



Virtual Resource Isolation for Applications in 5G network

Jing Ping
Nokia

Background

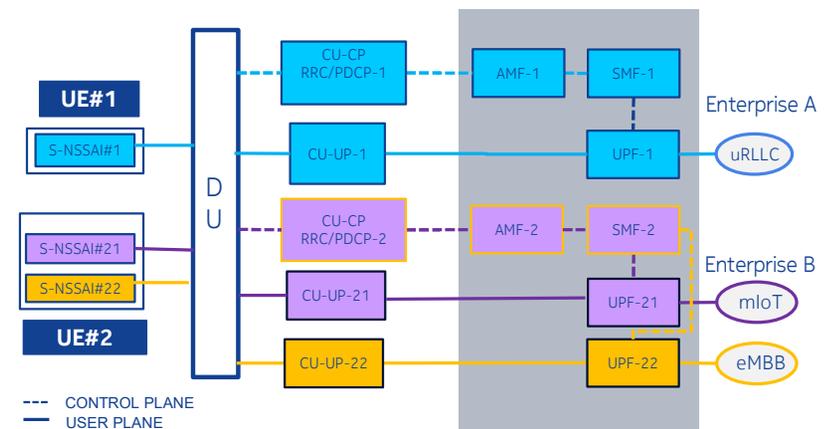


- 5G will be able to support extreme and diverse requirements for throughput, latency, availability, capacity. Security is another fundamental network requirement that needs to be optimized for each specific use case, especially for those uses cases where security becomes critical (e.g., V2X platooning, enterprise VPN or Electric grids).
- Operator allocates 5G network resources to vertical/enterprise customers to support various use cases and applications, the resource can be isolated from networks or network resources used by other cellular customers.
- Network slicing is a key feature and business driver for 5G, which enables enterprises and operators to address specific requirements of different market segments (e.g., industrial, smart cities, healthcare, automotive). The overall security architecture of 5G network is enhanced with new security features, available as well in network slices as logical networks created within the 5G network.



Motivation – business requirements

- A business wants to have a secure and isolated set of network capabilities that meets its communication needs, without having to purchase and maintain the network infrastructure. In this case, a mobile network operator can use network slicing as a means to provide a virtual private network, or private slice, for the enterprise.
- Isolation is a multi-faceted problem, on security dimensions, it's ensuring that any type of intentional attack occurring in one collection of network functions /resources have no impact on any other network functions/resources;
- Slice security isolation is a security feature, as it separates slice related data and activities of different customers. With the corresponding slice specific enforcements slice security isolation can prevent unauthorized access and modification to data, processes, services or functions.

