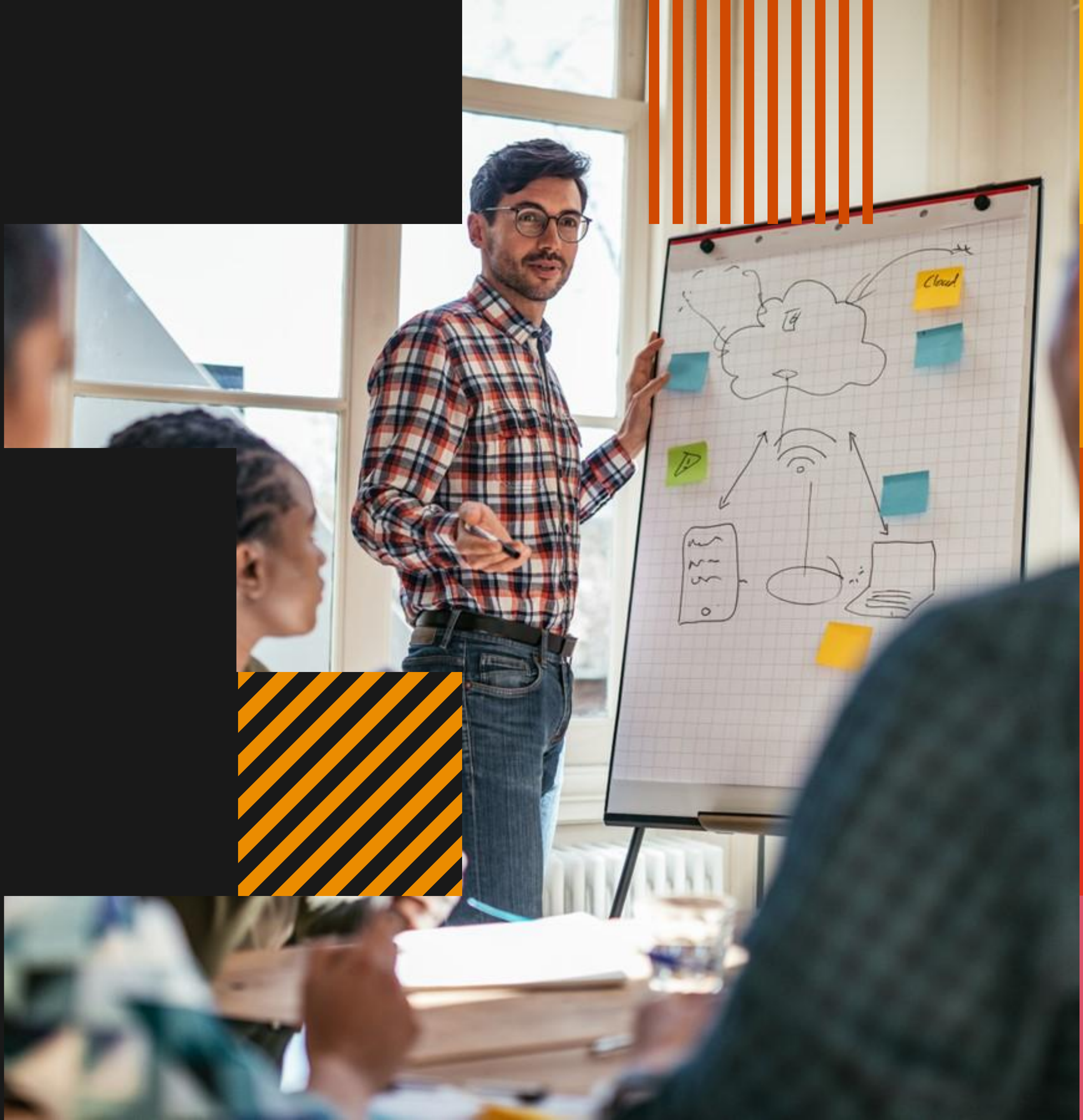
Cloud and data Centre security



Dr. Debabrata Nayak

Nov, 2024

pwc

Potential to Transform Lives of 125 crore+ Cloud and Data Centre

Healthcare

- Remote monitoring
- Telemedicine
- Remote surgery

Education

- Track objects, students, staff
- Instructional design
- AR/VR based lessons

Agriculture

- Monitoring crop yields, rainfall, pesticide, soil, etc.
- Environmental control

Safety

- Women and child safety
- Alarms and surveillance
- Connected cameras

Logistics

- Fleet management and optimization
- Navigation and fuel management

Financial Service

- Remote sales management
- Mobile point of sales

Power & Utilities

- Smart Meter, Smart Grid
- Facilities Management
- Equipment management

Automotive

- Infotainment and positioning services
- In-car emergency systems
- Remote diagnostics

“Cloud/Virtualization Security”

Cloud virtualization technologies such as software-defined networking (SDN) and network functions virtualization (NFV) are thriving in anticipation . The SDN controller updates or modifies flow rules in the data forwarding elements With these technologies, the security challenges have increased

- Most network functions are now implemented as SDN applications and hence solves the problem of vendor lock-in
- It simplifies network management by enabling programmability and logically centralizing the network control planes.

