USE CASES FOR RADIATOR

THE MOST FLEXIBLE AAA PLATFORM IN THE WORLD

Radiator

Two-Factor Authentication (2FA)

Securing username password AAA

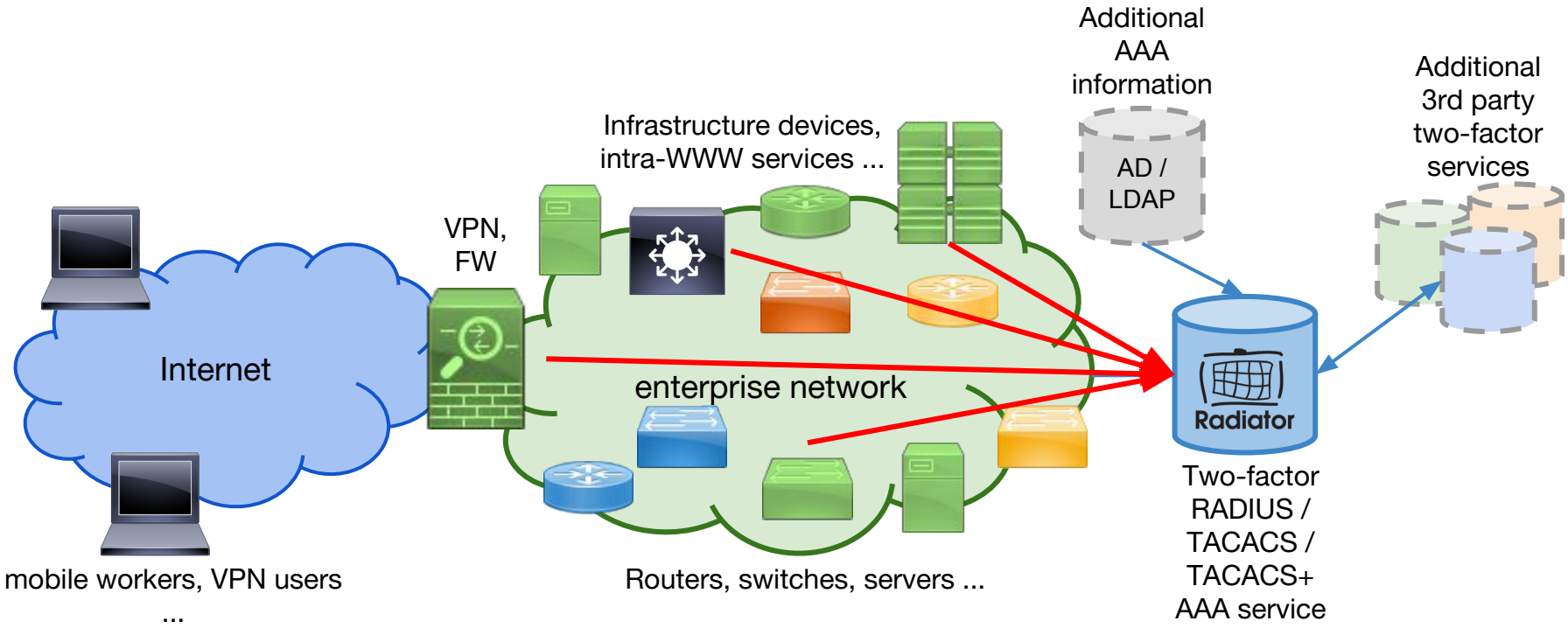
The problem with usernames and passwords

- Common username and password becomes common knowledge as employees/contractors change
- Manually configured user credentials need also manual maintenance
- Most people use really bad passwords and are vulnerable to social hacking

