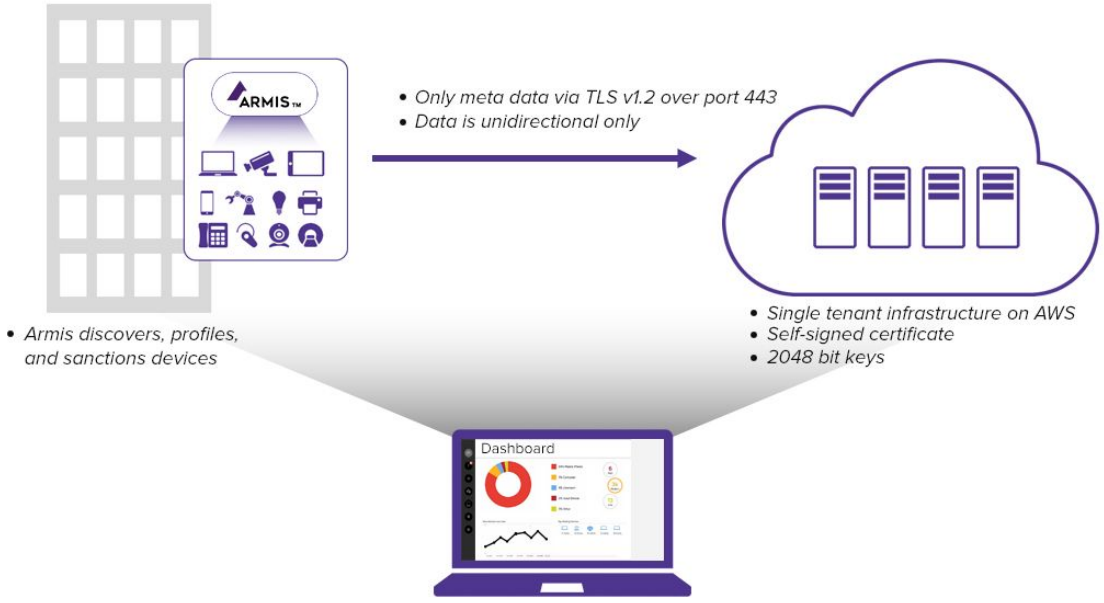
ARMIS CLOUD OVERVIEW

THE ARMIS CLOUD

Armis is primarily a cloud-based solution. All of the compute-intensive risk analysis, machine learning and threat detection that we do is done in the cloud. This allows customers to deploy Armis rapidly and not have to worry about server maintenance or administrative tasks.

Where Is the Armis Cloud?

The Armis risk analysis engine and device knowledgebase run in the AWS cloud. Each Armis customer gets its own database, instances, and certificates; these are not shared between organizations (single-tenant, as opposed to multi-tenant). The AWS servers and data are located in the United States by default, but we can locate servers and databases anywhere upon request.



What Data Is Sent to the Armis Cloud?

Armis only sends metadata to the cloud, meaning we never capture or transmit any data payloads. The metadata we send includes:

- Device profile attributes, for example, details like IP, MAC addresses, user names, type / category, model, OS, running apps, etc.)
- Device communication details, for example the wireless MAC layer (WiFi / BlueTooth), protocols used (HTTP, HTTPS, VOIP, etc.), what amount of data, encryption level, etc.
- Headers of the communication, but not the actual data payloads (the requests and the headers of responses, DHCP packets, etc.)
- Metadata representing connection and session set up exchanges, such as handshakes, synchronization, channel / encryption negotiation.

How Much Data Is Sent?

Actual transfer rate depends on the scope of the deployment, but the amounts sent are very low. Historically, we see about 5GB per week for a medium size organization.

How Is The Information Secured?

- Communication of customer data is unidirectional (Armis does not read data from the cloud, just write).
- Communication is over TLS version 1.2 over port 443.
- Secured Communications:
    - Armis uses its own certificate (self-signed with SHA256) for both appliance and server
    - The keys are 2048 bit, with Elliptic Curve Diffie-Hellman ephemeral (ECDHE-RSA) key exchange
    - The encryption is the ChaCha20 stream cipher with poly1305 message authentication.
- Armis DB's are encrypted at rest.
- Armis access to the organization's data is strictly limited to Armis' internal technical team.
- All data can be permanently deleted based on agreed timing specified in the process. We do this by deleting single tenant database, along with its local storage, and all snapshots.

What if the link between the Armis virtual appliance and the Internet goes down?

Armis virtual appliances, which are located on customer premises, can operate independently in terms of enforcing policy. They continue to enforce policy even if the link to the Armis cloud is disrupted.

What about GDPR?

Some courts have stated that an IP address and user name are personal information that are covered by the GDPR regulation. To address customer concerns, Armis can offer the following:

- All customer data can be stored in an AWS EU region of the customer's choice.
- Upon customer request, we can disable the collection of user names and IP addresses on a global basis.
- Upon customer request, we can delete all records that include an individual's IP address and user name

About Armis

Armis is the leading agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company headquartered in Palo Alto, California.