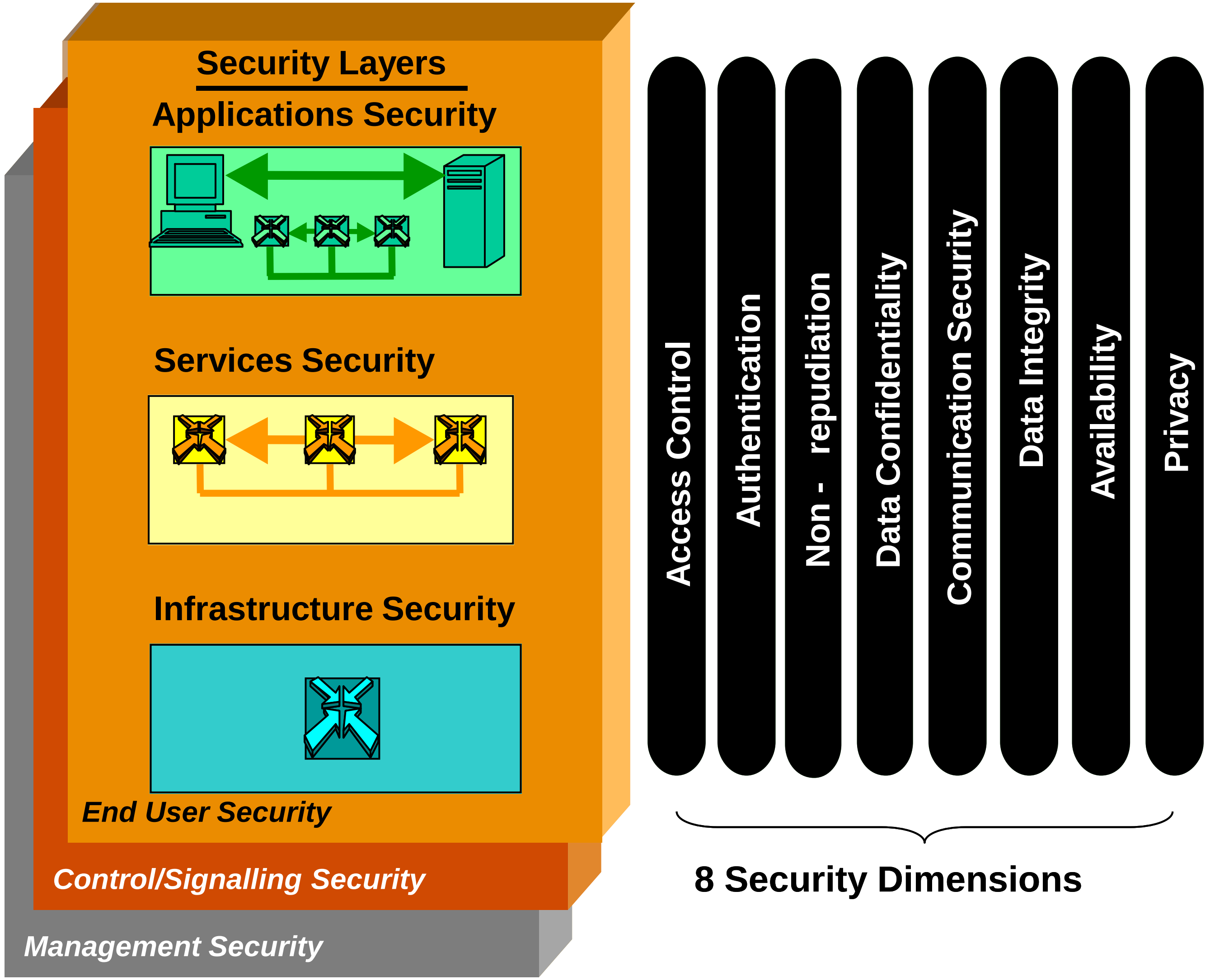
Common Security Challenges:

- Malicious programs applications or exposed critical API can cause several security implications
- As the control is now centralised, the attacker can easily target to compromise control in turn gaining access to entire network control
- Each virtual system running on the same network might have different security requirement
- Compromised hypervisor can cause the whole system failure
- Dynamic nature of VNF lead to misconfiguration errors and tracking and monitoring malicious virtual network would be difficult

Security Recommendations:

- For avoiding malicious applications in SDN/NFV:
  - There should be proper verification process performed on applications to ensure its validity and authenticity
  - Permission based system should be present which allows only the verified applications to access the control plane operations
- For SDN control plane:
  - The mechanism to ensure the verification of the data flow rules so as to avoid the bottleneck of the of the controller
- Hypervisor should be strengthened as it has the central role. To do so it is recommended to have least privilege rule followed
- Security as a service should be implemented which will help in defining the security according to needs
- SLA should include the data storage and protection policy as per legislation requirements
- Secure access layers across the stack of cloud.