Radiator two-factor advantage

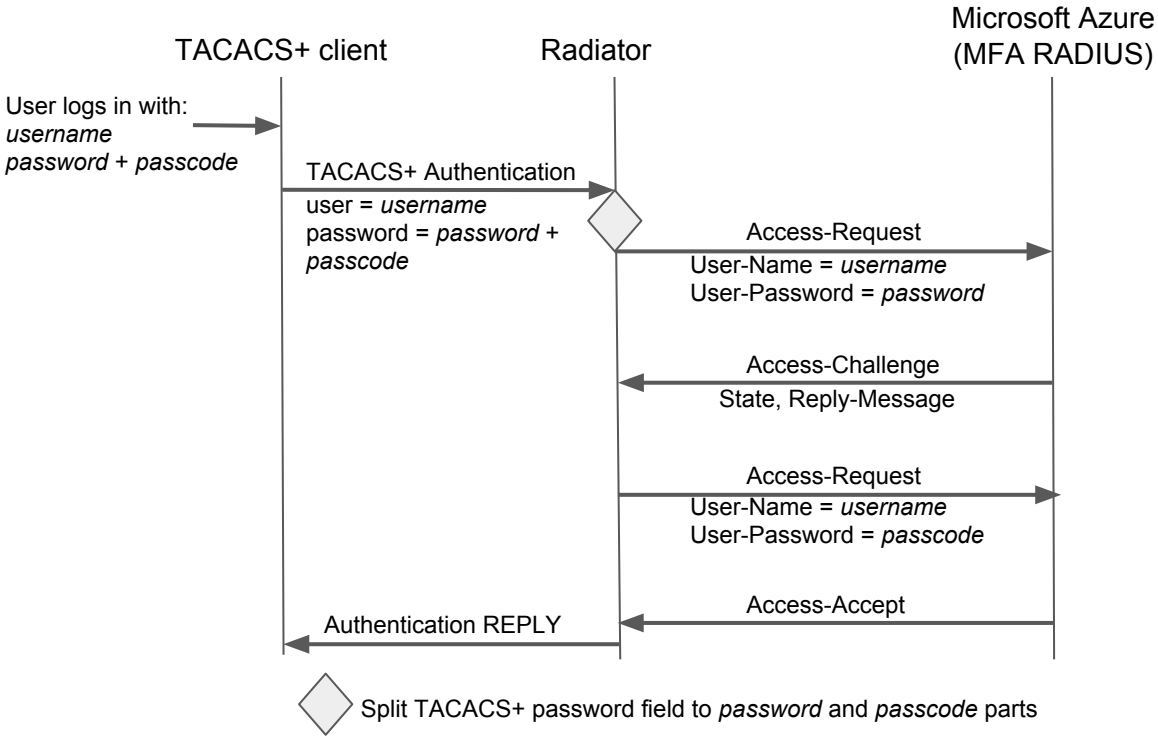
- Support for multiple 2FA standards and solutions
- Works both as the two-factor AAA end point and complementing proxy
- Excellent choice for making authentication and authorisation decisions based on multiple information sources (e.g. LDAP, AD, databases, connection details)

Multiple sources -- one AAA decision



Read more from: http://radiatorcookbook.open.com.au/2016/08/secure-your-network-and-services-with.html

Adding TACACS+ support to Azure MFA



Federated Identity

From eduroam to govroam and commercial Wi-Fi roaming

Connecting organisations is hard

- The diversity of organisations and identity solutions require adaptation and flexibility
- Translation is often required for interoperability and conformance
- End user organisation need for turn-key solution increase requirements for AAA product, licensing and support flexibility

