ATRIUS®

atrius.com

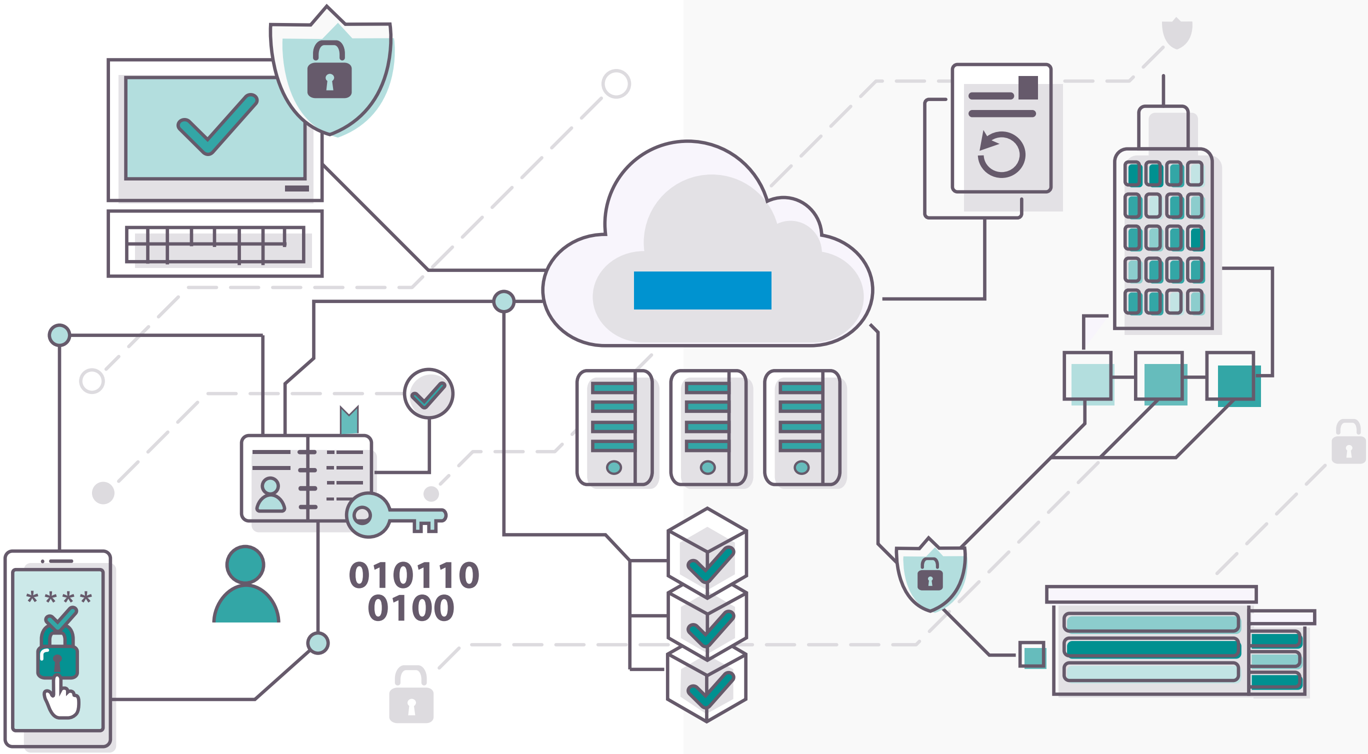
Building Insights

Security Overview

Hundreds of organizations across healthcare, financial services, education, and other industries deploy the energy management software solution, Atrius® Building Insights from Acuity Brands.

ACUITY BRANDS SECURITY
Prevent. Detect. Respond.

Acuity Brands is committed to providing security, scalability and reliability in the Building Insights platform.



Atrius is part of the Intelligent Spaces Group within Acuity Brands, a market-leading industrial technology company.

Physical Security

The Building Insights platform is hosted on Microsoft Azure, a state-of-the-art cloud services solution, which uses a wide variety of physical, infrastructure, and operational controls.

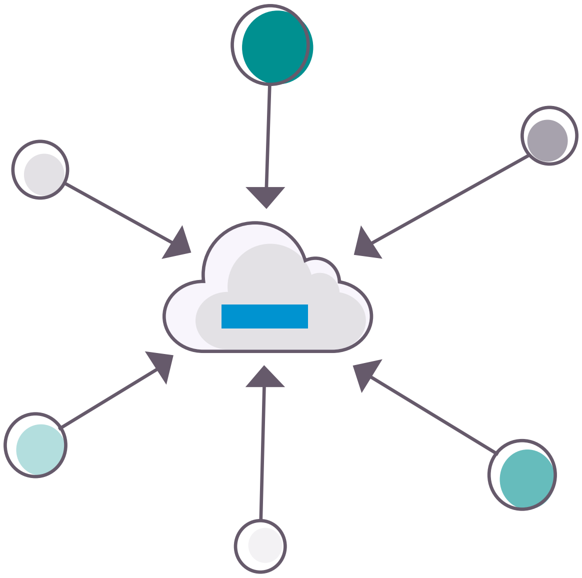
Azure employs redundant systems designed to ensure network uptime, power availability, cooling, and biometric security. Azure provides*:

- Independently managed SOC2 Type 2 and PCI compliant data centers
- 24-hour, 365-day year-round security including video surveillance, foot patrols, and perimeter inspections
- Computing equipment housed in access-controlled state of the art steel containers
- Facilities engineered for local seismic, storm, and flood risks
- Geographic redundancy and elevated disaster recovery

*Visit Microsoft's Azure Security Fundamentals documentation for more information.

