Gatewatcher AIonIQ

Proof Of Concept -- Technical Requirements
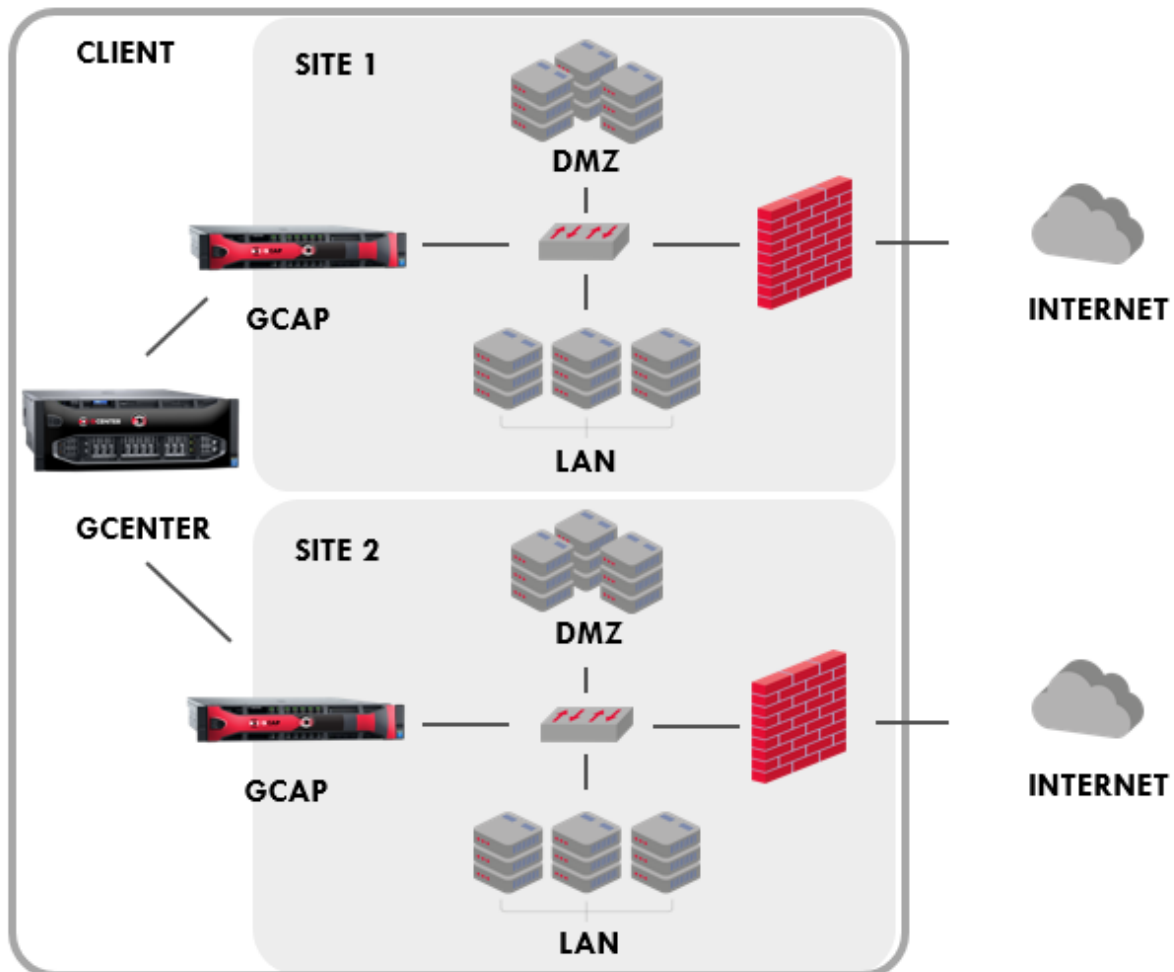
AIONIQ® detection system

Architecture requirements:

