buildingsIOT

Secured Edge-to-Cloud Communication: LaunchPad's Resilient Cybersecurity Framework

LaunchPad's cybersecurity framework is built upon a secured edge-to-cloud architecture, prioritizing data protection and ensuring reliable communication. The key components of this framework are the Arcbeam protocol and AWS System Manager (SSM).

The Arcbeam protocol acts as a bridge between the cloud and the LaunchPad devices, facilitating secure outbound communication across the network. It leverages HTTPS protocol and establishes encrypted connections, ensuring data confidentiality. This means that all data transmitted from the LaunchPad devices to the cloud is protected and inaccessible to unauthorized parties. To enable communication, the protocol requires valid and verified certificates on both ends, establishing mutual TLS authentication. This authentication process guarantees that only authorized entities can access the system, further enhancing overall security.

LaunchPad also takes measures to protect the data stored on the devices themselves. The hard disk on each LaunchPad device is encrypted, adding an extra layer of security to prevent unauthorized access in case of physical theft or tampering.

An important benefit of LaunchPad's architecture is that it eliminates the requirement to open incoming ports in the network firewall. LaunchPad devices initiate outbound communications only and do not accept incoming connections from external sources. This helps to reduced attack surface and minimizing the risk of unauthorized access.

In addition to secure communication and data protection, LaunchPad implements a user account system on each device, ensuring that individual passwords are required for each account. This adds an extra layer of authentication and access control, further safeguarding the system.

AWS SSM, a powerful system manager, plays a crucial role in managing and maintaining the LaunchPads up to date. It centralizes device management, allowing administrators to easily ensure that all devices have the latest security patches and updates. Additionally, SSM enables compliance management, automatically identifying any LaunchPad that is not in compliance with the defined standards. This proactive approach helps identify and rectify security vulnerabilities promptly.

To safeguard data during transit, all communications within the LaunchPad ecosystem are encrypted. This encryption in transit ensures that information exchanged between devices and the cloud remains confidential.

The security measures extend beyond communication and data transmission. LaunchPad incorporates robust login and auditing mechanisms. In case of any issues or incidents, administrators can remotely access device logs, eliminating the need for physical onsite inspection. This feature streamlines the troubleshooting process and enables prompt incident response.

In summary, LaunchPad's cybersecurity framework, fortified by the Arcbeam protocol, AWS SSM, encrypted hard disks, outbound communications, and various other security measures, provides a resilient and protected environment for efficient edge-to-cloud communication.

Configuration

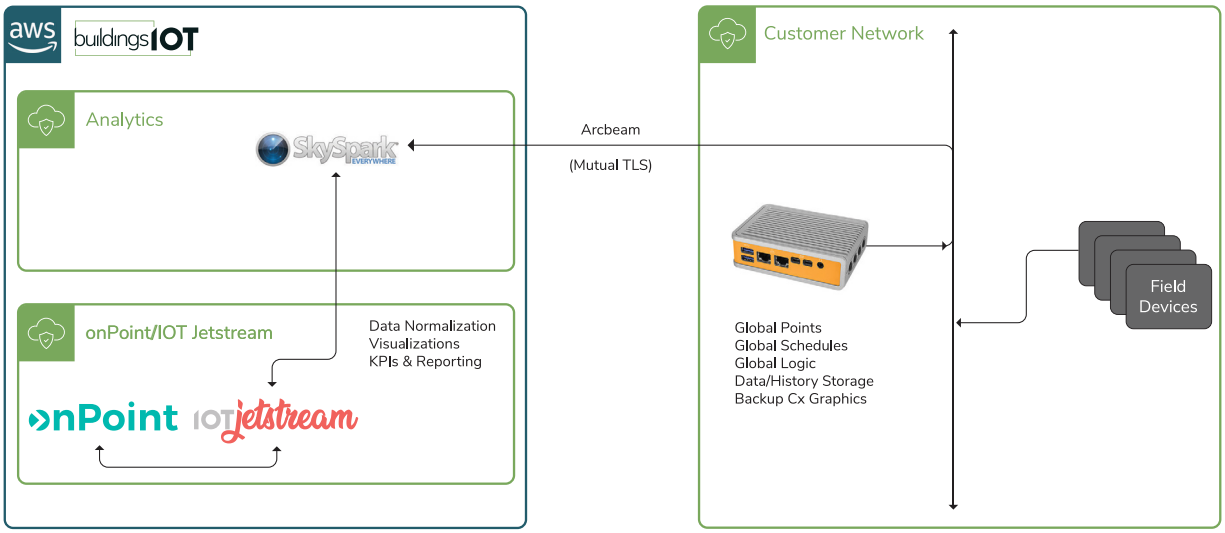

Figure 1: BMS Network has outbound internet access. LaunchPad is configured before panel installation with static IP or DHCP.

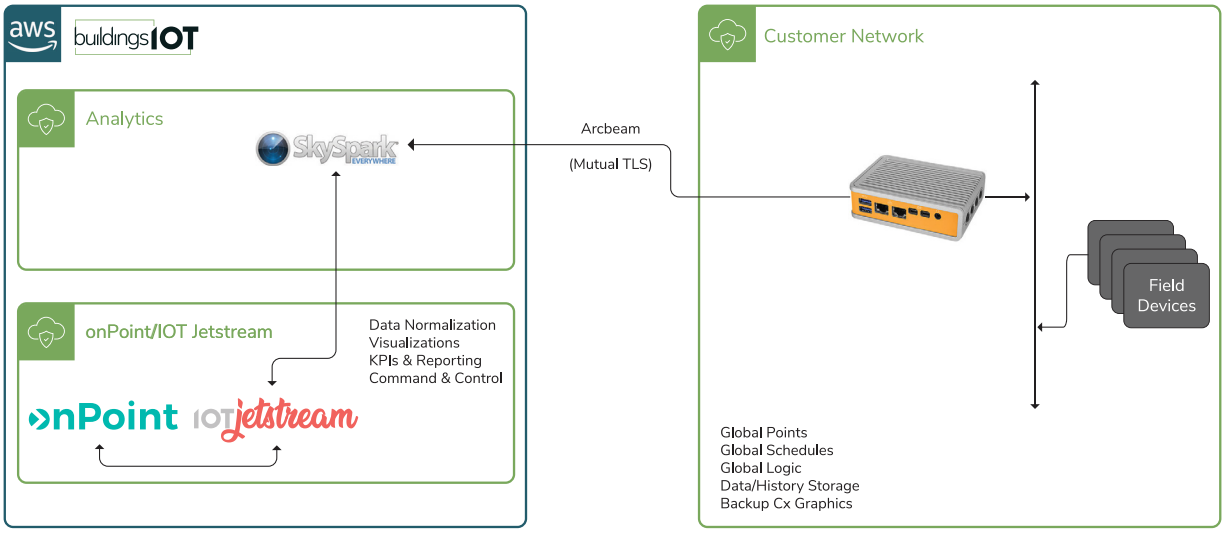

Figure 2: Dual IP configuration is required if the BMS/OT network does not have outbound internet access. There is no routing between networks so the LfC option is not available in this configuration.