# ROI Guide

Comparing costs of an in-house SOC vs. implementing AgileBlue as your SOC|XDR partner

AGILEBLUE

AgileBlue, 2022

# EASY ROI GUIDE

When it comes to considering SOC-as-a-Service for your organization, costs should be at the top of your priority list. Think about it this way, how can your team, which may generally be part-time on cybersecurity, keep up with all the alerts, notifications and required remediation? What about threat hunting? Can a part-time or small team of IT professionals be expected to run a SOC, remediate problems, and in between lunch and emails hunt for unknown threats trying to steal your most confidential data? It is very difficult, if not impossible, to go at it alone. The below table breaks down annual costs to operate and manage a Security Operations Center in-house vs. using AgileBlue for your SOCaaS partner.

| SOC COMPONENT | COSTS ESTIMATED FOR A MID-SIZE COMPANY WITH ABOUT 500 EMPLOYEES | SUPPORTING NOTES |
|---|---|---|
| **SOC Staffing Salaries** | $290,000 | - SOC Manager (CISSP): ~ $125,000<br>- 3 SOC analysts cover 24 hours: ~ $165,000 ($55k per employee) |
| **SIEM (i.e. Splunk)** | $45,000 | Assuming a SIEM license- Retail price for <50GB ingest per day |
| **External Threat Intelligence & Machine Learning** | $10,000 | Critical to clarify likelihood of attack, evolving and emerging attack types and methods, profiles of recent victims, and severity. |
| **Vulnerability Scanning** | $10,000 | Like SIEM, various options are available, and we applied the same conservative logic of pricing. Usage fees based on number of endpoints can contribute to costs, depending on the scanning product or service selected. |
| **General Office Expenses, SGA & Benefits** | $72,500 | Usage a 25% of base salary model |
| **ANNUAL COST FOR DIY** | **$442,500** | **Annual cost for Do-It-Yourself (DIY)** |
| AGILEBLUE | **$64,800** | **Assuming 500 workstations, O365, Cloud (Azure, AWS, GCP)<br>~50 servers, Firewalls<br>SOC-as-a-Service would run approximately $5,400/mo - or $64,800 annually** |

*Note: AgileBlue's pricing is based off the number of company connected devices

Source: AgileBlue

# THOUGHT-LEADERSHIP QUESTIONS

**Without proper threat detection tools, processes, and people, how would we be alerted about a threat today?**

- What visibility are we getting? What visibility are we NOT getting?
- Today, if we could respond, how would we respond?
- How long to learn we have a threat, and how long to respond?

**Do we have live staff to watch our cybersecurity 24/7?**

- How are we addressing holidays or weekends or hours hackers are working and we aren't?
- How often are we looking at all logs and alerts?

**What happens if we are breached because we weren't aware of the threat(s)?**

- What would happen to us operationally (downtime, cost to recover data, machines, time, etc)?
- What about our brand reputation?

## COMMON QUESTIONS THAT COME UP INTERNALLY

**What about the prevention tools we have today?**

AgileBlue typically doesn't replace your tools, but works in tandem with them. Security tools are designed to keep out known threats, but new threats are happening every day and prevention tools cannot keep up. If they could, we could have bought anti-virus and firewalls ten years ago and cybersecurity would not be a "thing". Think of AgileBlue as a powerful and comprehensive safety net that pulls in all your data, devices, logs, apps, etc. to detect when your tools get beat, or when you are being targeted for specific attacks.

**We are a smaller company with limited budget, why do we need to buy this?**

Prevention tools like anti-virus or firewalls only block most of the known threats. They don't stop new threats (0-day attacks), because definitions to block these new threats don't exist until AFTER the damage is done. Prevention tools can be a money pit, if you're not careful. Now, factor that each data breach cost averages in the millions. In some industries, the average cost per customer record is $150. If we are not monitoring threats, how do we prevent these extremely expensive and devastating surprises? We need a solution that scales to our size. AgileBlue gives us the tools and human capital to solve this in a way that easily fits the budget.

