SHERLOCK

# THE CASE FOR SECURITY IN THE CLOUD



SherlockCloud.io | @Sherlock_Cloud | info@sherlockcloud.io

# Contents



> "Security must become simple. It must be by default and by design. It cannot be an optional component."

# SECURITY IN THE CLOUD

On April 15, 2016, a security engineer working at the United States Office of Personnel Management (OPM) noticed something strange. OPM is one of those large bureaucracies that usually doesn't garner a lot of attention. However, OPM does manage a lot of sensitive data about intelligence assets (i.e., spies). On this spring day, the engineer found odd traffic coming from a component usually used in antivirus software.

Upon cursory analysis, this traffic looked normal. However, it was being directed to an odd domain name that was owned by "Steve Rogers"—Captain America from the Marvel movies. While this may make you chuckle, it is also an alias for a shadowy foreign hacking group. This group has been behind some of the biggest hacks in history, including the Anthem breach in 2014.

In a few days, OPM had uncovered a serious breach that affected millions of records, including highly sensitive records for intelligence personnel.

What is remarkable about the OPM breach was its simplicity. The malware used a well-known tool called PlugX that is common among Chinese hacking groups. The attackers used classic kill chain tactics including land-and-expand to access one host, which was then used to attack others. Once enough hosts had been compromised, the attackers set up a command-and-control infrastructure that reported back to the innocently-titled domain name "opmsecurity.org," which our Captain America owned.

> "Today, many CIO/CISOs view the cloud as merely part of a security program. In the future, the cloud IS your security program."

## YOU ARE A TARGET

Hackers, criminals, and rogue insiders using tactics like those of the OPM breach are a persistent threat to your business, reputation, and job. Like many of the other mega breaches, the OPM demonstrates with absolute certainty that traditional information security methods do not work.

Reasons for this include:

1. Current security technologies such as next-generation firewalls do not sufficiently protect sprawling enterprises.
2. Compliance frameworks such as PCI-DSS, ISO 27001, and FedRAMP do not provide continuous assurance.
3. Security policies are difficult to enforce in a dynamic and diverse workforce.
4. Security talent is scarce.
5. Hackers use complex, multidimensional attack techniques that are difficult to detect in a deluge of data.

How do we resolve these problems and build security programs that keep pace with a volatile threat landscape?

The answer is the cloud, which offers a robust, dynamic, and scalable platform that simplifies and streamlines security. The cloud can resolve many of these problems, and puts you ahead of the threat.

In this paper, we will make the case for security in the cloud and look ahead to the future of business security.

# PART 1

## By Default and By Design

In her keynote at the 2018 RSA Conference, futurist and game designer Jane McGonigal claimed, "Any useful statement about the future should at first seem ridiculous."

Here is a ridiculous statement about the future of information security:

*"In the future, security will be easy. It will be enforced and enabled* ***by default and by design."***

When you look at the modern security landscape in relation to the cloud and automation, the idea that it could be easy is not science fiction.

To understand this, let's look at the current state of information security and its problems with complexity.

## The Complexity Problem

Securing an enterprise, maintaining compliance, and managing risk requires disparate and complex technologies, requirements, and skills.

For example, to achieve PCI compliance, your organization must implement and maintain controls to meet over 200 explicit requirements, which are burdensome in terms of cost, technology, and personnel.

Most security tools are "point solutions" and fulfill a single (or narrowly focused) security need. These tools arose from companies pursing specific market demands. While tools such as next-generation firewalls share common features, they rarely integrate well with other tools. Even when they do, people need to manage and maintain configurations to keep them working together smoothly.

> "The idea that security can be easy is not science fiction."

Compliance frameworks such as NIST, ISO, and the PCI DSS have a similar divergence problem. There are as many areas where these frameworks are different as similar. The PCI DSS requires multi-factor authentication only for administrative access into the cardholder data environment. Other standards do not explicitly require this, which creates a divergence because best practice is to use multi-factor authentication for all remote and administrative access.

Organizations must reconcile this complexity in order to build effective security programs. This means hiring people with the skills to overcome these challenges and build a cohesive security program.

Amit Yoran said in his 2014 address at the RSA conference, “Complexity is the enemy of security.” Complex systems are inherently more difficult to secure. The amount of data and variables is overwhelming.

Consider the amount of event data a single web application can generate. Every API call, every use of rights and every data request is a single event. Multiply the size of this data by the number of users, and again by the number of events each user generates. A single application can produce terabytes of data in a single day. Now add all the security tools such as NGFW and endpoint security into that data stream. This staggering amount of data contains tiny slivers of information, which are often indicators of an exploit or attack.

