Connect Security

Traditional BAS Security Approach

Traditional building automation systems (BAS) and non-Cloud analytics solutions require installers or end-users to deploy their server solutions within a corporate network. While there is nothing inherently insecure about deploying vendor solutions within corporate networks, there is an increased responsibility taken on by the installer and end-user to ensure that the solutions are deployed in a secure manner. This includes taking responsibility for:

- SSL certificate management
- Network access management (Public and Private)
- Database management
- Application maintenance
- Operating System maintenance
- Hypervisor maintenance
- Physical security to data centers

When a vendor system is deployed, specifically in the building automation and analytics space, the expectation of the vendor and end-user is that the system is available from any location and any device. This is typically accomplished in one of two ways:

- VPN Access
- Exposing the application to the internet with a public IP address

Once the solution is exposed to the internet with a public address, that solution is now a target for attackers to leverage as a penetration point into the corporate network. While some attacks target applications like building automation and analytics systems, the attackers are typically more interested in corporate information that is placed behind the firewall with no direct access from the internet.

Traditional building automation systems (BAS) and non-Cloud analytics solutions, that require top-to-bottom management by vendors and end-users, are more susceptible to cyber-attacks.

Connect Security Approach

To address the security weaknesses in traditional BAS models, **Key2Act®** has architected the Connect and **ESMS℠** solution in a significantly different manner:

Fully Managed Cloud Services

- The Connect application service is deployed in a fully managed cloud in AWS
- The Connect database server is deployed in a fully managed cloud in AWS

AWS (Amazon) Handles	Key2Act® Handles
Operating System maintenance (Database)	Operating System maintenance (Application Servers)
Hypervisor maintenance	Network access management (Public and Private)
Physical security to data centers	Database management
	Application maintenance

SSL Communications between Clients and Server/Database

- Connect MiniAgents communicate with the Connect database and application server using SSL
- The Connect Desktop Application communicates with the Connect database and application server using SSL

Proprietary Communications Protocol

Our "mLink" protocol employs a proprietary messaging system that only **Key2Act®** devices and applications are able to decrypt.

MiniAgent Client Certificates

All MiniAgents are configured with a client certificate to identify it as a **Key2Act®** MiniAgent. This ensure that Connect can only talk to our MiniAgents and nothing else.

Outbound Only Ports for On-Premises Components (MiniAgent and Connect Desktop)

Instead of exposing the Connect MiniAgent to the internet, which would mark the MiniAgent as a potential penetration point into the corporate network, the MiniAgent sits securely behind a firewall and only requires outbound ports for communication with the Connect database and application server.

By employing the above security features Connect allows vendors and end-users to:

- Remove the need to handle top-to-bottom management and maintenance of the solution
- Securely access live and historic building automation data without exposing those systems to the internet

With the Connect tunneling feature, **Key2Act®** provides vendors and end-users access to the building automation system in a manner significantly more secure than the required exposing of other vendor solutions to the internet.

By architecting **Key2Act®** cloud solutions in the manner described above, a cyber-attack would be near impossible, and minimizes potential impact to vendors, building owners, tenants, and their end-users.