SDN Security Framework (X.805): Hierarchical Defense In Depth



1 - Infrastructure Security Layer:

- Fundamental security building blocks of networks element
- E.g.:
  - Secure OS: SELinux, GRSecurity/PAX, DEP, ASLR, NX
  - Trusted computing: secure boot, DIM, RA, TPM, vTPM
  - UTM security zone isolation and WAF/DoS, PacketIn/Out

2 - Services Security Layer:

- Security services provided to system/tenant-users
- E.g.:
  - Single sign on, radius, LDAP, NBI/SBI access control (RBAC and on behalf of security model), policy sandbox, KMC
  - PKI, TLS, WEB Security Framework

3 - Applications Security Layer:

- Security applications provided to end users
- E.g.:
  - SDN and big data based Anti-DDoS
  - Service Function Chain
  - Security eco-system based on SFC

Major Changes of Security Context In NFV

Sharing resource using virtualization technology

- Different virtual machines and tenants **share** the physical resource
- Isolation **boundary** reduced from physical to logical using virtualization technology
- The new introduced **virtualization** layer itself is an attack point
- **Hypervisor**, as super administrator, should be protected against abuse

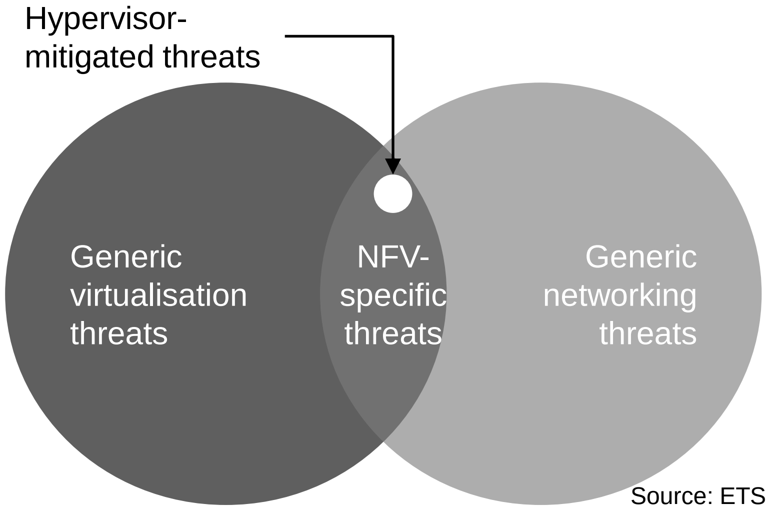
Multi-integration

- **Security responsibility** is divided between all the partners
- More complex identity and access **management**