Humans are not wired for this level of complexity and cannot comprehend all this data. However, systems are not becoming any less complex.

Because of systems complexity, we must make information security simpler.

To simplify information security, we must assess signals.

# Signals

One of McGonigal's other insights from RSA was that if you want to predict the future, you must look for "signals," or indicators of the future. There are three relevant signals currently happening in information security:

1. Unrealistic expectations are being placed on security professionals
2. Point security solutions have failed
3. Automation and the cloud are having an impact

# Unrealistic Expectations

Information security has inverted the natural order of humans and technology. In an ideal state, technology does the repetitive work that demands discipline while humans focus on oversight, design, and creativity.

With traditional information security frameworks, employees are performing all the repetitive work, while security programs are built specifically to suit a vendor's technology.

Based on our decades of interviews with CISOs and other technology leaders, we have documented a consistent management practice of defining a security program in the context of a specific vendor or technology. A CISO will often tell us, "Well, we're a Palo Alto Networks shop." Often information security leaders are vendor and product-focused when they should base their programs on goals and their employees.

This trend places vendors and technologies in inappropriate positions of authority. The CISO uses technology to define the security of the company, which elevates its status over employees.

The financial investment to acquire and maintain these technologies results in an elevation of their importance to a company's information security program far more than they deserve. In a large, complex enterprise, information security

> "Despite all our improvements in security technologies, there is no replacement for the intuition and creativity of humans."

may consume 75% of the department's budget. Managing and operating these technologies is also onerous and taxing on employees and resources.

For many organizations, security professionals are viewed as transient and undervalued. The talent scarcity and demand for security professionals has caused an overflow of unqualified people in the industry.

When organizations overvalue technology and undervalue people, they place unrealistic expectations on employees, including:

1. Knowing every possible attack technique, vulnerability, and compliance requirement
2. Never missing a single detail, issue, or attack
3. Closely monitoring every single detail using a sprawling, complex set of point solutions
4. Protecting the environment 24x7x365, when talent is scarce and turnover is high
5. Assuming full responsibility when they lack the ability, access, or authority to improve security
6. Reputation damage when mistakes happen

With artificial intelligence and machine learning, vendors are now promoting these technologies as direct replacements of people because they can anticipate problems before they happen. AI and machine learning are valuable assets that can improve the accuracy and effectiveness of security detection, but cannot replace humans.

**Despite all our improvements in security technologies, there is no replacement for the intuition and creativity of humans.**

The first barrier to overcome is a realignment between technology and humans. We must place people in charge and technology into a supportive role. We must redefine our security programs around a shared mission, vision, and values. Security technologies must evolve as well in addition to their tasking realigning with humans.

In this next section, we will take a look at how the current state of security point solutions has also created barriers to simple security.

## Point Security Failure

Walking around at security trade shows like RSA and BlackHat, we are bombarded with shallow vendor promises to stop hackers, clean up malware, prevent abuse, and provide absolute assurance.

Point solutions make up the majority of products on the market and promise to solve a narrow set of security challenges. Many products claim to be "game changers" when they really are "game rearrangers." While they eliminate one problem, they create new ones, typically in the form of onerous administrative overhead.

Whitelisting has existed for about ten years and controls the applications that run on systems. Applications that are not whitelisted are blocked, and those that are whitelisted can run normally. The vendor pitch is that whitelisting prevents hackers from installing and running unauthorized applications. When properly implemented, managed, and monitored, application whitelisting can stop malware from running.

Application whitelisting also stops legitimate applications. If you implement application whitelisting, you must have extremely tight control over your applications and an internal procedure to review, approve, and add new applications when necessary. While whitelisting can stop an attack, the resulting administrative overhead can be excessive, especially in dynamic, high-performance environments. Mistakes under these circumstances can cause system failure. The technology is never fully implemented in this environment, which devalues vendor product claims and promises.

"Silver bullet" solutions predate the Internet age and are not new concepts. The famous computer architect Fred Brooks said over 30 years ago, "There is no single development, in either technology or management technique, which by itself promises even one order-of-magnitude improvement within a decade in productivity, in reliability, in simplicity."

> "The problem with point solutions is they solve one problem, while creating other, different problems."

The effectiveness of point solutions depends on the diligence of the people needed to implement, configure, manage, and monitor the technology. This level of diligence increases as new controls are added to accommodate for administrative overhead.

