

ACILEBLUE
The AI-Powered SecOps Platform

LONG BUILDING
TECHNOLOGIES

CASE STUDY

Building Automation, HVAC
& Equipment Services



Table of Contents

Overview	01	The AgileBlue Difference	03
Challenges	02	Results & Outcome	04
The Solution	03	Contact AgileBlue	05



Overview

LONG Building Technologies is a leader in enhancing building performance through automation, efficiency, and safety. The company provides innovative solutions in HVAC systems, building automation, energy management, and equipment services. LONG relies heavily on secure, uninterrupted access to its enterprise systems, customer data, and internal IT infrastructure.

COMPANY:

LONG Building Technologies

HEADQUARTERS:

Littleton, Colorado

FOUNDED:

1965



INDUSTRY:

Building Automation, HVAC & Equipment Services

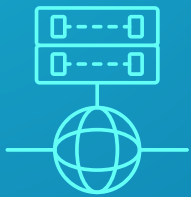
AGILEBLUE SOLUTION:

AI-Powered SecOps Platform, *Core Subscription*

WEBSITE:

LONG.com

Main Challenges



No centralized logging system



Inability to detect and respond to threats in real time



Manual monitoring processes consuming valuable IT resources



Limited insights to meet compliance and audit readiness

Challenges

Prior to partnering with AgileBlue, LONG Building Technologies was facing significant cybersecurity challenges including several gaps and inefficiencies, including the lack of real-time threat detection, insufficient monitoring of their systems, and the inability to effectively respond to potential cyber incidents.

01 Challenge

No centralized logging system to track activity across systems. Without a centralized logging system, LONG Building Technologies couldn't effectively track or investigate activity across its digital infrastructure. This left the IT team operating in a reactive state—unable to see the full picture or get ahead of potential threats.

"The lack of logging and always being reactive as opposed to proactive was a big driver in changing our processes," said Jason Johnson, vice president of IT.

02 Challenge

Inability to detect and respond to threats in real time. The absence of real-time detection capabilities made it difficult to identify and contain threats quickly. This increased LONG's exposure to risk and placed a burden on their internal IT resources to manually track potential incidents after the fact.

03 Challenge

Manual monitoring processes consuming valuable IT resources. Before AgileBlue, LONG's IT team relied on manual monitoring and reporting processes that were time-consuming and inefficient. This took focus away from higher-value strategic work and left room for human error in identifying issues.

04 Challenge

Limited insights to meet compliance and audit readiness. With no centralized data and minimal automation, meeting compliance requirements and preparing for audits was an uphill battle. The team lacked the insights and documentation needed to confidently align with industry standards and regulations.

“

"Cybersecurity isn't just an IT issue for us, it directly impacts our ability to serve clients, maintain uptime, and protect sensitive business data."

JASON JOHNSON

VP of Information Technology



The Solution

While others are still detecting, we have already responded. AgileBlue is an AI-powered SecOps platform, built to detect and stop cyberattacks.

We combine intelligent automation with real human analysts to protect your endpoints, cloud, and network 24/7.

AgileBlue's combines **eight critical security modules, in one platform**— built to detect faster and with precision, so you can go from reactive to proactive defense.



The AgileBlue Difference

From the start, AgileBlue brought a proactive, partner-focused approach that aligned with LONG's operational and budgetary needs. The AgileBlue platform integrated seamlessly with existing systems and immediately began delivering value.

What Stood Out to LONG Building Technologies:

- ✓ Seamless integration with LONG's existing tech stack
- ✓ AI-powered threat detection and real-time alerting
- ✓ Cost-effective compared to other platforms
- ✓ Actionable insights with automated reporting and logging
- ✓ Highly responsive SOC team and customer support

“

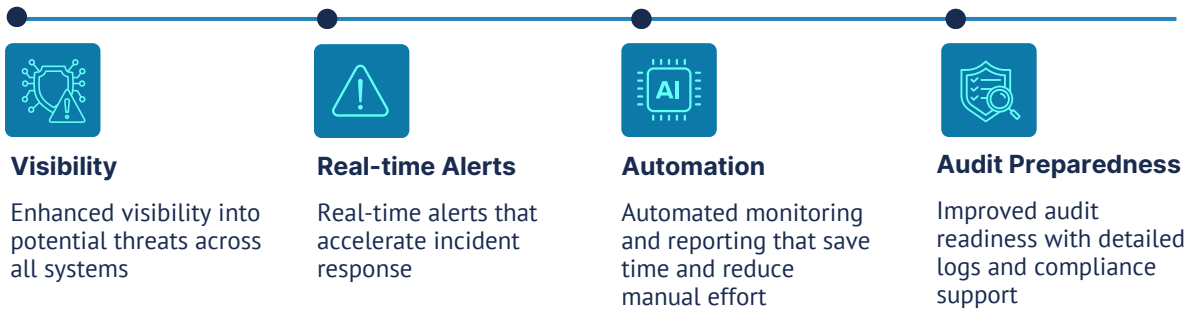
"AgileBlue has transformed our approach to cybersecurity, providing us with the tools and insights needed to protect our critical systems and data effectively. Their platform and team have been instrumental in enhancing our security posture and ensuring peace of mind."

JASON JOHNSON

VP of Information Technology

Results & Outcome

Since implementing AgileBlue, LONG Building Technologies has significantly strengthened its cybersecurity posture. What was once a reactive process is now a proactive, data-driven strategy.



Business Value & Peace of Mind

Perhaps the most meaningful result for LONG Building Technologies has been the peace of mind that comes from knowing their systems are monitored around the clock. The IT team now spends less time chasing alerts and more time focused on strategic initiatives.

One example came when AgileBlue flagged a suspicious file that resembled ransomware. The AgileBlue SOC team immediately investigated and alerted Johnson's team. "Fortunately, it was a false positive," Johnson said. "But the speed and clarity of the response gave us real peace of mind."

AI-Powered Outcomes

AI automation has fundamentally transformed LONG Building Technologies' cybersecurity operations. With real-time, AI-powered alerts, the team now responds to threats faster and more confidently.

By automating monitoring, triage, and reporting, AgileBlue has significantly reduced the manual workload on IT staff, allowing them to focus on more strategic initiatives.

From Alert Fatigue to Confidence and Control

Since implementing AgileBlue, LONG has transitioned to a security posture defined by real-time visibility, automation, and peace of mind. The shift from manual monitoring to AI-driven detection has allowed the IT team to focus on high-value work instead of chasing false alarms.



Real Security, Means Real Partnership.

Most vendors vanish after onboarding. Not us. AgileBlue combines 24/7 AI-powered threat protection with a dedicated SOC team and proactive support that never goes dark.

It's why 96% of our clients stay with us—because we don't just detect threats, we act on them.

Contact Us →