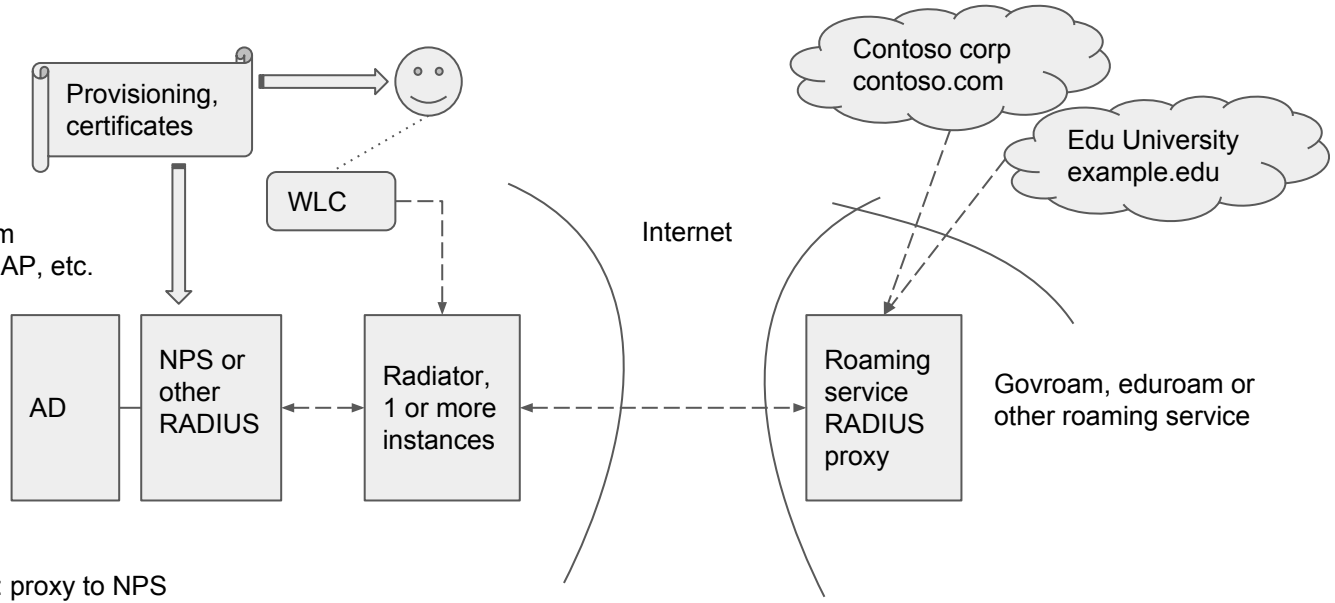
Radiator: been there, done that

- Radiator has the best support for various authentication sources and interfaces
- Radiator is already used on identity (IdP), service (SP) and roaming federation provider level
- Radiator is already used to adapt, translate and complement various other vendor solutions to connect organisations to identity federations
- Field-tested complete configurations for various use cases help create turn-key solutions

Radiator: been there, done that

- Used by several organisations as eduroam top-level, national, regional and local RADIUS servers
- Commercial Wi-Fi operators such as Fon and iPass have been using Radiator since beginning
- Connects organisations to govroam and e.g. to roaming federation for national health organisations

AD + NPS + Radiator proxy



Customer site

- AD domain: ad.example.com
- WLAN username: user@example.com
- Authentication method: EAP-TLS, PEAP, etc.

Radiator does proxying decision:

- Username ends with @example.com: proxy to NPS
- Username ends with @something: proxy to roaming service
- No @ or otherwise invalid username: generate a reject

NPS and Radiator

- NPS only authenticates, it never proxies or handles roaming users
- Radiator only proxies, it takes care of requirements set by the roaming service

Wireless LAN Controller (WLC) and Radiator

- WLC sends all requests to Radiator
- Radiator masks any differences between local and roaming authentication requirements

AD native connection

RADIUS client to server connection

RADIUS client to server and server to client connection

Wi-Fi connection

Onsite IoT and Industrial Internet Security

Securing access to devices even without Internet connectivity

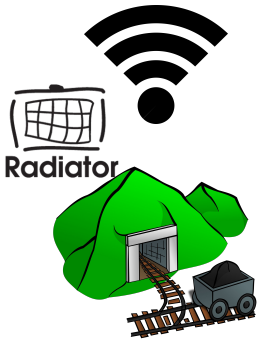
Security must work even without Internet

- IoT and especially Industrial Internet demand reliable, always-on security solutions
- These solutions must work even if the connection to the Internet or cloud is broken
- Onsite security solutions ensure the reliability production facilities and equipment require

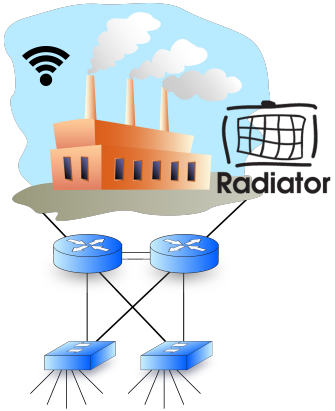
Radiator: on every site

- Radiator has small memory, processor and disk space requirements
- Radiator can be deployed on any embedded, industrial or even mobile platform running Linux, *BSD or Windows
- Flexible Radiator licensing options enable cost-efficient deployment of Radiator on every site
- This way Radiator can provide RADIUS, TACACS+ and multi-factor authentication and authorisation with reasonable costs on any site everywhere

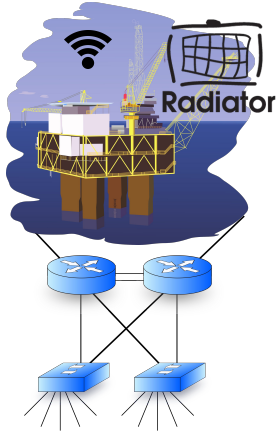
Radiator -- on every site



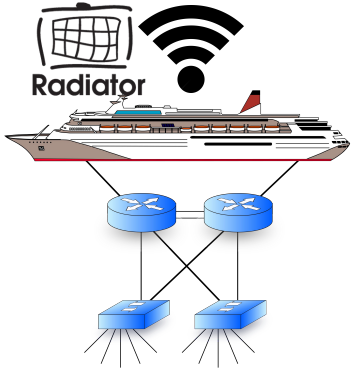
Mine Wi-Fi for autonomous trucks etc.