For example, you install a new NGFW which requires ten new administrative procedures to operate it successfully. Then you implement an advanced endpoint product, which also requires ten new administrative procedures. New procedures must align and coordinate with existing ones which creates an additional ten. With the complexity of a sprawling enterprise, the administrative burden eventually becomes overwhelming.

These administrative and technical elements have been present in every breach over the past ten years, including Target, Anthem, and Equifax. These companies had the latest security technologies—next generation firewalls, malware sandboxes, application whitelisting, and endpoint security. These products performed based on vendor specifications but did not stop the breaches.

In every case, the lack of human due diligence caused the breach. Target, for example, had the latest FireEye appliances. These products reported the malware that lead to their breach. The people monitoring those systems however, did not follow procedures properly, and the attacks went unreported.

Security teams keep adding technology, reducing staff, and hoping that procedures, policy, and compliance efforts will compensate  with no success. All of these breaches demonstrate that people cannot keep pace with the volatility of modern environments. Likewise, traditional onsite security is too inflexible to handle this volatility.

Our last signal looks at the impact of the cloud and automation.

# By Default, By Design

In an onsite environment, security is dependent upon your people and their level of discipline. If you have a highly disciplined team, you can manage security effectively. Unfortunately, building and retaining a team of highly disciplined security people is extremely difficult, especially with the scarcity of security talent.

In the cloud, there is no hardware, network, or system for you to purchase and maintain in the traditional sense. Everything is code and systems are virtual. Systems, networks, and entire architectures are created, destroyed, scaled, and secured entirely through code. When people need to build a new system, they build new code.

Even the most disciplined security teams are subject to the whims and interpretations of each individual. This is not an indictment of those people but merely a fact of the human condition. We are inconsistent, flawed creatures.

The cloud, and more specifically automation through code, allows us to circumvent this inherent human condition. Rather than be at the mercy of our human inconsistencies, code is always consistent and either runs or fails. Once optimized, code is predictable and repeatable with near absolute assurance.

Cloud environments can be fully automated. When new systems are created, they use known-good images. Secure configurations and controls (like anti-malware or intrusion detection) can be installed automatically. These controls are then automatically configured for maximum protection. Data is automatically encrypted and access rights are automatically restricted. Security becomes enabled by default, and by design.

**All of the big breaches from the past ten years follow a similar pattern:**

1. Gain access to the environment

2. Establish persistence on one or more hosts

3. Use that persistence to attack other hosts

4. Once the attacker has the data they seek, exfiltrate it through the persistent channels established

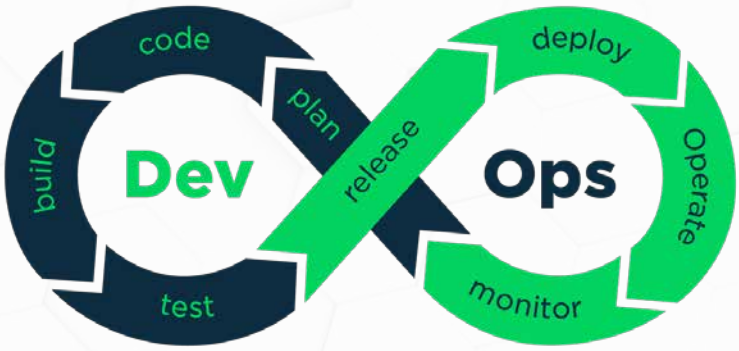
## DevOps

DevOps is a software engineering culture and practice that aims at unifying software development (Dev) and systems operations (Ops). The main characteristic of the DevOps is automation. Every step of software construction is automated and closely monitored, from integration and testing to deployment and infrastructure management. DevOps is derived from Agile software development. Organizations that have adopted DevOps consistently report faster and more reliable time-to-market with new products.

# Persistent Break

When security is automated, another huge benefit emerges; persistence breaking. When hackers break into an environment, they do not steal everything at once. They must gain persistence in the environment, and then branch out to discover where valuable data resides.

The Office of Personnel Management breach in 2015 followed this pattern. Using a PlugX malware variant, the attackers gained access to the environment and then spread to other hosts. They used a special domain name to send encrypted communications back to a command and control system. The attackers were persistent in the OPM environment for months before being discovered.




When an environment is automated, this persistence can be easily broken. When the entire environment and its configuration is stored in a code repository, the environment can be rebuilt at a moment's notice from known-good images. If an attacker has gained entrance, this access disappears when the environment is recreated. Recreating an environment quickly and consistently is one of the most effective security measures any organization can implement. It breaks persistence, and stops many attacks before they ever progress. Since attackers require weeks or months to carry out a complex attack, automating this teardown and rebuild process on a routine basis can provide security protection that no endpoint or network security product could ever achieve.

