Automated Logic

Technical Guide

Optimizing Building Automation System (BAS) Security with Network Isolation

The New Frontier of BAS Security

In today's intelligent buildings, the building automation system (BAS) has advanced far beyond simple controls, now acting as the facility's central nervous system to manage key functions such as HVAC, lighting, security, and energy management. This increased connectivity and sophistication also creates new points of vulnerability. As a result, specifiers have a vital responsibility to consider more than just a system's efficiency and functionality. They must now take steps to help make these systems more secure and resilient against cyber threats.

A 2025 report shows that while the global average cost of a data breach declined for the first time in five years to $4.44 million, the United States average breach cost rose to a record high of $10.22 million, a 9% increase over last year.[i] This guide will explore a technical framework for achieving enhanced BAS security, focusing on network segmentation and the critical role of a specialized network router in helping to protect a client's business continuity, their investments, and increase the safety of occupants. By incorporating industry best practices and keeping pace with cybersecurity trends, specifiers can demonstrate their commitment to excellence and build critical trust with their clients.

$4.44M

GLOBAL AVERAGE COST OF A DATA BREACH [i]

$10.22M

UNITED STATES AVERAGE COST OF A DATA BREACH (SURGING BY 9% -AN ALL-TIME HIGH)[i]

Automated Logic

[i] Cost of a data breach 2025 | IBM. (2025). Ibm.com. https://www.ibm.com/reports/data-breach

The Principle of Network Segmentation

A critical first step in specifying a secure building is understanding the difference between Information Technology (IT) and Operational Technology (OT). IT refers to the traditional systems that manage data for business operations, like computers and servers. OT, on the other hand, is the hardware and software that directly monitors and controls physical processes and devices, such as HVAC, lighting, and access control systems. These systems are the building's operational nervous system.

The convergence of IT and OT in modern smart buildings has created a new, complex attack surface. A breach in an OT environment, for example, can have a tangible impact, disrupting business operations and may even cause physical damage. In fact, studies indicate that BAS security system complexity and compromised IoT and OT environments are both factors that increase the average cost of a data breach.[ii] As a specifier, you have a vital role in ensuring these two worlds are connected securely yet remain segmented to mitigate risk.

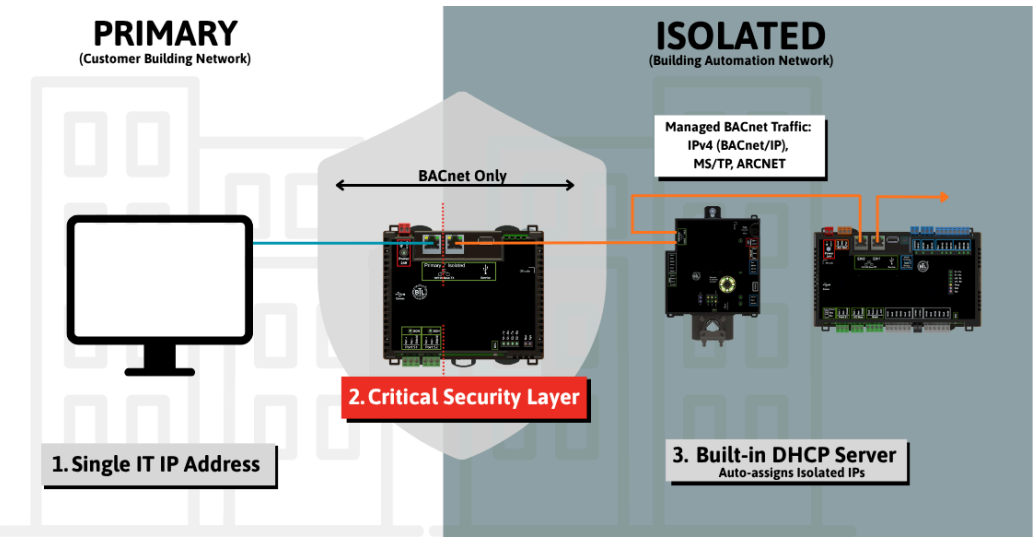
Benefits of Segmentation

Threat Reduction: By isolating the OT network, a security breach in one part of the network cannot easily spread to other critical areas.