Network & System Security

Building Insights software integrates with various business, building, and utility systems through a wide range of one-way protocols. These integrations are one-way into Building Insights, meaning that Building Insights does not write data into other systems. The one-way connection makes it harder to use the system as a jumping off point for malicious activity, thereby limiting the risk profile of Building Insights relative to these other systems.



All Building Insights functions, including authenticated services such as logging in, using the REST API, or transmitting data to the platform, follow the Transport Layer Security (TLS) protocol. TLS is a protocol designed to provide communication security, thereby enabling customer data protection. Additional network and security controls include:

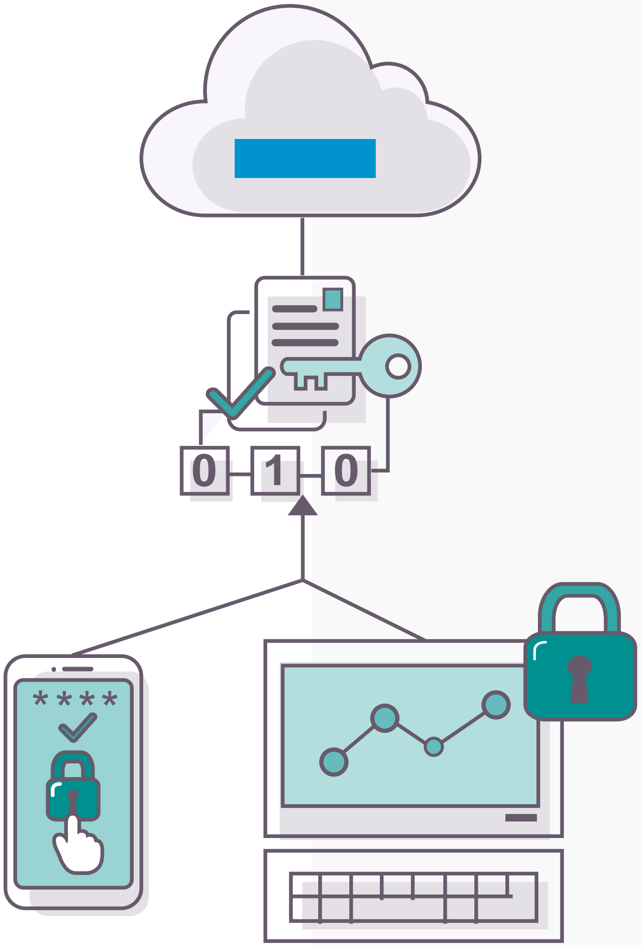
- Perimeter firewalls and edge routers that block unused protocols
- Unique tokens created at login to identify and re-verify each transaction during individual user sessions
- Secure transmission and user sessions via SSL 3.0/TLS 1.2
- All systems run in isolated docker containers based on consistent images that are tested and scanned for vulnerabilities before deployment.
- Role Based Access Control (RBAC) for all resources leveraging the principle of least privilege

Application Security

ATRIUS®
atrius.com

Building Insights protocols comply with industry standards for privacy and network security. Building Insights access is encrypted for privacy.

Building Insights supports many identity providers such as Okta® Single Sign-On (SSO) and Azure Active Directory™ using OpenId Connect, allowing customers to reuse their existing user management solutions.

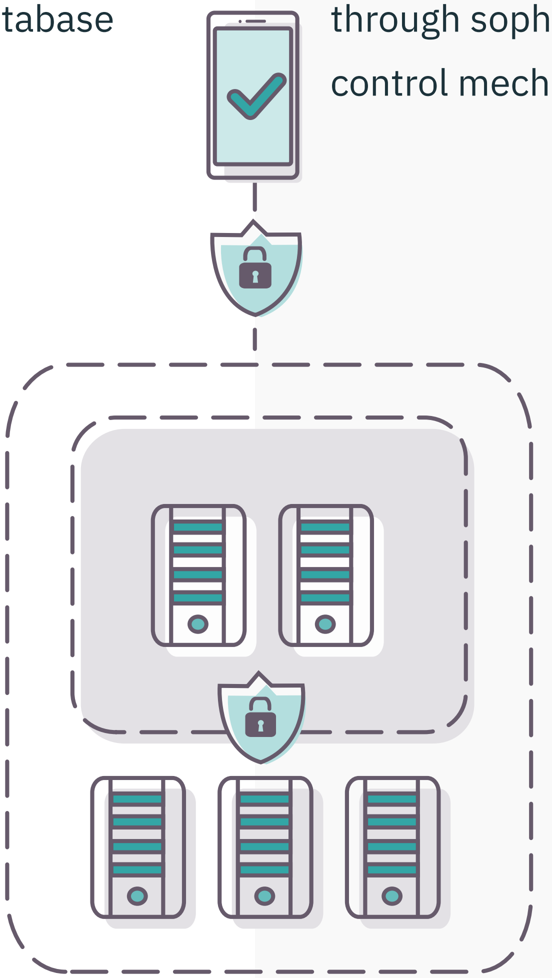


Atrius is part of the Intelligent Spaces Group within Acuity Brands, a market-leading industrial technology company.