Automation and code also allow guard rails. These are controls that automatically prevent an environment from remaining in an insecure state. If a user accidentally opens public access to confidential data, automation processes can detect this and shut it down, with no human intervention necessary. Guard rails maintain the security of the environment, which relieves humans of the burden of remembering redundant tasks.

# Future Mind Games

**So, if we accept that the cloud can make security easier in the future, what does information security look like in 2030?**

**There is good news, and bad news.** In the future, many security professionals will become obsolete. If you want to future-proof your security career, learn cloud automation and coding. Stop obsessing over hacking techniques, compliance, or security appliances. These practices will diminish significantly in ten years.

> "The traditional model for a SOC is not working. Every breach in the past 10 years is proof of this."

In 2030, security will be more like DevOps. Security professionals will either be coding security into automation cookbooks or monitoring the output of systems. Security will also be integrated into the entire lifecycle of DevOps: from planning, coding, and testing, to production.

The other good news, our jobs will be much more rewarding. Rather than chase down security configurations or obsess over PCI requirements, automation will do that work for us. We will be able to step back and focus on architecting solutions and incident response. Security will also become more integrated into the organization.

There are a lot of changes that must happen between today and this easy future. In this next section, we will look at the Security Operation Center (SOC) of the future, how it will function, and how we are building that future right now at Sherlock.

# PART 2

*"Are you waiting for something bad to happen, or working toward something good?*

This is one of those questions everybody in security must face. Are we focusing on the problem or the solution?"

## Future SOC

For decades, the conventional design of a Security Operations Center (SOC) has been to centralize everything in one place and then have people monitor alerts. During an alert, people react, respond and resolve.

Technology vendors have focused attention on security operations centers. They have designed increasingly complex tools to help analysts identify and monitor threats. These tools can be useful at stopping attackers. As discussed earlier, technology alone does not fix all issues when used independently. When humans and technology align correctly, then implementing security solutions becomes more realistic.

This traditional SOC model is not working. Every breach over the past ten years is proof of this, including recent megabreaches from Equifax, Target, or Anthem. All of these companies had the latest security technologies and SOCs, yet still failed to stop the breach.

Why is the modern SOC so ineffective?

## Today's SOC

**It is passive**
The traditional SOC is event-driven, resulting in passive and reactive security operations.

**It incentivizes inaction**
When security practitioners operate passively, serious incidents mean more work and greater scrutiny. This practice creates panic and an incentives dismissive behavior toward alerts. When people are incentivized to inaction, they can easily ignore serious attacks as noise or false positives.

**It assumes you know everything**
Passive security also assumes your people have a complete picture of the environment. Even under ideal conditions, there are

ample blind spots in the data. When a serious alert is reported, it is extremely unlikely the people monitoring the SOC will have a complete picture of the incident. Recent innovations in security analytics, security "fabrics," and SIEM products can provide more information, but a total picture would evade even the best SOC analyst.

**It assumes you can effect change**

SOCs presume that when there is serious problem, you do something about it. But if the SOC team does not have access, authority, or respect, then they cannot make any change or remedy the problem, making them ineffective. The SOC detects and reports problems but they cannot mitigate them.

**The 4:00 AM Fallacy**

Perhaps the most significant fallacy is that humans can react in a consistent and decisive manner to stop an attack in progress. Waiting for an alert from the SOC creates panic and causes people to make short-term decisions. It is unfair to put people in the position of having to react in a panic situation. Analysts in these situations will likely rationalize the problem as being less serious. If the security of your business depends on people passively watching data, you can almost count on a breach.

## Tomorrow's SOC

We must transform SOC analysts from passive chair-squatters to active hunters. The SOC of the future will function differently by embracing a "by default, and by design" model to provide proactive defense. This model will realign the SOC, put people in an analytical role, and technology in a response role.

**Continuous Integration / Continuous Delivery**

The first step to building the SOC of 2030 is to move security operations to the cloud and adopt the principles of DevOps. On-premises security operations are too inflexible to handle the threats of today and tomorrow. On-premises equipment also has the negative side effect of maintaining the status quo. The SOC of tomorrow must be able to adapt quickly to a changing landscape. It must scale quickly, support quick reconfiguration, and tolerate change.