Dynamic management and orchestration

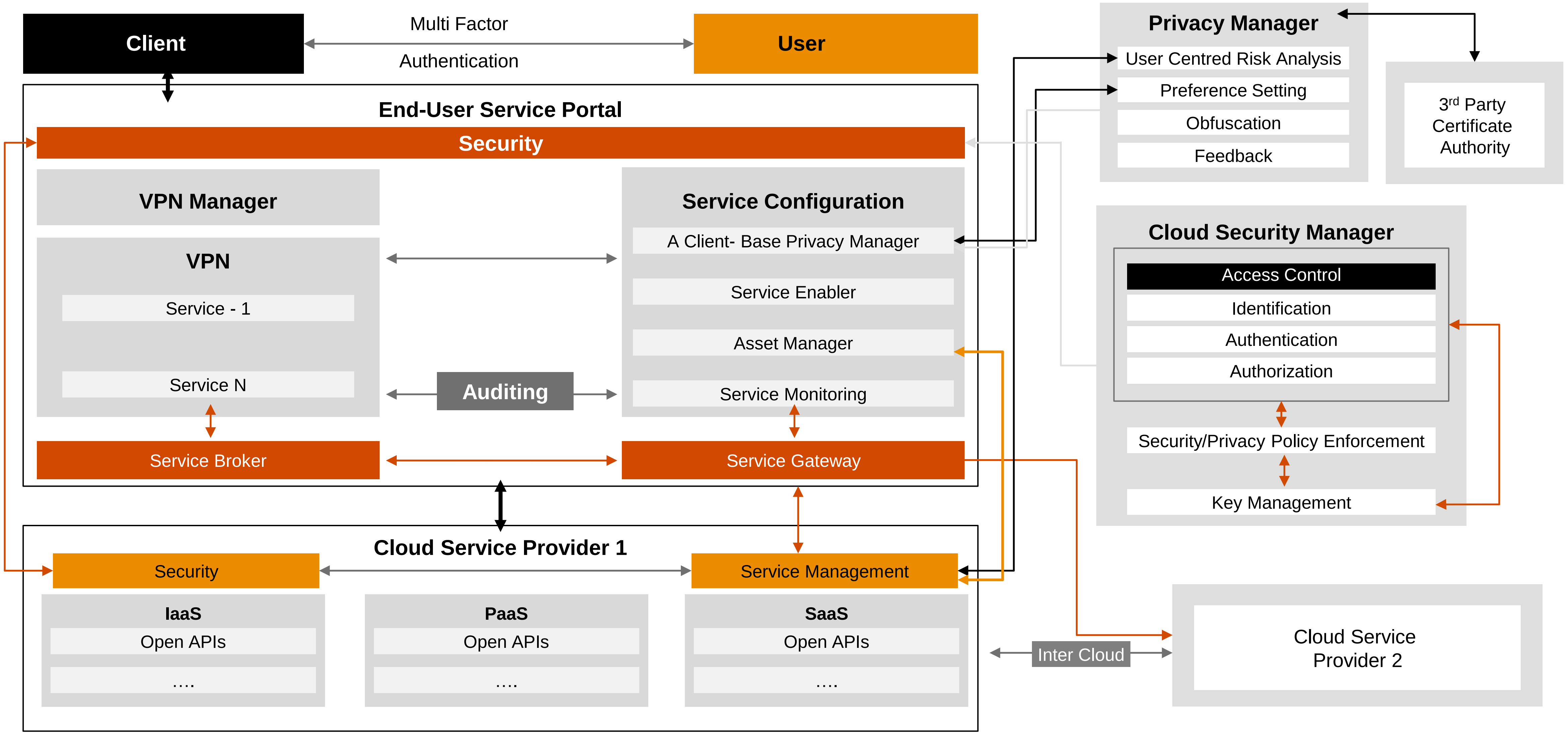
- **New** management and orchestration elements and interfaces are introduced
- VNF is managed and orchestrated **dynamically**

- **Virtualization Platform Security**
- **Virtual Network Security**
- **Data Security**
- **Management Security**


Hypervisor-mitigated threats
Generic virtualisation threats
NFV-specific threats
Generic networking threats

Source: ETSI NFV SEC

Cloud Security Framework



Focus on cloud security technologies, key features to support large-scale cloud and its distributed & flexible deployment in Data Centre.

Cloudization of network security technologies

value:

Solve the problems such as performance bottlenecks, can not scale –in/scale-out flexible, complicated policy management.

Key Technologies:

Software NAT / cluster management / iunified management policy of iptable./Anti-DDos