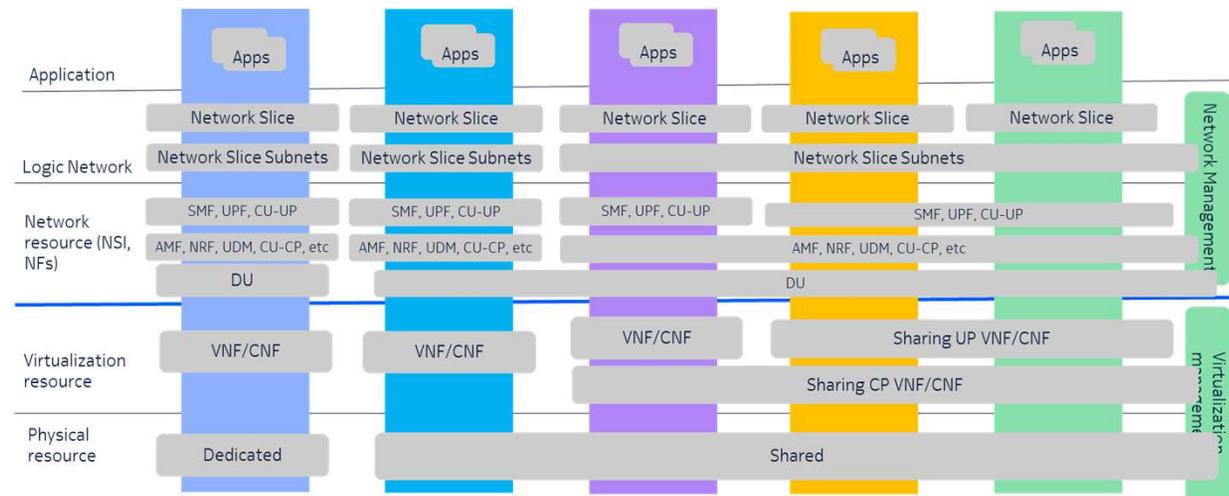


Virtual resource isolating expectation for applications in 5G network - horizontal



Motivation – operation requirements

- Operator allocates 5G network resources to vertical/enterprise customers to support various use cases and applications, the resource can be isolated from networks or network resources used by other cellular customers.
- The network resources are isolated from logic network layer (e.g. network slice), a set of NFs/resource layer (e.g. network slice subnet, or network slice instance), virtualization layer (e.g. VNF, CNF), physical layer (e.g. physical server, RF)



Virtual resource isolating expectation for applications in 5G network - vertical



Threat analysis

Threat modeling:

Refer to MITRE ATT&CK, e.g. MITRE FiGHT

Threat agent:

Advanced threat, e.g. organized crime

Motivation:

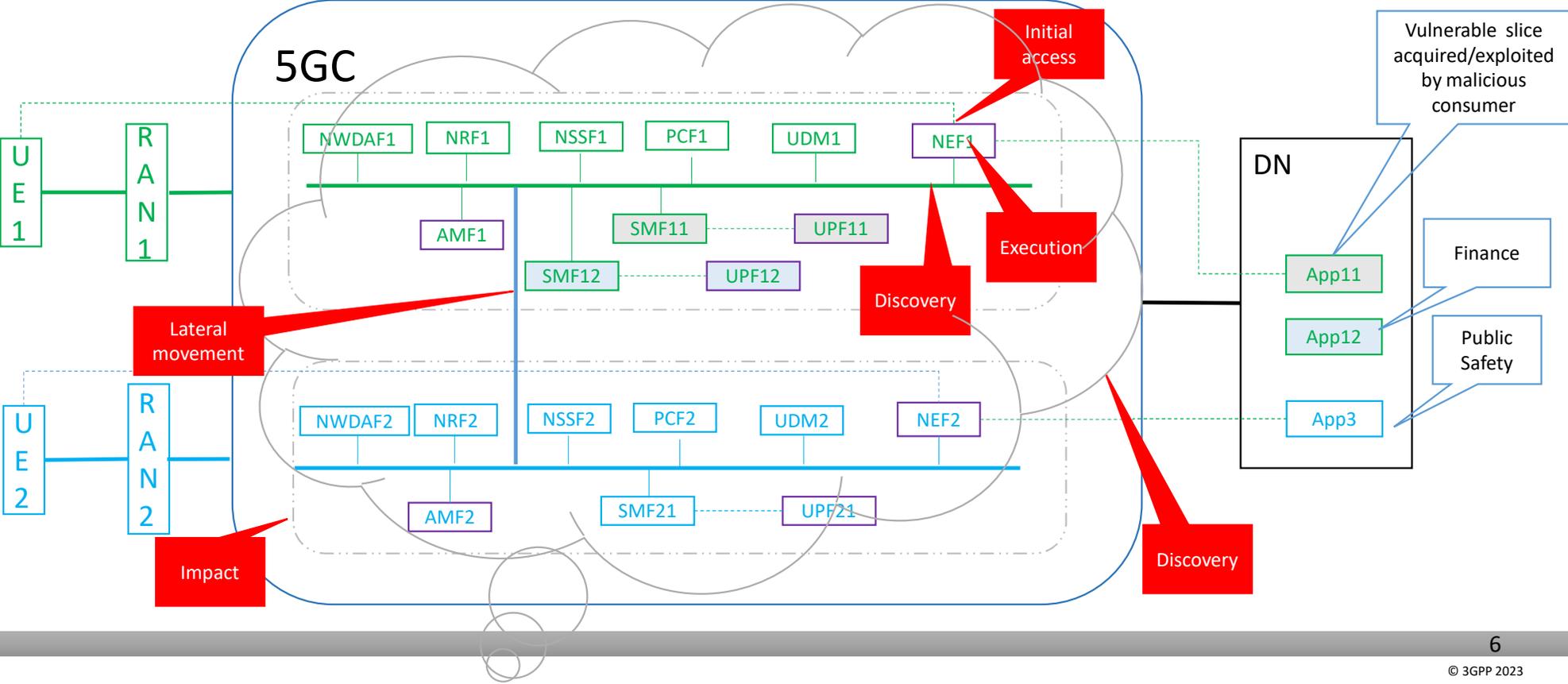
Steal information of sensitive/critical slice and/or deny the service of the slice