### CI / CD

Continuous integration and continuous delivery (CICD) is a coding philosophy and set of practices that help development teams produce code in a more consistent, reliable, and rapid manner. Continuous integration focuses on building processes to introduce changes using a structured, automated process. These processes automatically validate the code integrity, function and (ideally) security. Continuous delivery then picks up to automatically promote new code through dev, test, and prod environments.

Security can use the concepts of CICD to perform similar functions. When security changes are fed into an environment, and automatically checked, they can be rapidly deployed to production environments. CICD is a hallmark of cloud environments.

Using the DevOps concept of continuous integration and continuous development, security teams can deploy changes and updates more quickly and consistently.

**Imagine a scenario** where a new malware emerged that targeted a specific Linux distribution component and was difficult to detect. Using a complex and dynamic encrypting method, it could remain hidden from detection products like endpoint malware scanning. How would your new cloud-deployed SOC environment handle this issue?

**First,** you could update the configuration for the systems in your environment to resist this specific malware. This new configuration could be automatically pushed to a test environment, which then tests that everything works. If those automated tests pass, the changes would automatically be promoted into production.

**Second,** you could rebuild the entire environment from known-good images. This would wipe out all traces of the malware. These new configurations would ensure that when new systems come online, they are automatically resistant to the malware.

**Lastly,** you could kick off automated scans anytime a new device is detected to ensure new systems remain secure. Since all of this is automated, it does not require the discipline of a team of people and no human has to remember to perform a specific task. Once it is in the code, it will always execute.

# Automated Hunting

The next step is to build a hunting strategy. Not a SIEM per se, but a capability that hunts for evidence of an attack. While most commercial SIEMs can function as a hunting platform, they are not one out of the box. You must configure them to do the hunting, and that is not easy.



To perform effective hunting, the SIEM must have four interlocking sources of data:

1. **Log data:** Full event data from every host in the environment.
2. **Security data:** Logs for every event, detection, and block from every security control in the environment (NGFWs, endpoints, WAF, etc.)
3. **User behavior data:** Granular user access data from your identity repository (such as Active Directory) showing what every user is doing, when, and why.
4. **Network data:** Data flow information from key connections to corroborate activities on hosts.

Further, you need five primary capabilities within your environment.

1. **Endpoint scanning:** You must be able to scan any host anywhere at any time for specific files or activities. Most (but not all) endpoint security products, like Carbon Black and Bitdefender, support this capability.
2. **Network control:** Typically a NGFW that performs this function, but in the cloud. NGFWs are not architecturally viable, which means you must have an endpoint product on your cloud hosts that can provide firewall functions.
3. **Network scanning:** Most commercial vulnerability scanners can provide this capability.
4. **Intrusion detection:** Whether it is endpoint-based or network-based, the classic IDS/IPS is still a crucial component of security. All NGFW products provide this capability. However, in the cloud, classic “tap” style IDS does not work. You also cannot perform packet capture in the cloud, which requires IDS placement on the endpoint.
5. **Deceptions:** These are decoy systems, files, or user accounts deployed throughout the environment that set off alerts when an attacker attempts to access them. Deceptions are an excellent way to detect hacking activity early.

## SIEM

Security Information and Event Management

A class of security and data management technologies that aggregates log and event data for monitoring, alerting, reporting, correlation, and archive.

Additional capabilities that are useful include data loss prevention and a WAF.

With these capabilities in place, you can begin to build hunts (or detections). A hunt is a sequence of events or actions that indicate potential attack behavior. Some SIEM products include a library of hunts. Our Sherlock SIEM product natively includes hunting as part of the SIEM logic.

A hunt typically looks at a specific action. For example, one of the common hunts we use in the Sherlock platform focuses on systems with high-bandwidth connections to a foreign IP address during abnormal hours, which is a classic indicator of compromise. For many environments, a laptop sending large amounts of data to foreign IP addresses is unusual. If the platform detects this, it can raise an alert for analysts to investigate.

It is vital that a hunting platform have the speed and scale to handle thousands of hunts, which is a common problem with on-premises SIEM technologies. The hardware they run on limits their performance, and requires ongoing purchases and upgrades. In the cloud, hunting platforms can scale to any size.

The Sherlock Managed Detection and Response platform has unlimited scale and unlimited storage. Using the power and scale of the AWS cloud, we can handle thousands, even millions of hunts per second. And since this is all in the cloud, costs can be contained using flexible sizing to ramp up when demand is needed, and ramp down when it is not.

# Human Hunters

In addition to automated hunting, a team of human hunters is essential. Automation can handle nearly all the routine hunting, but humans must be available to perform manual hunts as new threats emerge.