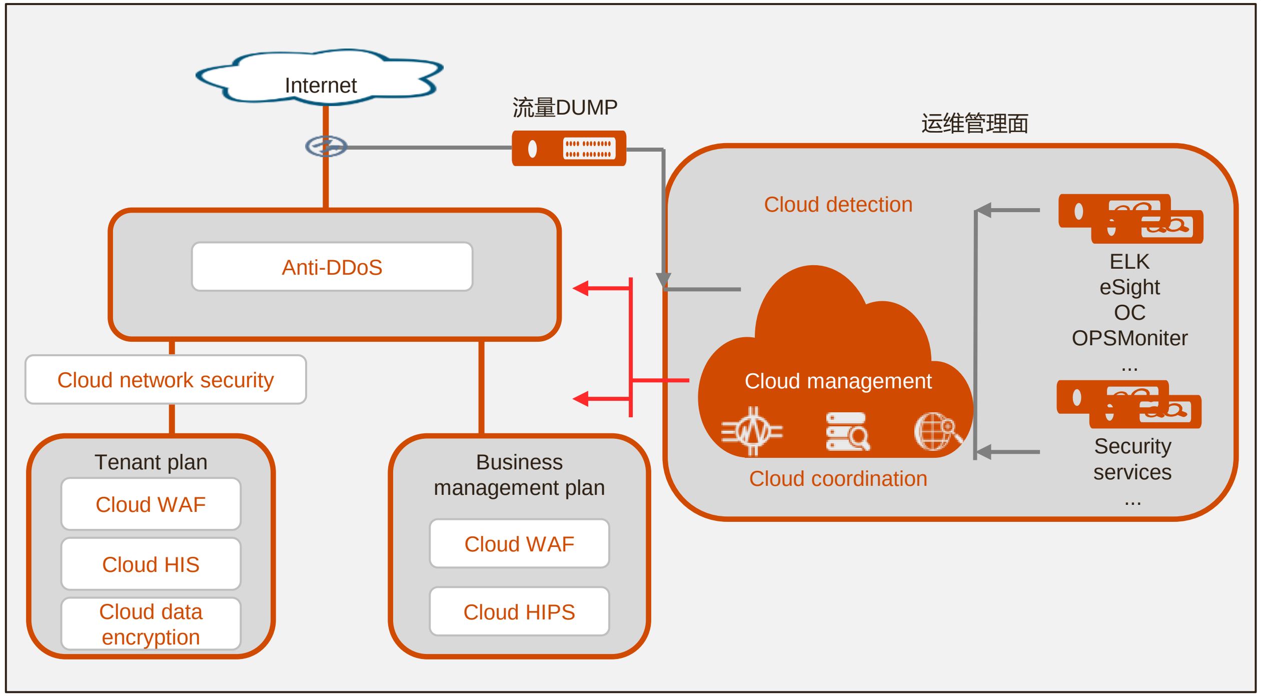
Cloud HIPS

value:

To resolve the problems of cloud host such by external intrusion, internal management, routine inspection

Key Technologies:

Whitelist / Intrusion Detection / Security Patrol / Privilege Escalation Detection



Cloud WAF

value:

To solve the traditional WAF problem, such as can not stretch, performance bottlenecks, high cost

Key Technologies:

Web Intrusion Prevention / Web Malicious Code Protection / Web Application Delivery / Web Unauthorized Protection

Cloud data encryption

value:

Address the need for reuse of encryption machine in multi-tenant scenario.

Solve the high cost of the encryption machine,

Key Technologies:

HSM Virtualization Technology / Software Key management Technology

Cloud thread detection

value:

To solve the inefficiency of detection of traditional security equipment;;

Rapid response to emergence;. Baselines the attack and defense experience;. Second-level discovery, minute-level decision-making;

Key Technologies:

Flow DUMP High Performance Probes / Detection Algorithm

Cloud coordination

value:

Quickly resolve threats in a clouded environment, quickly isolate them, and take effective in minutes

Key Technologies:

Analysis model / decision-making algorithm

Cloud management

value:

access, authentication, audit, analysis, decision-making, tools, management can be done in a unified way in cloud-based environment,