Possible Attack Scenario:

Threat agent launches DoS from around the globe with grey-zone access to interconnecting networks to hijack a slice, and impact another slice.

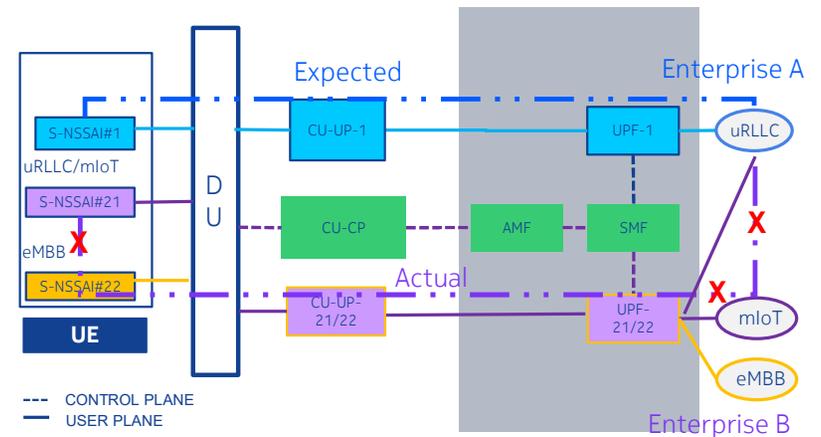


Potential attack scenario



Motivation – gaps and problems

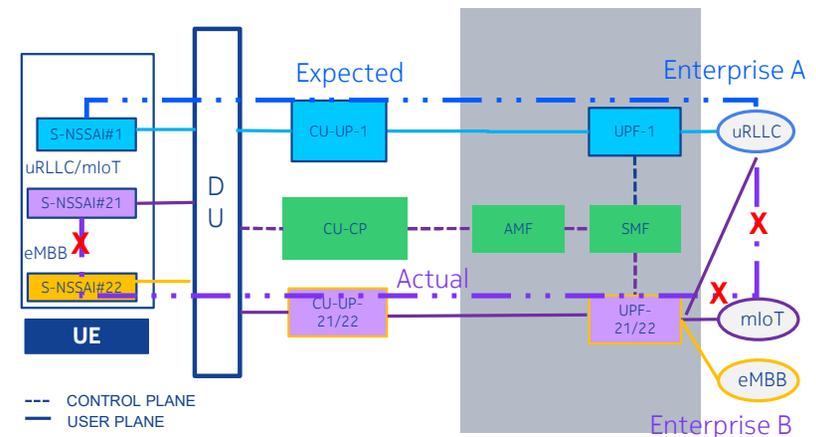
- A UE may select an unexpected logical/virtual network for an application based on local configuration, or outdated URSP, that causes the isolation requirements of vertical cannot be satisfied even network and resource isolation are implemented in 5G network side
- Compromised or malicious UE may misuse slice and intentionally steer security sensitive application to “lower secured” slice hence steal application data, or steer low security and priority application to high priority slice, and may cause DoS on the target slice.