Reduced IT Complexity: A segmented network can help simplify IT management by providing a single, controlled point of access.

Enhanced Performance Reliability: By isolating building automation traffic, a router can manage communication more efficiently, ensuring that critical control commands are not delayed by other network activity.

Actionable Insight: To help reduce risk and cost, avoid over-complicating the system. A well-designed, segmented network can help simplify the management of security policies and make it easier to monitor for suspicious activity, which is a factor that can contribute to the total cost of a data breach.



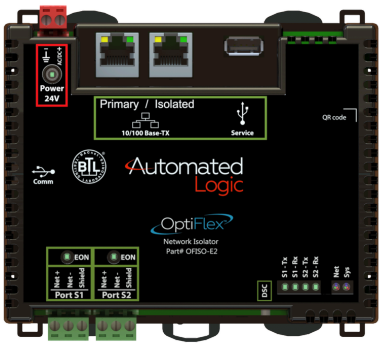
[ii] IBM. (2025). Cost of a data breach report 2025: The AI oversight gap (T. J. D. C. P. J. R. & P. J. F., Eds.). IBM Security. https://www.ibm.com/reports/data-breach

Automated Logic

Streamlining Communication and Integration

In addition to supporting BAS security, a thoughtfully designed network architecture should facilitate efficient communication and support integration across diverse systems. A specialized router, such as those designed for building automation, can serve a central connection point for multiple building protocols. This enables integration of environmental, energy, security, and safety systems, helping to streamline operations within a cohesive platform.

Automated Logic OFISO-E2: A Specialized Router for Secure Integration

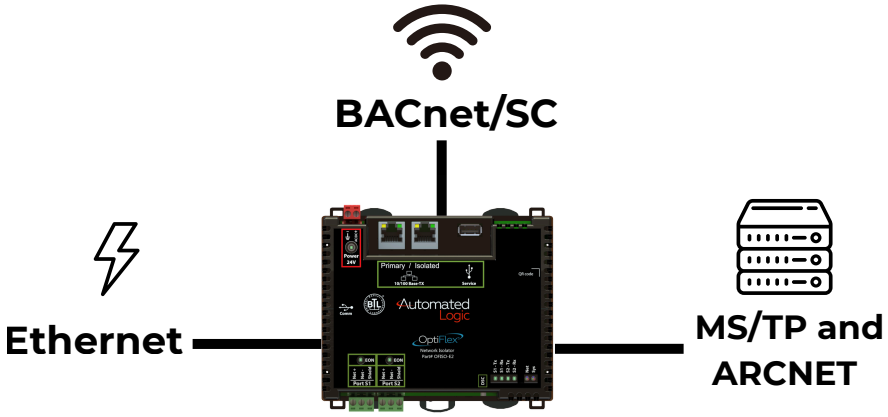


A key component in this architecture is a specialized router, such as the Automated Logic OFISO-E2, which is designed to facilitate communication among multiple building protocols. It supports integration capabilities across a range of environmental, energy, security, and safety systems, helping to streamline operations within a unified platform.

Routing Capability: A well-designed router can support the routing of BACnet traffic across widely used network types, including IP, Ethernet, BACnet Secure Connect (BACnet/SC), ARCNET, and MS/TP, helping promote compatibility with a broad range of infrastructure. This adaptable approach supports the implementation of open protocols with built-in security features, aligning with evolving industry standards.

Flexible Network Connections: Such a device provides flexible connectivity options:

- **Primary Port:** One 10/100 BaseT Ethernet port for communication with BACnet/IP, BACnet/IPv6, BACnet/Ethernet, and/or BACnet/SC networks.
- **Isolated Port:** One 10/100 BaseT Ethernet port for a separate BACnet/IP network.
- **EIA-485 Ports:** At least two EIA-485 ports for communication with BACnet ARCNET and/or MS/TP networks.