Cooperation & Ecosystem

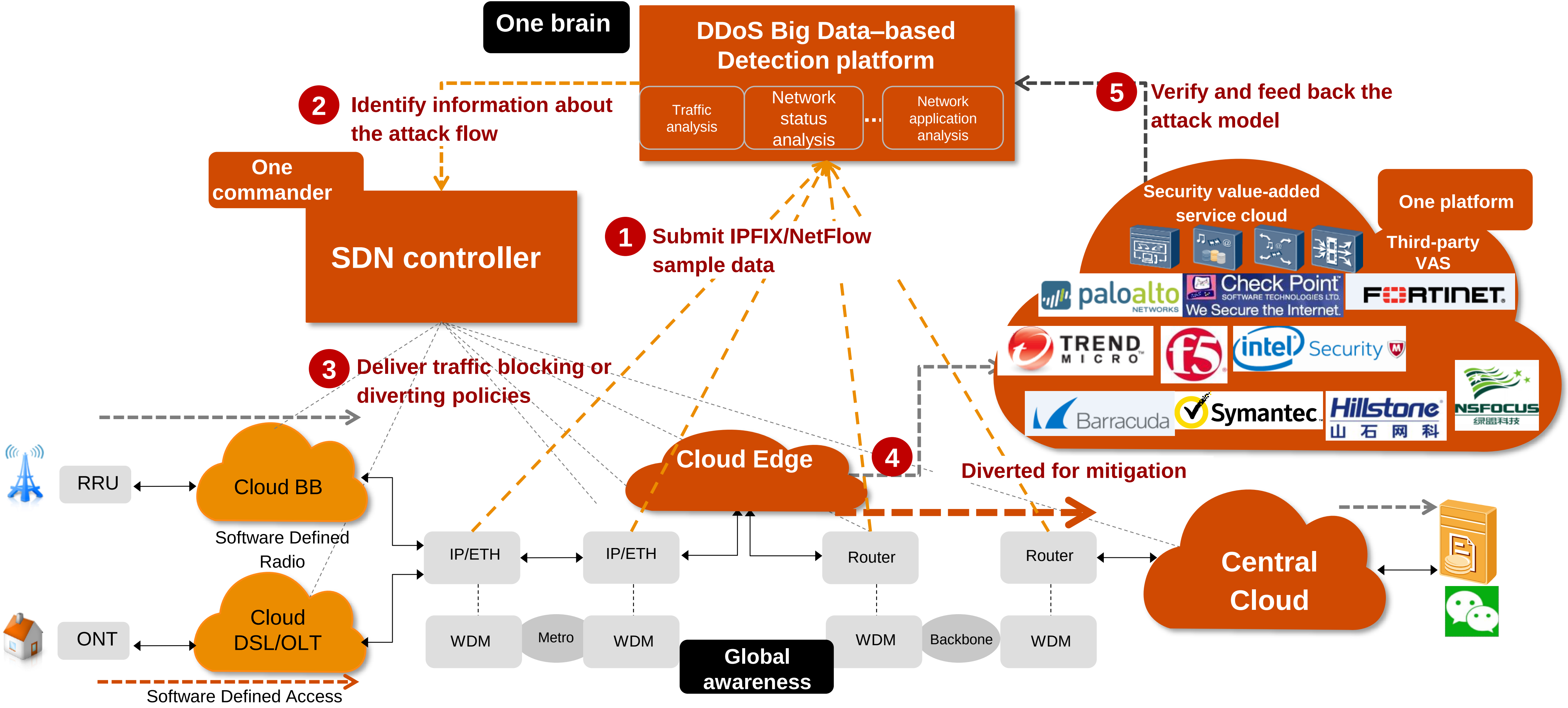
value：

Dynamic application market place allows choice of best-of-breed

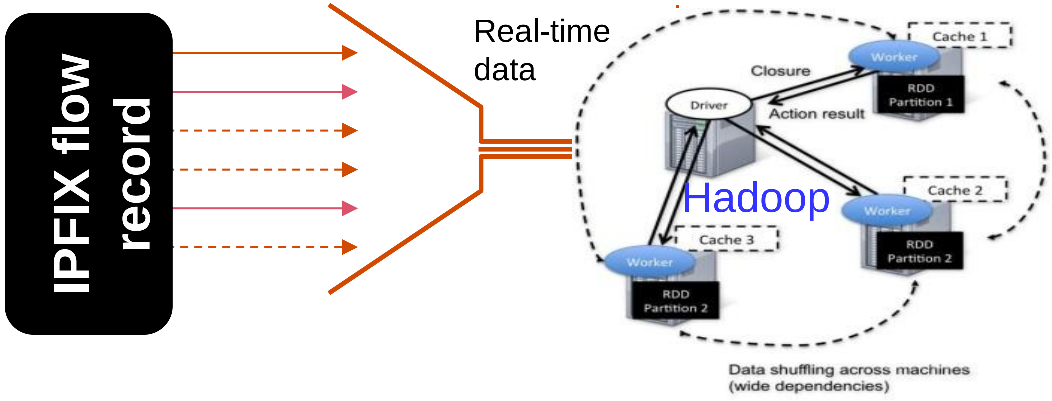
App market place recommendation

Cooperate with foreign manufacturers , tailor to market.

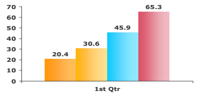
Security Collection, Intelligent Analysis, Near-Source Scrubbing, and Flexible Connection in Data Centre.



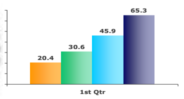
Intelligent Detection and Quick Source Tracing in Bulky Stream Data in Data Centre



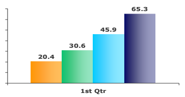
Top 1000 IP addresses



Top 100 services

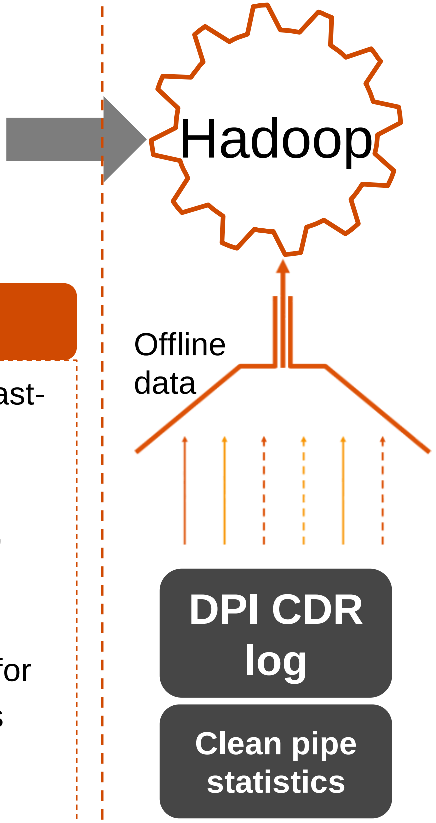


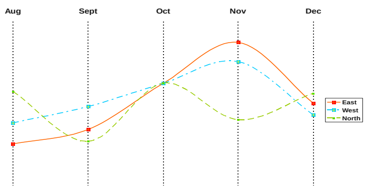
Top 500 servers



Key technology: high-performance parallel computing

$$Y_{n,m} - Y_{n-1,m} = Z_{n,m} - \min\left\{0, S_{n,m} - \min_{1\le k\le n-1} S_{k,m}\right\} = \max\left\{Z_{n,m}, Z_{n,m} - S_{n,m} + \min_{1\le k\le n-1} S_{k,m}\right\}$$
$$= \max\left\{Z_{n,m}, \min_{1\le k\le n-1} S_{k,m} - S_{n-1,m}\right\} = \max\{0, -Y_{n-1,m}\}.$$