# COMMON QUESTIONS THAT COME UP INTERNALLY

**My last audit revealed that I need to log my critical infrastructure (firewall, servers, etc.) Does this keep me compliant and secure?**

While logging critical infrastructure is helpful and gains you some mileage in compliance, it doesn't guarantee you are fully compliant, nor does it suggest you've reduced risk properly, or enough. Keep in mind, that most threats are now existing and occurring in the cloud and with users, before they latch onto endpoints. AgileBlue satisfies a lot of regulatory compliance and security needs.

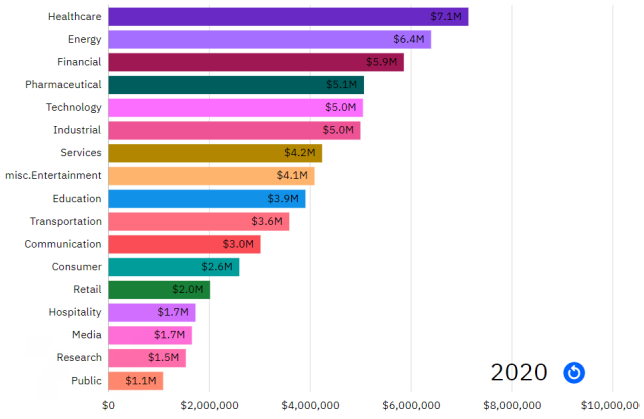
**Can't we just hire a few people to solve this?**

For a 24x7 Security Operations Center, four security analysts would be a minimum. Then, consider who is going to train, manage, and re-hire and re-train when they potentially leave. A SIEM tool is recommended in tandem with the SOC, then you need to build a SOC playbook. All of this would take most organizations 6 months to deploy, cost significantly more, and is typically a non-starter. AgileBlue is affordable and typical deployments are two weeks or less.

# WHY SOC-AS-A-SERVICE?

- Average SOC Analyst Salary is $55K - Assume you need to hire 4 SOC Analysts to cover 24 hours, you're looking at $220k in salaries per year.
- Minimum head count for 24/7 SOC is 4 analysts. This allows for breaks and time off. Note: One analyst per shift increases burnout.
- Internal SOC strategies typically only cover 20% of all alerts and 33% are false positives. This leads to burnout and studies show CISO's have a 63% desire to leave cyber security altogether.*
- Legacy SIEM tools typically have a range from $10,000-$100,000, per year, in the small to mid-sized space. This is based on what we've observed in 10 employee to 1,000 employee organizations.
- In 2020, Ponemon Institute discovered the average data breach to cost $3.86m. It also showed Healthcare as being the highest cost per breach at 7.1m and Public being the lowest at 1.1m**
- Regulatory compliance and audits are more frequently demanding that logs are both stored and reviewed consistently. We see this often in HIPAA, FFIEC, PCI, PII, CMMC, etc.

**AVERAGE COST (IN MILLIONS) OF A SINGLE BREACH PER INDUSTRY**




Source: Ponemon Institute

# WHY AGILEBLUE?

- Organizations are struggling with visibility into cloud, remote workers, and digital infrastructure. A lot of organizations using other SIEM products are limited to endpoints or firewalls, due to cost or technical limitations. AgileBlue's modern SOC-as-a-service has over 30 (and growing) integrations into your digital infrastructure, such as Office365, Salesforce, Microsoft, Cisco, etc.
- Varonis cites IBM that the average time to identify a breach in 2020 was 207 days.***AgileBlue has 30 minute response times to critical threats.
- Agent-based, no hardware required. Typical deployment times are 2 weeks or less. Significantly faster than 2+ month deployments seen with other similar type products or services.

Automated threat monitoring means faster detection in real-time

Our cyber risk scoring algorithm shows your risk gaps in real-time

With our pricing model, you're locked in a fixed monthly cost. No expensive surprises.

Our Silencer technology reduces false positives with a 95% confidence score

Ready to invest in your organization? Contact us or request a demo!