Actionable Insight: When specifying protocols, it's important to prioritize those that support open integration and incorporate security features. This includes recommending protocols designed to help protect data integrity and confidentiality during transmission and storage.

Deployment, Diagnostics, and Specifications

A secure system involves more than just technology; it also depends on ease of deployment and long-term maintainability. Specifiers are encouraged to consider solutions designed with future scalability and operational efficiency in mind.

Streamlined Deployment and Diagnostics:

Built-in DHCP Server: The inclusion of a DHCP server can help automate IP address assignment in isolated networks, potentially simplifying configuration and reducing installation time.

Local Configuration: A dedicated USB port enables local system setup and troubleshooting via a direct connection to a computer or compatible wireless service adapter.

Advanced Diagnostics: The device is designed to capture network data and statistics to assist with troubleshooting and performance monitoring.

LED Status Indicators: Visual indicators, including Tricolor NET LED and Tricolor SYS LED, provide feedback on network and system status, along with additional LEDs for power and port activity.

Specifications:

Power Requirements: The device operates on either 24 Vac (±10%, 50-60 Hz, 50 VA) or 24 Vdc (±10%, 18 W).

Environmental Range: Operates in a wide temperature range from -40 to 158°F (-40 to 70°C) with 10-95% non-condensing relative humidity and can be installed both inside and outside the building envelope in a UL listed enclosure.

Memory: 8 GBs eMMC Flash memory (120 MB available for use) and 512 MB DDR3 RAM.

Mounting: 35mm DIN rail mounting or screw mounting.

Actionable Insight: Consider specifying a router that includes an integrated DHCP server. This feature can help streamline installation and commissioning by automating IP address assignments, which may reduce setup time and lower the likelihood of configuration errors. When evaluating network architecture, look for routers that require only a single IP address from the corporate network, this can support efficient IP resource management. In some cases, this design may also contribute to network isolation, potentially easing the IT team's administrative workload.

Automated Logic

Optimizing BACnet Communication and System Integration

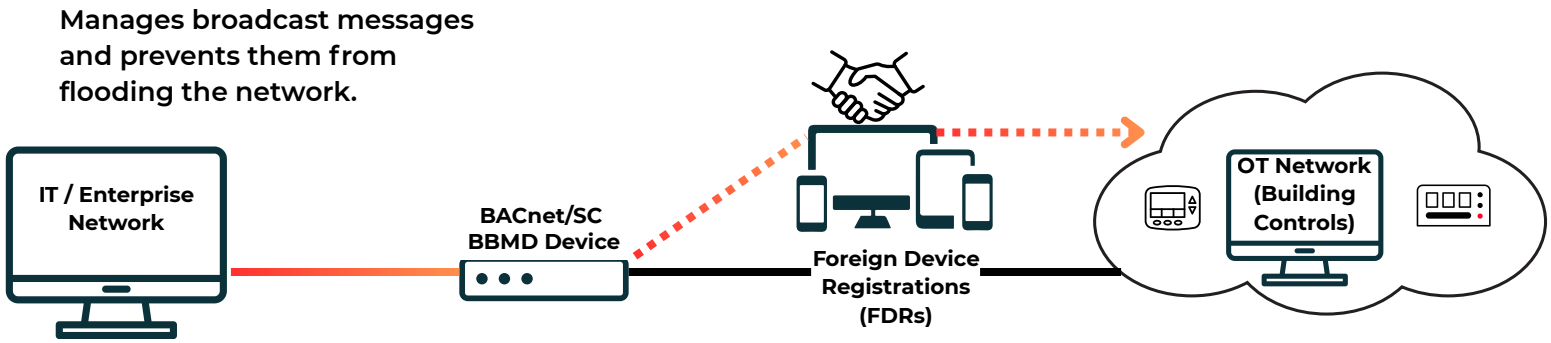
A resilient system should be designed with the end-user in mind, aiming to support operators with accessible interfaces and effective communication tools. Selecting solutions that offer intuitive user experiences and streamlined connectivity can help simplify system management. A specialized router can play a key role in facilitating communication across building automation systems, contributing to more coordinated and responsive operations.