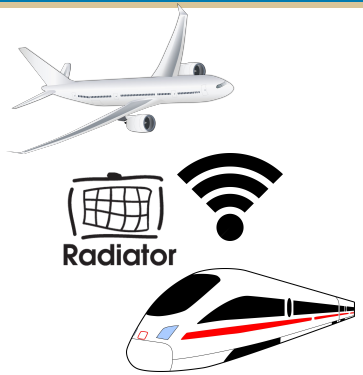
Factory network access control



Oil rig networks, staff Wi-Fi



Ship networks, staff/guest Wi-Fi



Wi-Fi in mobile transports

… two-factor authentication, employee/contractor/etc. authorisation, staff/guest/contractor Wi-Fi separation, network device access control ...

IoT device configuration provisioning and accounting

Extending operator connectivity services

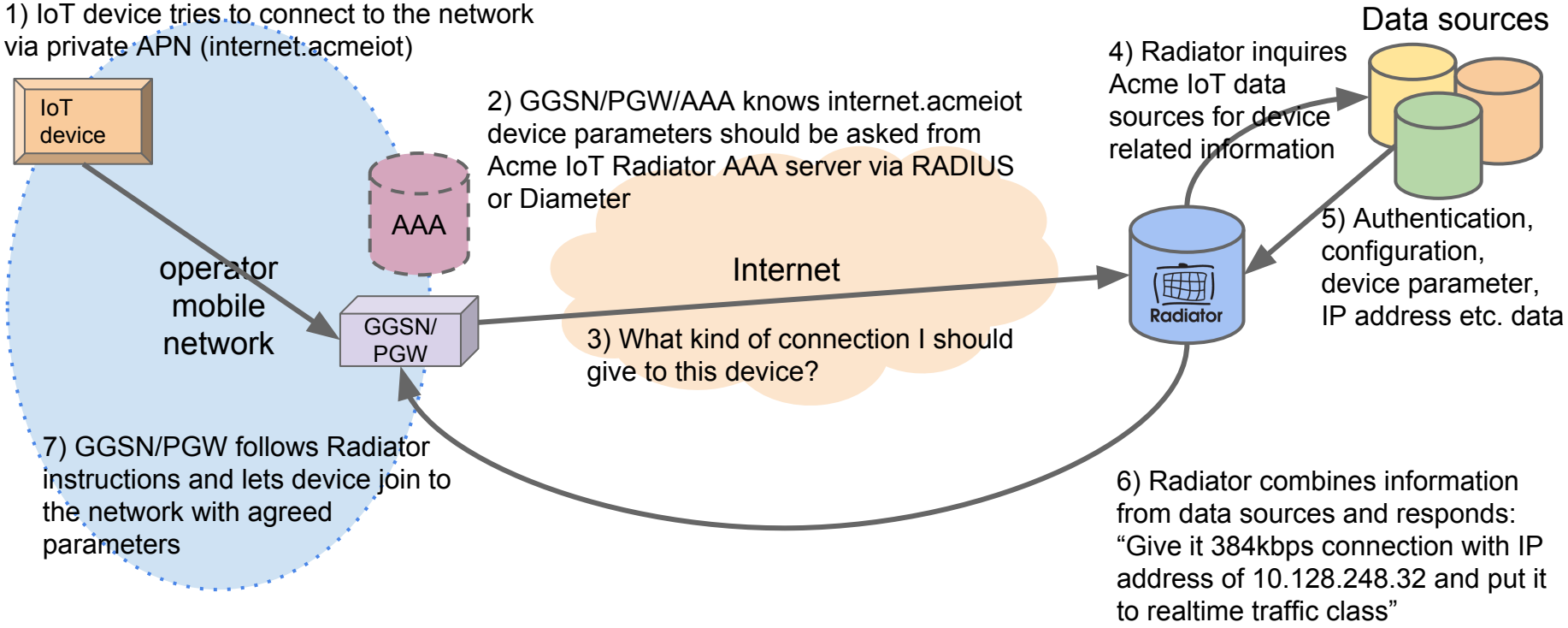
When one size does not fit all

- Operator M2M and IoT services often have limited use cases and flexibility
- Connectivity services (e.g. private APNs) often require customer specific AAA for more advanced or flexible configuration
- Having AAA controlled by you, makes it easier to configure, provision and account all your devices in the field

Radiator fits like a made-to-measure suit

- Radiator has active use cases such as IP address allocation, detecting inactive devices etc.
- The information returned to network devices can be augmented with Radiator with information from your sources
- Radiator configuration, its actions and responses can be tailored according to your needs and use cases instead of static use cases.
- Radiator's licensing enables you to focus on tailoring and not to the stock license costs