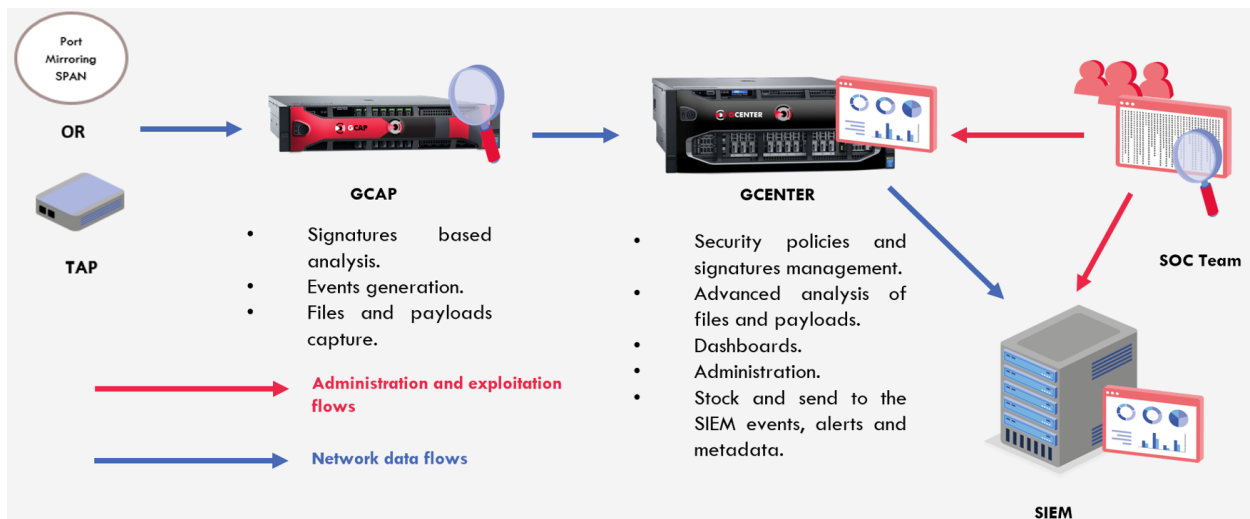**AIONIQ detection solution** is composed of two appliances:

>GCAP (probe)

>GCENTER (management server)

- GCAP receives network flows through TAP or Port Mirror, the entire solution is transparent and passive.
- On premise analysis, none of your data are sent to a cloud.
- Updates are downloaded through repository.

Deployment prerequisites:

The Gatewatcher POC solution is based on 2 Dell R640 appliances server:

A GCAP probe, to be placed close to the flow to be analyzed (Core Switch):

- The GCAP capture interfaces use SFP ports. The following are supported SFP's. However, not all media types may be supported in a PoC due to PoC kit specifications. Please advise of specific requirements prior to PoC.
    - SFP Copper 1G T-base
    - SFP Fiber 1000Base SMF & MMF
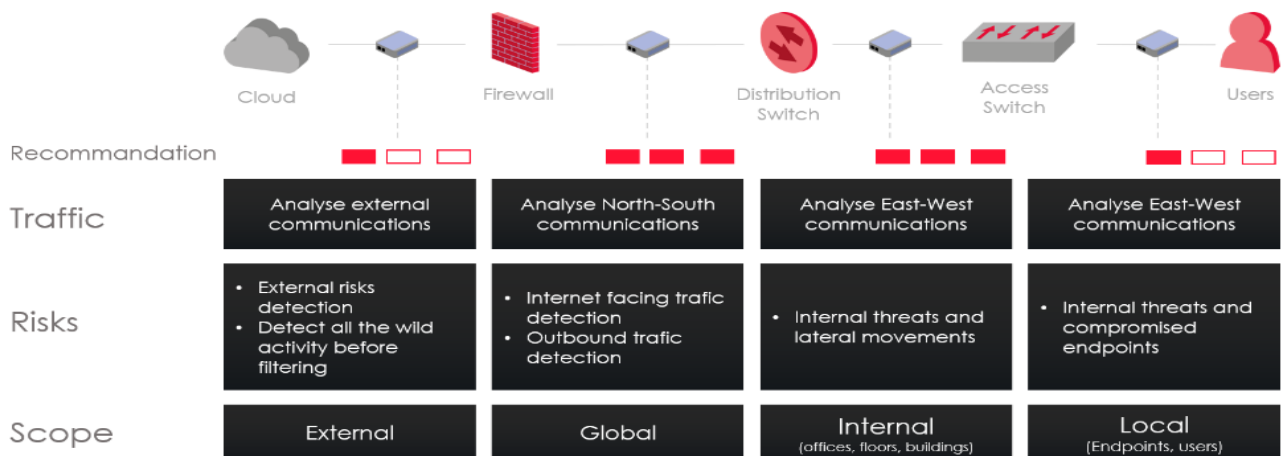   - SFP Fiber 10GBase SR & LX
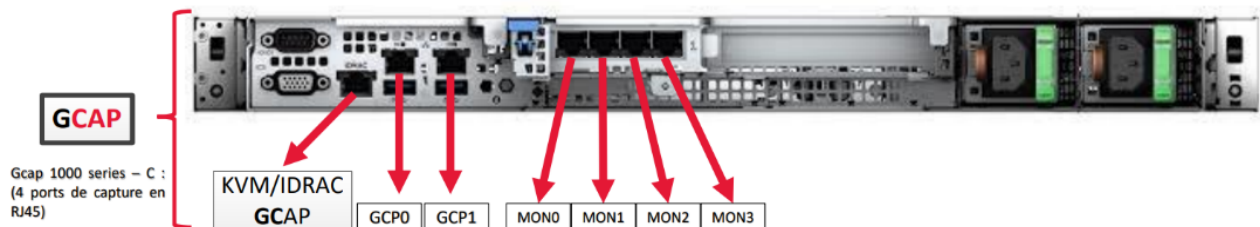
A GCenter manager which can be placed anywhere in your infrastructure.