Issue #1: Unexpected logical network is selected for a vertical application

Motivation – gaps and problems

- As shown in the right figure, the operator allocates logical/virtual network (e.g. identified by S-NSSAI#1) to Enterprise A for its uRLLC service and allocate logical network S-NSSAI#21 and 22 to Enterprise B for its mIoT and eMBB services. According to customer security requirement and operator policies, operator isolated resource of S-NSSAI#1 from resource of S-NSSAI#21/22. The operator and Enterprise A expected application traffic for the uRLLC service will route to dedicate resource for S-NSSAI#1.
- However, as mis-behavior of the UE, logical network S-NSSAI#21 may be selected to transmit traffic of the uRLLC service, and the application data maybe leaked to NFs (e.g. CU-UP, UPF, etc.) of other resource group, which may even be outside the campus of the Enterprise A. That may violate security and other SLA of Enterprise A, operator policies and regulation. If S-NSSAI#21 support only DNN for enterprise B, the uRLLC traffic from UE even cannot reach the uRLLC server, and DoS may be triggered.

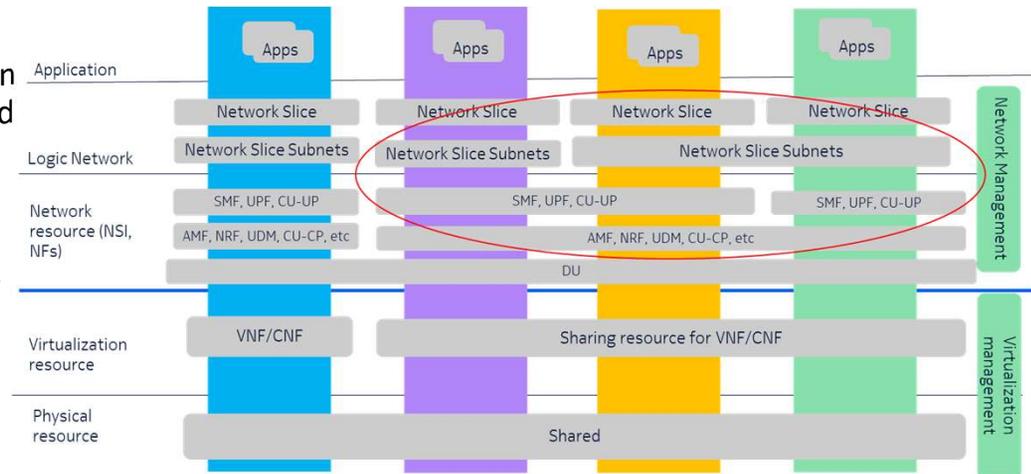


Issue #1 example: Unexpected logical network is selected for a vertical application



Motivation – gaps and problems

- As shown in right figure, operator may allocate virtual network and network resource to specific vertical applications with using network slicing, and expect the resources are isolated for application based on corresponding policies and existing isolation solutions in network, e.g. slice aware access control for SBI based 5GC, select right CP or UP NFs considering S-NSSAIs, etc.
- However, as lack of coordination between management and network layers, the isolation policies may not be correctly provisioned on NFs, so all isolation solution in control plane may not take effective. E.g. management plane expects isolate resources of apps in purple from apps in yellow and green, but incorrectly configured NSI and S-NSSAI in NFs as lack of standardized information model, which cause the NFs in yellow can access NF Services of NFs in purple.
- Without appreciated isolation, a compromised or malicious low security profiled slice may impact a highly sensitive slice, e.g. steal services/resources and data of mission critical applications.