Pre-processing of IPFIX flow records

- IPFIX template management
- Merger of sample flow data
- Application-layer data management through DPI
- Data enrichment for storage

Anomaly information collecting

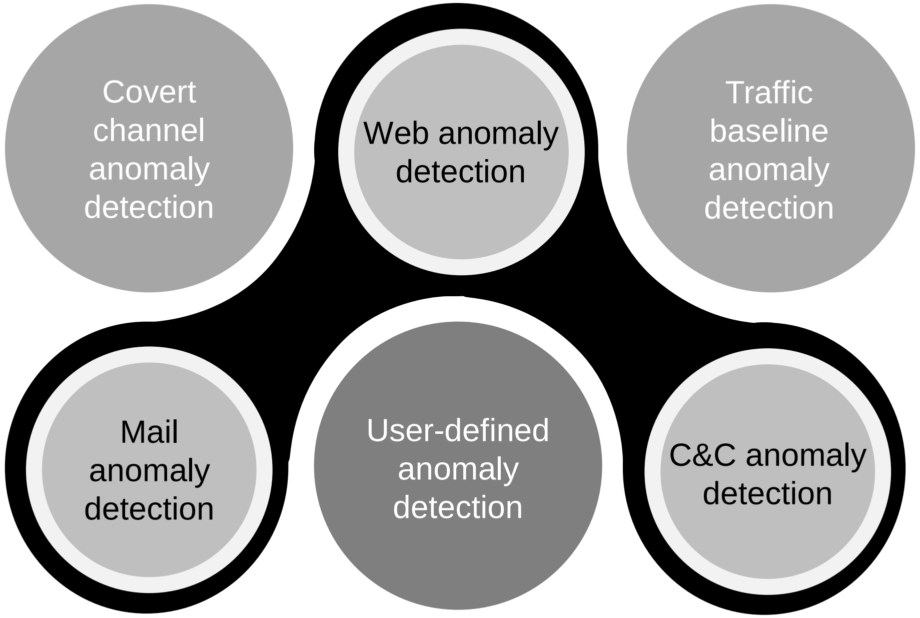
- Identification of elephant flows and fast-changing flows based on specific algorithms
- Statistics of the concurrent sessions, time latency, rate of successful connection, and abnormal sessions
- Statistics of top source destinations for each indicator and business analysis

Attack detection and defense

- Spectrum analysis based on specific algorithms
- Top data polynomial interpolation fit
- Identification of the source and agent of the attack, the service under attack, victim hosts, and zombie hosts
- Automatic generation of attack suppression policies

Security Analysis and Threat Detection on the AI Platform in Data Centre

Anomaly detection based on behaviour and content



Covert channel anomaly detection

Web anomaly detection

Traffic baseline anomaly detection

Mail anomaly detection

User-defined anomaly detection

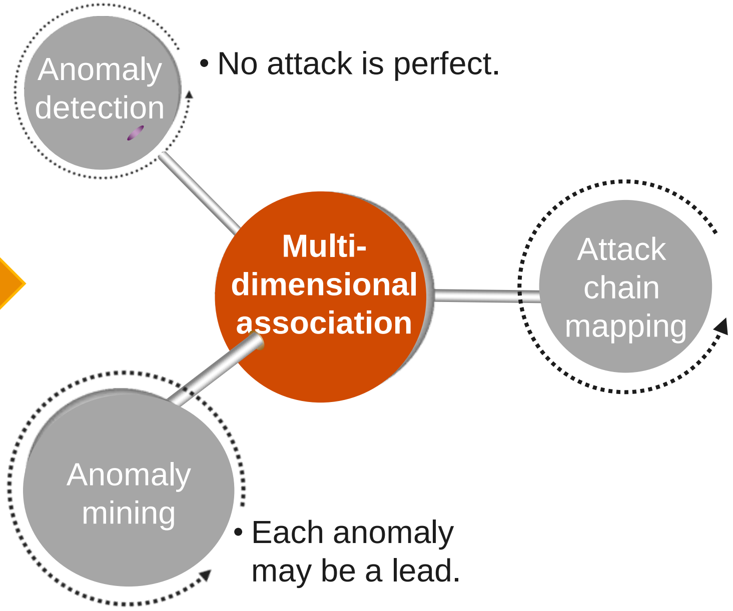
C&C anomaly detection

Number of abnormal behaviours that can be detected: higher

Latency of intelligent search: shortest

Early warning: fastest

Anomaly correlation based on attack chains



Anomaly detection

Multi-dimensional association

Attack chain mapping

Anomaly mining

- No attack is perfect.