- Networks ports for management are 1000BaseT:
- Usually installed in the Datacentre
- Remote connection to GUI through https
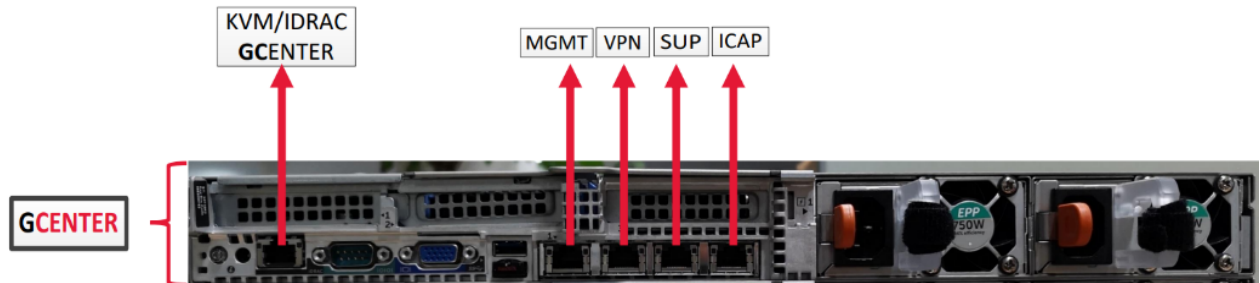
To prepare the POC, could you please consider and provide the following information:

- Equipment Information:
  - Each Dell R640 requires 1U in standard bay (2U Total). Each equipment must be connected to 2 power supplies (4 in total).
  - Each device requires VGA and USB access to be configured to connect the screen and the keyboard. This is just for initial configuration.
  - Required SFP media types.

- Define the type of traffic to analyze:
  - East-West or/and North-South (Depending on the position of the probe in your network)
  - Bandwidth of traffic to monitor.

Standard PoC Architecture

Network Interfaces

IDRAC – Out-of band management interface.
GCP0 – Dedicated VPN interface (IPSEC) for GCAP
GCP1 – Dedicated management interface (SSH) for GCAP
MON_0-3 – Monitoring (Capture) interface for GCAP

MGMT0 – Management interface for GCENTER

VPN0 – Dedicated VPN interface for GCENTER
ICAP0 – Interaction with third party Proxy
SUP0 – Interaction with third-party monitoring solution

Network Flows

MGMT - SSH
MGMT - HTTPS[443] , SSH[22]
IPSEC TUNNEL - UDP[500], UDP[4500], ESP[50]
KVM - HTTPS[443], TCP[5900], TCP[5901]

LUKS key - USB key for GCAP and GCENTER disk encryption.

Network requirements (**Info provided by Customer – Configuration by Gatewatcher on the GCenter and the GCap**):

GCAP INFORMATION	
GCAP Machine Name	
GCAP Domain Name	
GCAP IP Address (GCP0)	
GCAP Network Mask	
GCAP Gateway	
DNS Server 1	
DNS Server 2	
NTP Server 1	
NTP Server 2	
SFP Media type for Monitoring Port	

GCENTER INFORMATION	
GCENTER Machine Name	
GCENTER Domain Name	
GCENTER IP Address (MGMT0)	

GCENTER Network Mask	
Ping godfas	
DNS Server 1	
DNS Server 2	
NTP Server 1	
NTP Server 2	

Bandwidth & IP addresses (numbers can be estimates)	
Approximate number of IP addresses that will be monitored as part of this PoC	
Approximate Bandwidth of traffic monitored as part of PoC	
Total number of IP addresses across the organisation	
Total number of sites to be monitored	

Site Contact Information	
Contact Name	
Contact Email	
Contact Phone	
Delivery address for PoC equipment	

Setup of the servers:

- Customer to provide the Network requirements as above.

Integration of the solution in the customer infrastructure:

- Configuration of your network:
    - Setup port mirroring (SPAN) or provide TAP (**Configuration by Customer on the Core Switch**)
    - Network requirements (**Info provided by Customer – Configuration by Gatewatcher**)

- Installation of the GCap in Datacentre:
    - 1 Port for GCP0 to GCenter (**Configuration by Customer on Switch**)
    - 1 Port to the SPAN port (**Configuration by Customer on Switch**)

- Installation of the GCenter in your infrastructure:
    - 1 Port MGMT0 to GCap (**Configuration by Customer on Switch**)

Once installed within the customer environment:

- Fine tuning of the solution configuration.
- Tracking analysis, detection, and optimization of the configuration.

Following on from the initial configuration a weekly review call will be scheduled for the period of the PoC.