Optimized Broadcast Communication: The router should function as a BACnet Broadcast Management Device (BBMD) to manage broadcast communication efficiently on BACnet/IP networks, reducing traffic, and improving response times.

Simplified BACnet Device Integration: The device should support Foreign Device Registration (FDR), enabling automatic discovery and registration of third-party BACnet devices to streamline communication within the BACnet network.

Intuitive Interfaces: Look for platforms with intuitive, visual interfaces that make complex building systems easy to understand and manage. An intuitive interface can help empower operators to act quickly and confidently, which may improve response times and contribute to operational efficiency. For example, look for platforms with high-definition, factory-generated graphics and point-and-click navigation.

How a BACnet Broadcast Management Device (BBMD) Works



Actionable Insight: When developing your specifications, consider including a router that supports BACnet Broadcast Management Device (BBMD) functionality. This feature can help manage broadcast traffic more efficiently, contributing to improved network responsiveness as size and complexity increase. Additionally, support for Foreign Device Registration (FDR) may simplify the integration of third-party devices, potentially reducing the effort and cost associated with system expansion or upgrades.

Automated Logic

Cybersecurity

U.S. and Canadian Cybersecurity Frameworks

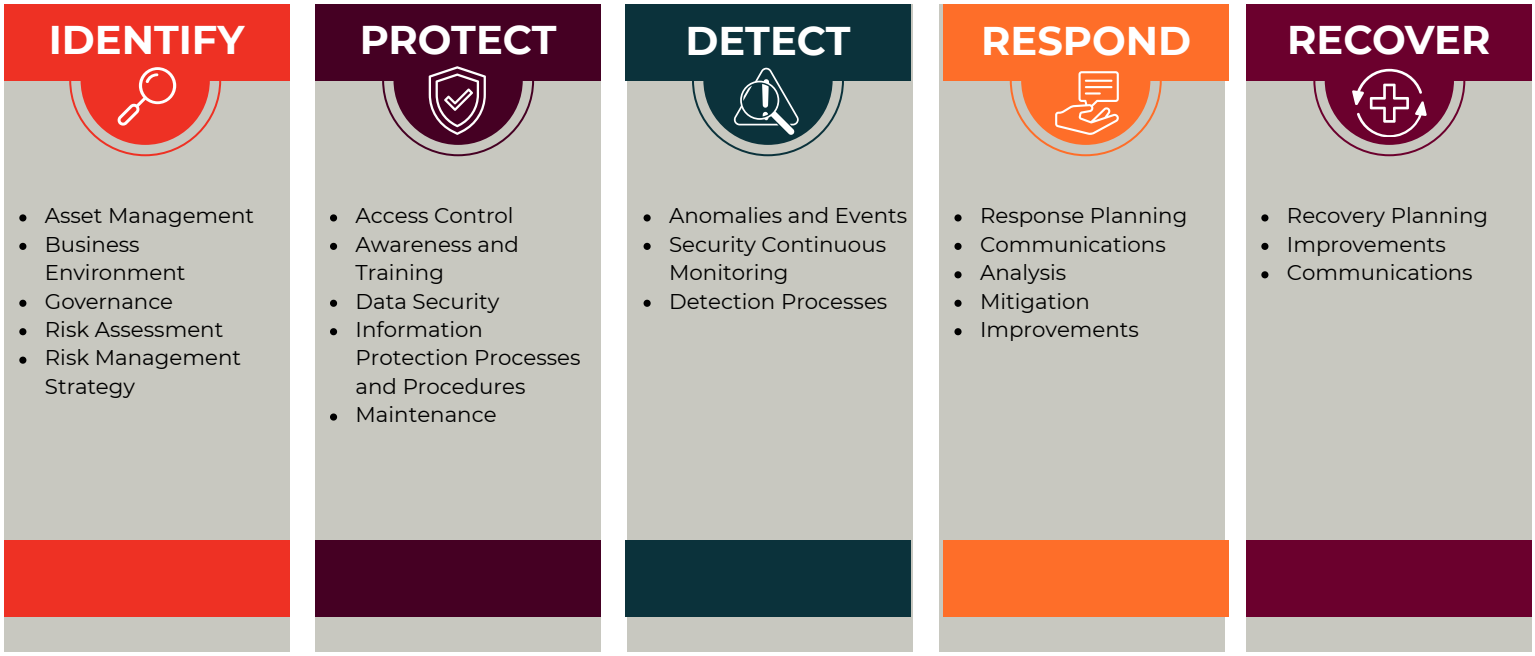
In the United States and Canada, cybersecurity frameworks primarily consist of voluntary guidelines and best practices aimed at managing risk. Regulatory requirements tend to focus on critical infrastructure sectors.