Private APN + Radiator example



Detecting anomalies

Collecting data for machine learning

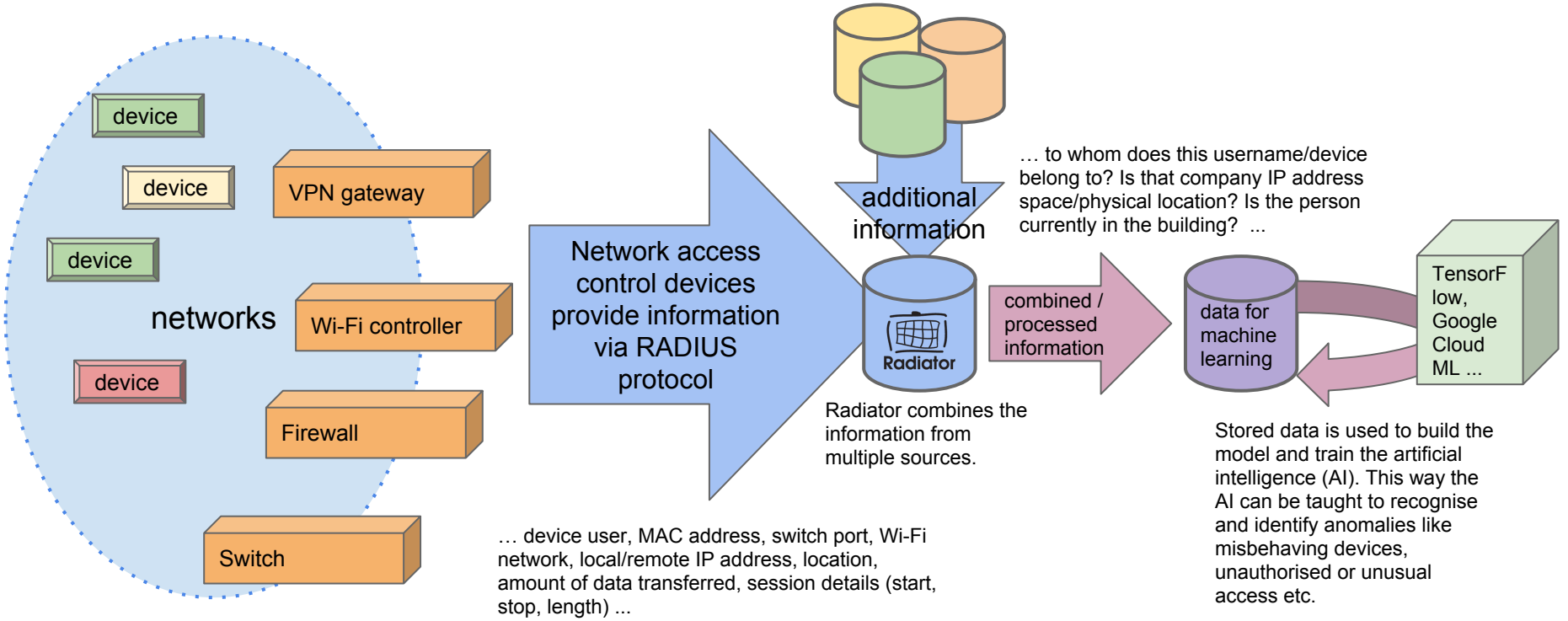
AAA is an excellent source of data

- All network authentication, connection and session details can be stored with proper AAA solution
- AAA can also process, normalise or extend the information from network devices with additional data from other databases
- Flexibility to combine information from multiple sources improves the data quality for machine learning

Radiator is an excellent data processor and AAA

- In addition to regular AAA data sources (RADIUS, Diameter, TACACS+) Radiator has support for multiple database backends.
- Radiator is designed to be extendable and not limited to static use cases.
- Radiator can process, extend, normalise or manipulate AAA information to expand its usability and quality for machine learning
- Machine learning can then be used to detect anomalies such as exceptional traffic, unusual login locations etc.

Network anomaly detection



… device user, MAC address, switch port, Wi-Fi network, local/remote IP address, location, amount of data transferred, session details (start, stop, length) ...

Radiator combines the information from multiple sources.

… to whom does this username/device belong to? Is that company IP address space/physical location? Is the person currently in the building? ...

Stored data is used to build the model and train the artificial intelligence (AI). This way the AI can be taught to recognise and identify anomalies like misbehaving devices, unauthorised or unusual access etc.

For more information...