SOC teams must transform from passive gatherers to active hunters. Team members must be incentivized to search for new threats. They must have access to the latest threat intelligence and the authority to conduct hunts and investigate activities.

Authority ultimately becomes the primary limiting factor in most SOCs. The staff must report to a manager who also reports up a chain of command. Hierarchical power structures create resistance, which hinders security operations. The ability for SOC analysts to perform hunts, especially those that investigate the configuration of another department's systems, has the potential to inflame inter-organizational strife. We have seen this behavior in organizations of all sizes and across all sectors. Security staff are routinely denied the authority to investigate serious issues, which renders them irrelevant. This trend leads to data breaches, alienates SOC analysts, and creates employee turnover.

When analysts are given the freedom to investigate, they are consistently more effective. SOC team members must have access and authority to operate effectively.

Since we are security experts and not politicians, navigating the nuances of corporate bureaucracy is outside the scope of this publication. In our experience, third parties are not tied to the political and hierarchical complexities of an organization. They can remain focused on hunting and threat reduction without the fear management retaliation.

However, this means that managed security providers must perform hunting. In our experience, most MSSPs do not perform hunting. They typically manage devices and provide monitoring, but not active hunting for attacks.

# How Sherlock Works

1. **Sherlock is automatically deployed** on the AWS cloud and connects to all your environments.

2. **The Sherlock SIEM ingests** all your security, application, network, and user behavior data. Using machine learning and automated threat hunting, the platform scours this data for evidence of compromise.

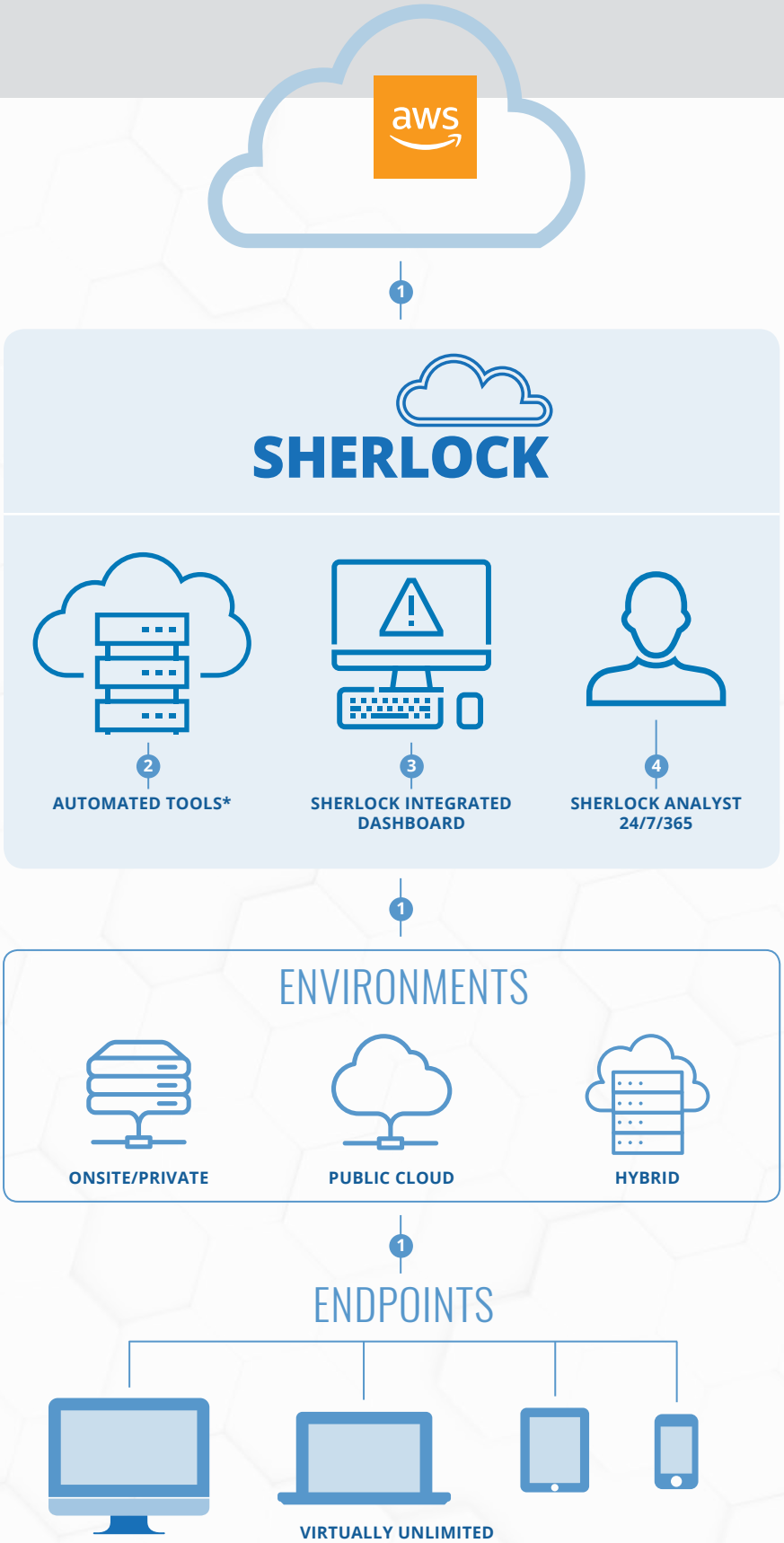
3. **Security controls deploy** throughout your cloud and on-premise environments and augment the data the platform analyzes.