NIST Cybersecurity Framework (U.S.)

The National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF), which is widely referenced and structured around five core functions: Identify, Protect, Detect, Respond, and Recover.

The OFISO-E2 router is engineered to support aspects of the Protect function by offering features that help safeguard building systems. Its network segmentation capabilities can assist in isolating operating systems from IT networks, which may help limit the spread of potential threats. Additionally, support for encrypted BACnet/SC communication contributes to maintaining data confidentiality and integrity, a key consideration in cybersecurity protection strategies.

NIST Cybersecurity Framework



Canadian Centre for Cyber Security (CCCS) (Canada)

Canada's cybersecurity landscape is shaped by guidance from the Canadian Centre for Cyber Security (CCCS). Including resources like the Cyber Security Readiness Goals (CRGs). These goals outline cross-sector cybersecurity practices intended to strengthen the cyber resilience of essential services.

The OFISO-E2 router is designed to support network resilience by offering features that help establish secure zones and managing data flow. These capabilities may assist in aligning with CRG objective related to network security and access control. When implemented as part of a broader cybersecurity strategy, such features can contribute to hardening building automation networks against potential cyber risks, an important consideration in CCCS's guidance for critical services.

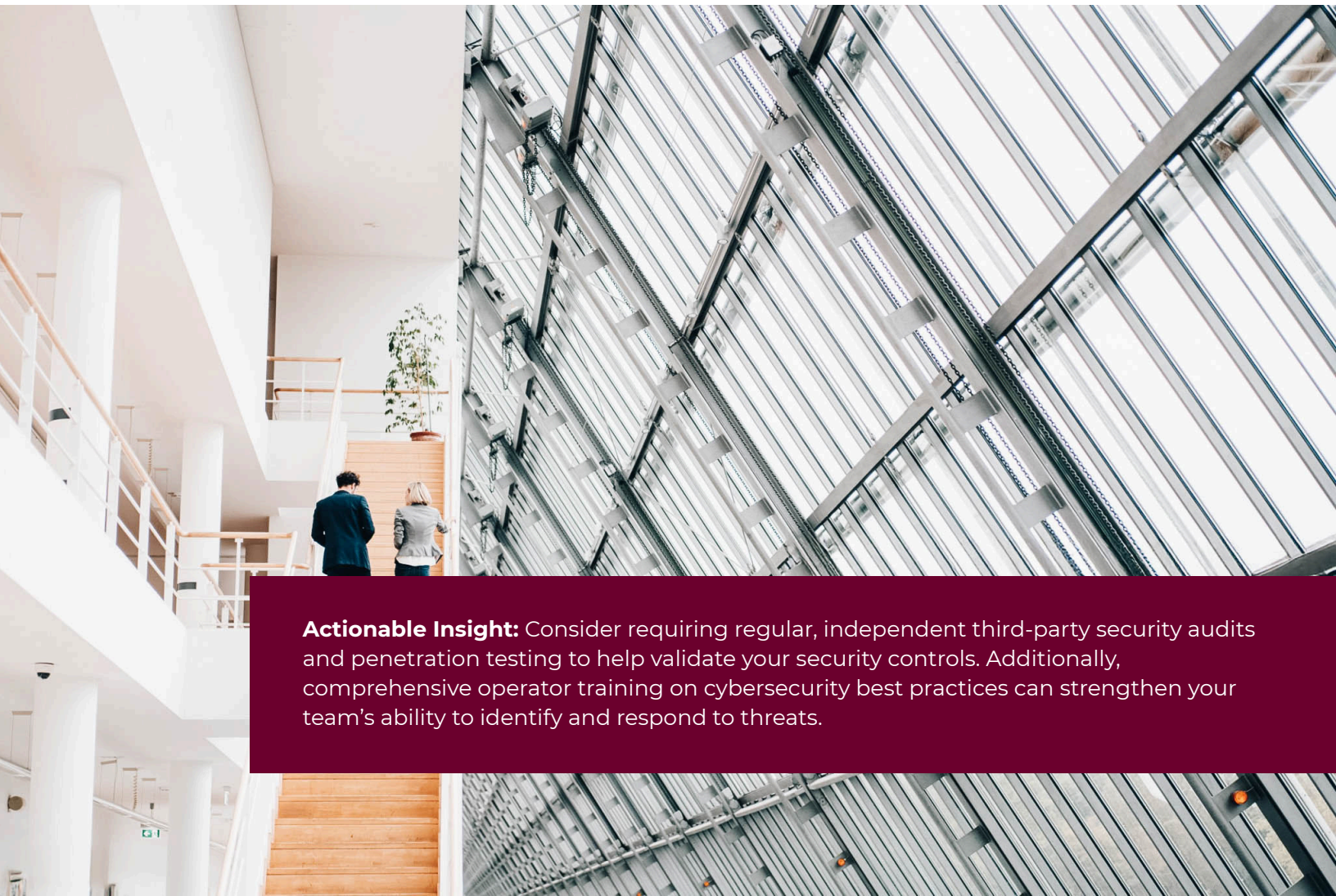
The Long-Term View of a Secure System

A secure and resilient system involves more than just technology; it also depends on the people who operate it. Specifiers are encouraged to prioritize long-term system viability and operational readiness.

Secure Development Practices: Recommend that manufacturers follow secure coding practices and perform regular vulnerability assessments throughout their product's development lifecycle to help reduce exposure to security risks.

