Swimlane are user-defined templates for collecting, storing and organizing your data. They can contain any combination of user-defined and out-of-the-box content, including both preconfigured and custom case management forms, workflow templates and relevant dashboards.

### Swimlane Applets

Swimlane Applets are a preconfigured set of fields and layout specifications and can include playbook or workflow components that can be plugged into any Swimlane Application easily. By dropping them into an existing Application, users can quickly and update and expand their existing Swimlane deployment to rapidly adapt to their unique security toolsets, incident response processes and personnel. Applets are essentially reusable building blocks that can be deployed in any combination to address virtually any use case with simple drag-and-drop deployment.

What's more, Swimlane's predictive orchestration mapping largely automates the process of integrating new tools so that adding new technologies into an environment is virtually seamless. Thus, combining these two features, new use case-specific Applications can be deployed rapidly to address an infinite number of incident response scenarios.

### Modular by design

The modular nature of Applets is what makes them so versatile and valuable. SecOps teams can reuse previously built Applets easily, either on their own or as part of a collection. Users can mix and match Applets as needed to quickly build out customized Applications that rapidly map to unique configurations and processes. For example, with Applets, a team could quickly reconfigure an existing threat hunting SOAR application to incorporate an EDR's alarm data and its enforcement capabilities to facilitate automated responses to specific threats. Hundreds of Applets are available out-of-the-box to address specific threats and use cases.



SWIMLANE

### Sharing without tipping off the bad guys

The availability of Applications and Applets helps resolve another challenge of collaboration between security teams: They may be reluctant to share detailed information about their responses for fear of inadvertently tipping off attackers about their security practices and architectures.

This lack of cooperation amongst security professionals is becoming increasingly problematic as the bad guys are increasingly sharing their own information and code on the dark web. The unprecedented level of organization and "professionalism" amongst cybercriminals and state actors, many of whom are working in loose concert, is an incredible challenge for even the largest organizations trying to adapt their defensive postures on their own quickly and effectively.

Swimlane helps address the core reasons behind this isolation in two key ways:

- The modular nature of Applets compartmentalizes sensitive information
- With AppHub, a trusted and open marketplace for Applets where all contributions are validated by Swimlane.

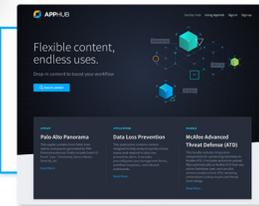


Figure 1: The Swimlane AppHub allows trusted organizations to securely share Applets, Applications and Bundles of integration components... All validated by Swimlane.

SWIMLANE

### Conclusion

Security teams don't have time and resources to waste. With the ever-growing and evolving threat environment, duplicative and redundant SecOps environments can be costly and exhausting. Safe and effective collaboration in addition to automation and orchestration can solve these problems. Swimlane's approach to Applets and Applications harnesses the wisdom of the entire SecOps community and allows teams to build and share security response workflows that embody best practices that don't have to be constantly reinvented.

### About Swimlane

Swimlane is a scalable and innovative leader in security orchestration, automation and response (SOAR). The flexible solution delivers powerful, consolidated analytics, real-time dashboards and reporting from across your security infrastructure, maximizing the incident response capabilities of over-burdened and understaffed security operations.

The scalable, innovative and flexible security solution offers a broad array of features aimed at helping organizations to address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire organization.

To arrange for a demo of Swimlane or to speak with one of our security architects to see if SOAR would be helpful to your organization, please contact us at 1.844.SWIMLANE or email us.

SWIMLANE

### Vendor-neutral community: SecOps Hub

Swimlane is also supporting SecOps Hub, a new vendor-neutral community for security operations professionals. This open community is aimed at helping security analysts and admins get better at what they do. It gives security professionals a place to share ideas about incident response processes, preferred security tools and specific threat management strategies. One could think of it as a hive mind for the SecOps community.

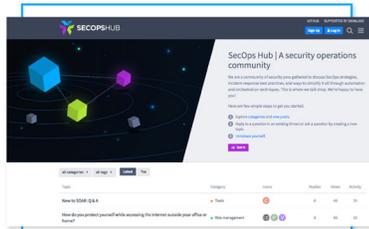


Figure 2: Join the vendor-neutral SecOps Hub to share SecOps tips and tricks with fellow professionals.

SWIMLANE



Client: Swimlane



What they do: Security Orchestration Automation and Response (SOAR) platform



Summary: An introduction to the benefits of modular security applications including the ability to create playbooks, modify workflows, and share optimized processes with peers.

Want to read the entire 10-page eBook?

CONTACT US

## About glassCanopy



You could probably write a fantastic eBook every quarter that would engage your prospects and customers... if you had the time. glassCanopy effectively creates that time by taking on all of the heavy lifting: conceptualization, research, writing, and final layout. All you have to do is provide feedback and revisions.

We then take those eBooks and integrate them into a lead generation machine that we run for you. We handle everything:

- Content creation
- Ad buy planning and execution
- Landing page and banner design
- Integrating with your CRM and marketing automation
- Lead nurture campaigns
- Closed-loop analytics, reporting, and optimization

Our core services cost between \$10-25K per month plus media buys. We're best suited to companies with complex products/services with average deal sizes of \$10K or more.

**If you're interested in seeing what we can do for you:**



**Give us a call at  
(415) 663-7826**



**Send us an email at  
[rich@glasscanopy.com](mailto:rich@glasscanopy.com)**



**[Get in touch](#)**