4. **The Sherlock SOC investigates** incidents and responds to threats.

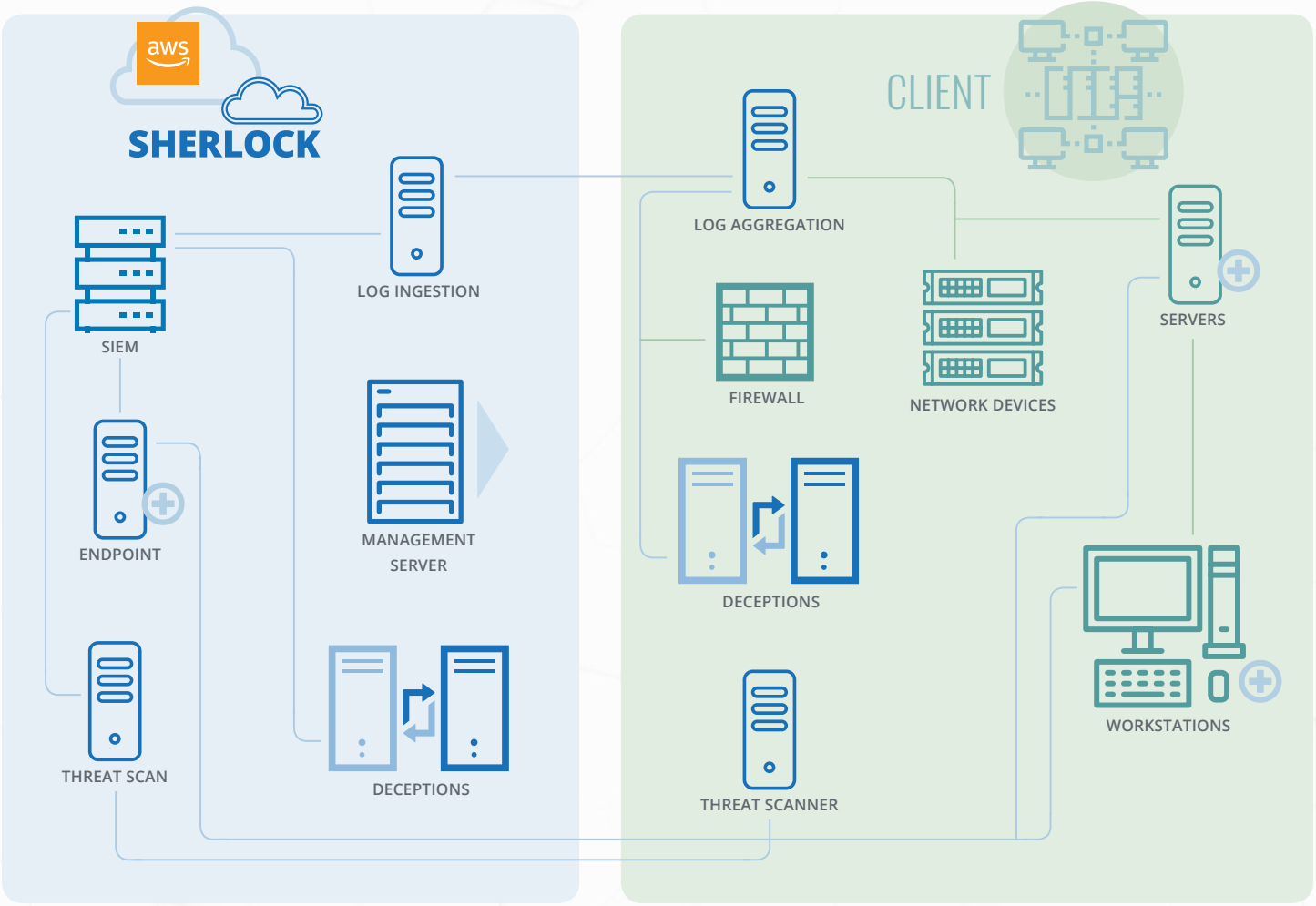
* **Sherlock includes a stack of cloud-native controls:**