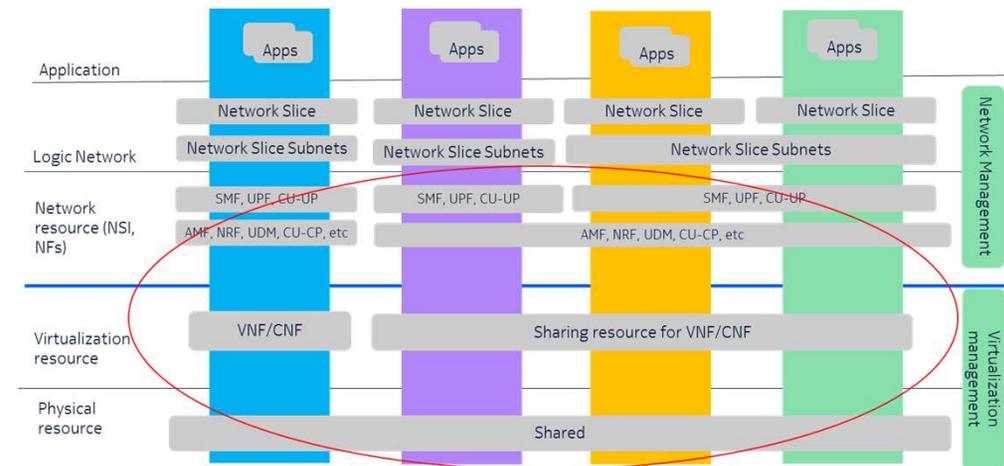


Issue #2: Unexpected isolation in network resource layer



Motivation – gaps and problems

- SBI and virtualization technologies are applied in 5GC network, all NFs in the core network (e.g. (AMFs, SMFs, UPFs, etc.) may share common infrastructure and deployed as VM or container.
- As shown in right figure, operator may allocate virtual network and network resource to specific vertical applications with using network slicing, and expect the resources are isolated for application based on corresponding policies and existing isolation solutions in network. However, as lack of coordination between 3GPP system and cloud/virtualization system, the VNF/CNF serving different application may not be correctly isolated in virtualization and physical layers. It's even worse for partially sharing/isolating resources case (e.g. sharing some NFs but isolated others), and MEC scenario where operator's NF may deploy with applications of verticals.
- Without proper isolation and security control in cloudified environment, sensitive data of one network slice could be exposed to network functions running in other network slices through side channel attacks, although the access control is correctly performed on SBI based 5GC network.

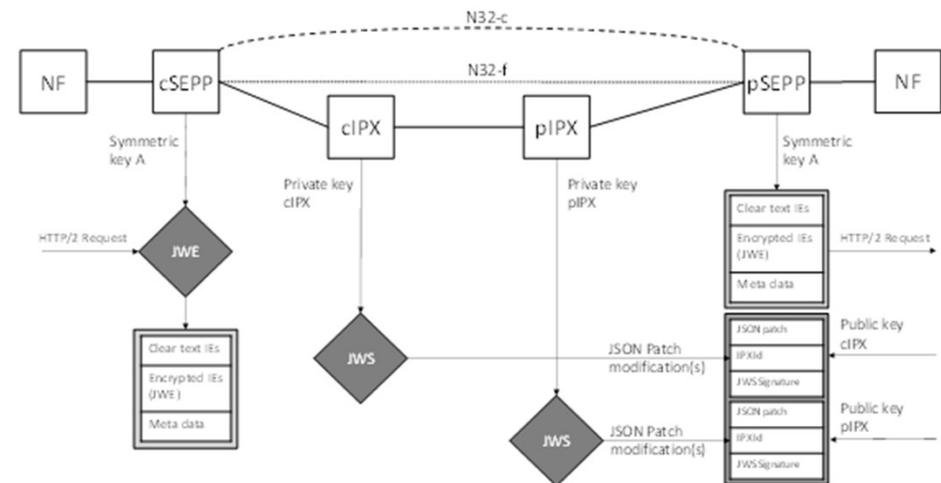


Issue #3: Unexpected isolation in virtualization resource layer

Motivation – gaps and problems

As defined in TS 33501, two PLMNs can decide either to use PRINS or TLS between them. It is based on the operator policy. If we use the PRINS protocol, then IPXs can modify the data or can read the data between the PLMN. If we use TLS between the SEPPs, then IPXs can not read the data. Currently N32 traffic is not segregated per slice. Therefore, if a specific slice does not want IPX to modify or read the data, then it is not possible because N32 connections are not slice-specific.