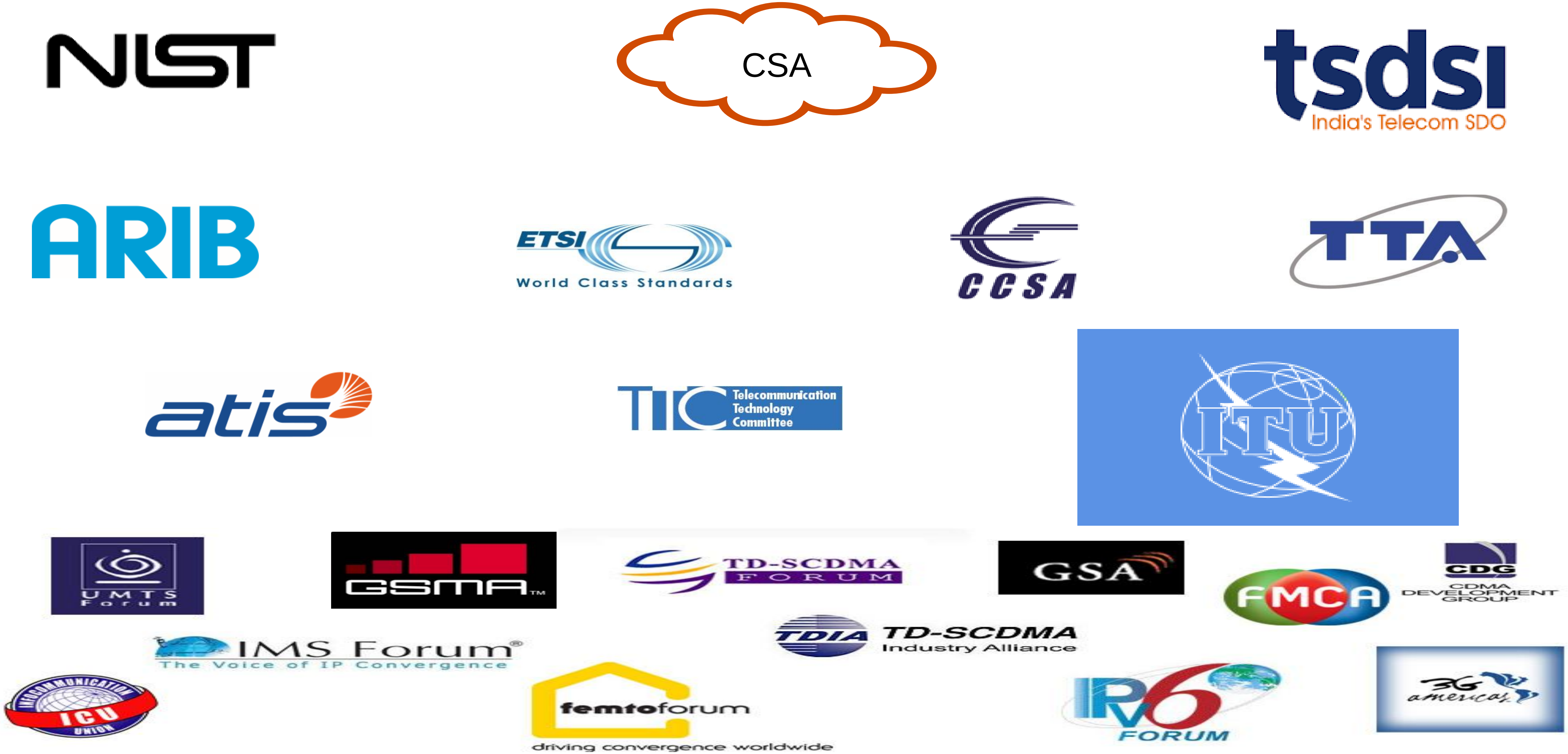
- Associate anomalies based on the attack chain.

- Each anomaly may be a lead.

Industry	170+
Industry	< 10s
Industry	Monthly/ Yearly

Elastic scale-out of hundreds of devices is supported. AI–based analytics helps carriers and enterprise customers realize security posture awareness and implement optimal security defense policies.

Standard Bodies Referenced/followed



Thank you

Data Classification:

All images in this presentation are protected by copyright, trademark, patent, trade secret and other intellectual property laws and treaties. Any unauthorised use of these images may violate such laws and shall be punishable under appropriate laws. Our sharing of this presentation along with such protected images with you does not authorise you to copy, republish, frame, link to, download, transmit, modify, adapt, create derivative works based on, rent, lease, loan, sell, assign, distribute, display, perform, license, sub-license or reverse engineer the images. In addition, you should desist from employing any data mining, robots or similar data and/or image gathering and extraction methods in connection with the presentation.

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.