Long-Term Viability: Specify systems that are designed with long-term customer value in mind, including support for backward compatibility across versions. This can help building owners upgrade gradually, potentially reducing the need for costly system overhauls and minimizing operational disruptions.

Proactive BAS Security Stance: BAS security should be viewed as an ongoing process. Specifiers may require comprehensive training and documentation, along with systems that support automatic security updates and patching to address emerging vulnerabilities. Independent, third-party security audits and penetration testing can also provide valuable insights into the effectiveness of security measures.



Actionable Insight: Consider requiring regular, independent third-party security audits and penetration testing to help validate your security controls. Additionally, comprehensive operator training on cybersecurity best practices can strengthen your team's ability to identify and respond to threats.

Conclusion

By applying these actionable insights to your specifications, you can help advance the building automation systems that aim to be efficient, secure, and resilient, for the evolving operational and cybersecurity demands. Your expertise in this critical area plays a vital role in supporting the protection of your clients' assets, personnel, and their reputation, while contributing to a more secure and reliable built environment.

To learn more about how a comprehensive building automation system, paired with a dedicated network isolation router, can support these goals, contact your local authorized dealer. They can offer guidance on designing, engineering, installing, and maintaining solutions aligned with your project's requirements.

Automated Logic

Find a Dealer:
https://www.automatedlogic.com/dealers

1150 Roberts Boulevard, Kennesaw, Georgia 30144
770-429-3000 | automatedlogic.com | A Carrier Company

 v10/25