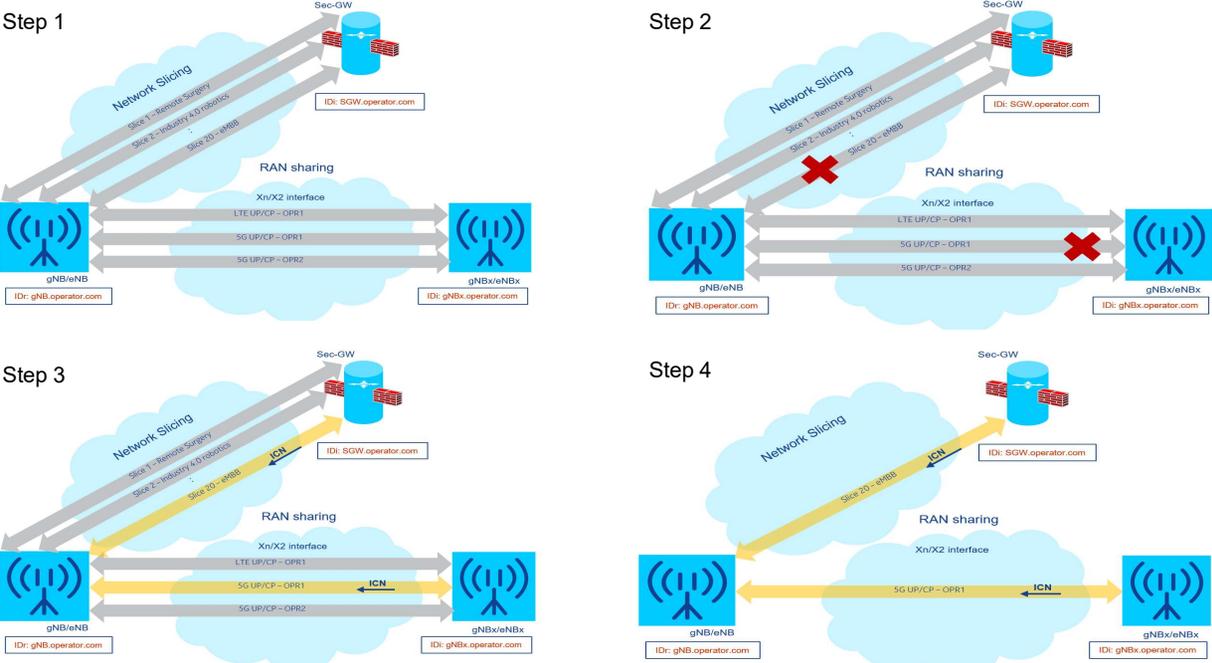
This limitation leads to a problem where if a business demands that Slice-X data should not be read by IPXs, then whole N32 traffic needs to be diverted over an TLS then IPX lose the visibility and business use case on the non slice specific data



Issue #4: Unexpected isolation at N32 interface



Motivation – gaps and problems



Issue #5: Unexpected interference at transport layer

Objectives



Study how to enable verticals, operators and cloud service providers to address diverse requirements of different market segments for security and isolation, and to holistically investigate the gaps in existing specification and collect potential solutions to enforce resource isolation for applications in 5G network.

- 1) Clarify resource isolation concept especially in security point of view.
- 2) Investigate the gaps of existing specification on correctly logical network selection for vertical applications.
- 3) Investigate the gaps of existing specification on network and virtualization resource isolation and protection for vertical applications.
- 4) Investigate the gaps of existing specification on transport (e.g. N32, N3 interfaces) isolation and protection for vertical applications.
- 5) Collect potential solutions to fulfil differentiated security SLA of enterprise applications and enforce resource isolation for applications in 5G network, hence satisfy the security requirements of various business cases from different industries and improve compliance with industry regulatory and business requirements.