Data Security

Building Insights secures access to the platform using Azure Web Application Firewall (WAF) with intrusion detection. External systems handling data are cordoned into a demilitarized zone (DMZ). All customer metadata stored in the production database is encrypted at rest.

The Building Insights platform protects customer data with system level features, centralized logging, and privilege separation. Although Building Insights is a multi-tenant system, all data for a given customer is isolated from other customers through sophisticated access-control mechanisms.



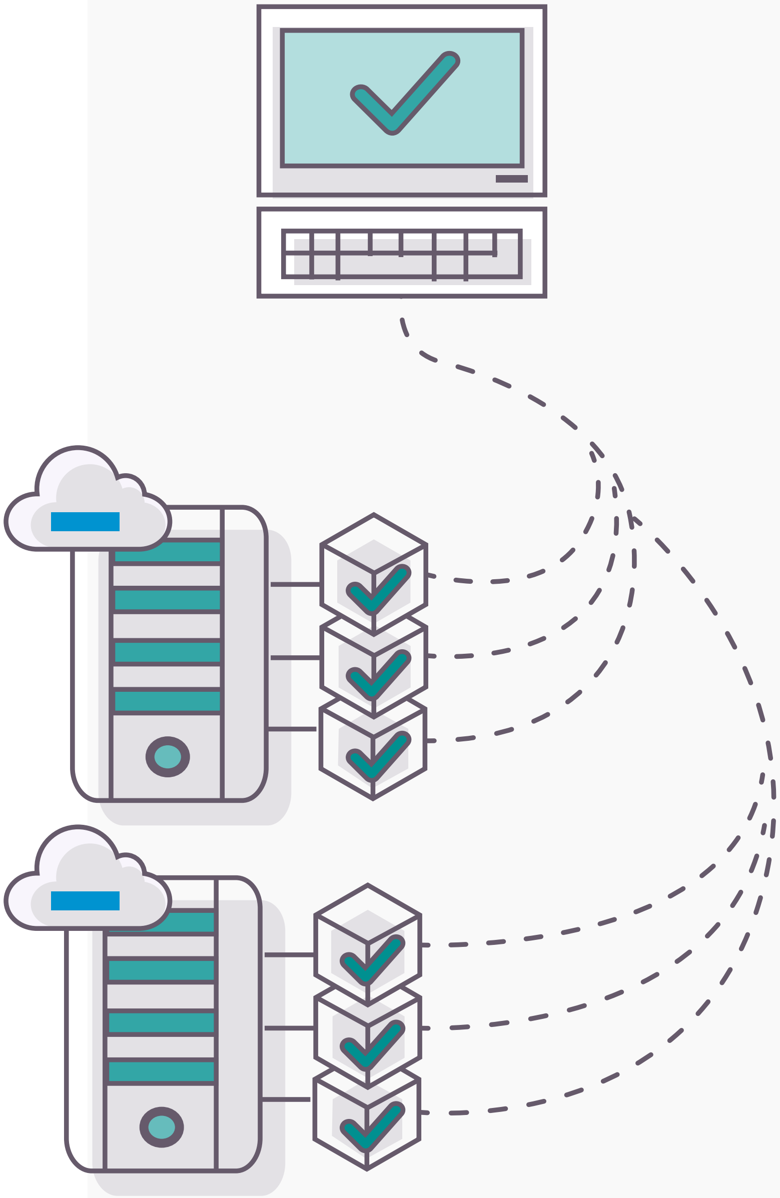
Reliability & Resilience

Building Insights is built on a fault-tolerant software stack with high availability (HA) to maximize uptime and operational performance.

All interactive services are fronted by efficient load-balancing technologies designed to ensure a highly available system while maintaining responsive end-user experiences.

Building Insights maintains a 99.9% uptime, except during periods of planned outages and routine maintenance, as backed by a Service Level Agreement (SLA), available by request.

Attention to reliability extends to Building Insights data collection services as well. Building Insights stores data on redundant disk arrays spread across a cluster of storage servers.



Third-Party Validation

Internal and external security and reliability evaluations are performed regularly.

Building Insights evaluations also include an annual penetration test performed by a leading global cybersecurity solutions provider.

End User Privacy

Acuity Brands is committed to respecting customers', employees', and the general public's privacy. We comply with applicable privacy legislation, including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

As part of this effort, the Privacy Policy on our webpages details how we use information we collect and describes the process by which people can request changes and deletions to their information.

Additionally, we provide information about how we use tracking software (cookies) and how the public can restrict such tracking.

Atrius Building Insights collects only minimal personal information as required for user access and role mapping.