- Sherlock SIEM: Data analytics platform with integrated hunting.
- Sherlock Threat Scan: Automated system and network scanner.
- Sherlock Decoy: Deceptions to spot hackers pivoting in the environment.
- Sherlock Endpoint: Anti-malware, file integrity monitoring, system integrity monitoring and more.

**We also support many third-party technologies.**



# Sherlock on the Network



## What is Transformational Leadership?

Transformational leadership is a philosophy where leaders appeal to the values and sense of purpose among employees to inspire and drive performance. Transformational leaders focus on setting a clear vision, goals, and mission. They coach team members to develop themselves so they can serve the greater vision of the organization.

Transformational leadership is similar to Servant Leadership in many ways. However, where servant leaders are focused on individual development, transformational leaders focus on getting people to identify with the vision and mission, and then develop themselves in service of that vision.

# Leadership

Leadership is the last factor in building the SOC of the future, which in many ways, really is the first and most important part. You cannot lead a future SOC using traditional "enforcement" or "audit-based" security leadership. The leadership of tomorrow's SOC looks and acts a lot like the leadership in a DevOps team. Each year, Puppet publishes a State of DevOps report. In the

2017 report, they focused on leadership and its role in building a dynamic, high-performance DevOps shop. Specifically, the importance of Transformational Leadership.

The basic tenants of Transformation Leadership include:

**Vision:** Establishing a concept of where the organization is going and what that means.

**Inspirational communication:** Leadership inspires and motivates people, even when the environment is uncertain or changing.

**Intellectual stimulation:** Challenges people to solve problems, look at things creatively, and take charge of their own development.

**Supportive leadership:** There is genuine empathy for each team member and their role.

**Personal recognition:** There is a regular recognition of accomplishments. Every team member has a chance to shine.

If your organization cannot make the SOC an engaging, exciting, and interesting place to work, then no amount of "next-generation" technologies are going to protect you.

The security operations center of 2030 has people at its heart, not technology. It does not need a giant room full of monitors, it needs a room full of people, collaborating and working toward a common goal.


Image Credit: https://puppet.com/resources/whitepaper/2017-state-of-devops-report

# CONCLUSION

In this paper, we have discussed the failure of traditional security operations. We have shown how using the principles of DevOps, transformational leadership, and the cloud can profoundly alter your security operations. So how do you incorporate these complex ideas and implement these changes into your organization? Here are some steps you can take today to start building the SOC of 2030.

**Put the Vendors on Ice**
Vendors have a vested interest in selling you the next shiny object. Stop letting vendors and VARs sell you products. Another technology is not necessarily going to get you to a future SOC.

**Assess your Cloud**
How much of your environment is in the cloud now? Like most organizations, you probably have some in the cloud and some on-premises.

**Assess your internal DevOps culture**
Do you have internal people who understand the concepts of DevOps? If not, then that is going to be a serious hurdle for you. Traditional development and IT management practices, like ITIL, are not going to work in the DevOps world.

**Evaluate Your SIEM**
A powerful SIEM is the center of your future SOC. The development, management, and optimization of this platform is more important than any other security tool you have.

**Automate Response**
Every security tool must automatically respond to attacks where possible. This includes NGFW and endpoint technologies.

**Seek Out Fabrics**
If you are going to look at new technologies, look for products that interoperate and work collaboratively. Vendors such as Fortinet have tied together their products to provide unified responses.

**Insert Security into DevOps**
Make security an integral part of your development practices. Start building relationships with your development teams. Remember, you need to automate security. High performance development teams are not going to tolerate long, complex, manual audits.

**Install Guard Rails**
There are numerous technologies, such as CloudCheckr, Evident.IO, and Dome9, which can provide security "guard rails" around your cloud environments. These technologies are extremely helpful in detecting security problems and correcting them. Automate the correction wherever possible.

**Outsource**
Building a future SOC is not easy. Let the experts at Sherlock help you. Our cloud-native platform can accelerate you to the SOC of 2030.