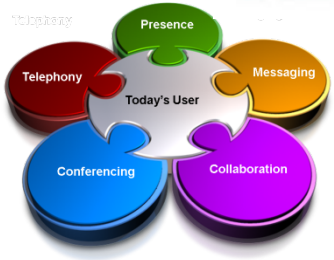
Real Time Communications
Sicurezza Informatica e Compliance

Una piattaforma di sicurezza informatica conforme ai requisiti normativi (GDPR/ENISA),

sviluppata per rispondere alla evoluzione del contesto delle comunicazioni e delle tecnologie verso modelli aperti ed interconnessi

UM Labs Unicus SIP security service

Evoluzione del contesto



- ✓ Comunicazioni VOIP e servizi cloud
- ✓ Unified communication (Voce, Video, Messaggistica, Presenza)
- ✓ Servizi UC erogati da player OTT
- ✓ Costo, flessibilità, utenti remoti ed in roaming, accesso ovunque e per tutti
- ✓ Integrazione di soluzioni multivendor
- ✓ Come garantire la sicurezza in un mondo aperto e interconnesso

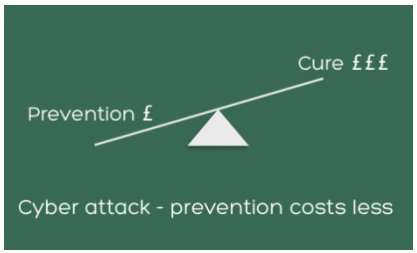
UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Rischio informatico - Compliance

Frodi Telefoniche 7,5 $/miliardi

CFCA 2015 ©



EU General Data Protection Regulation
GDPR

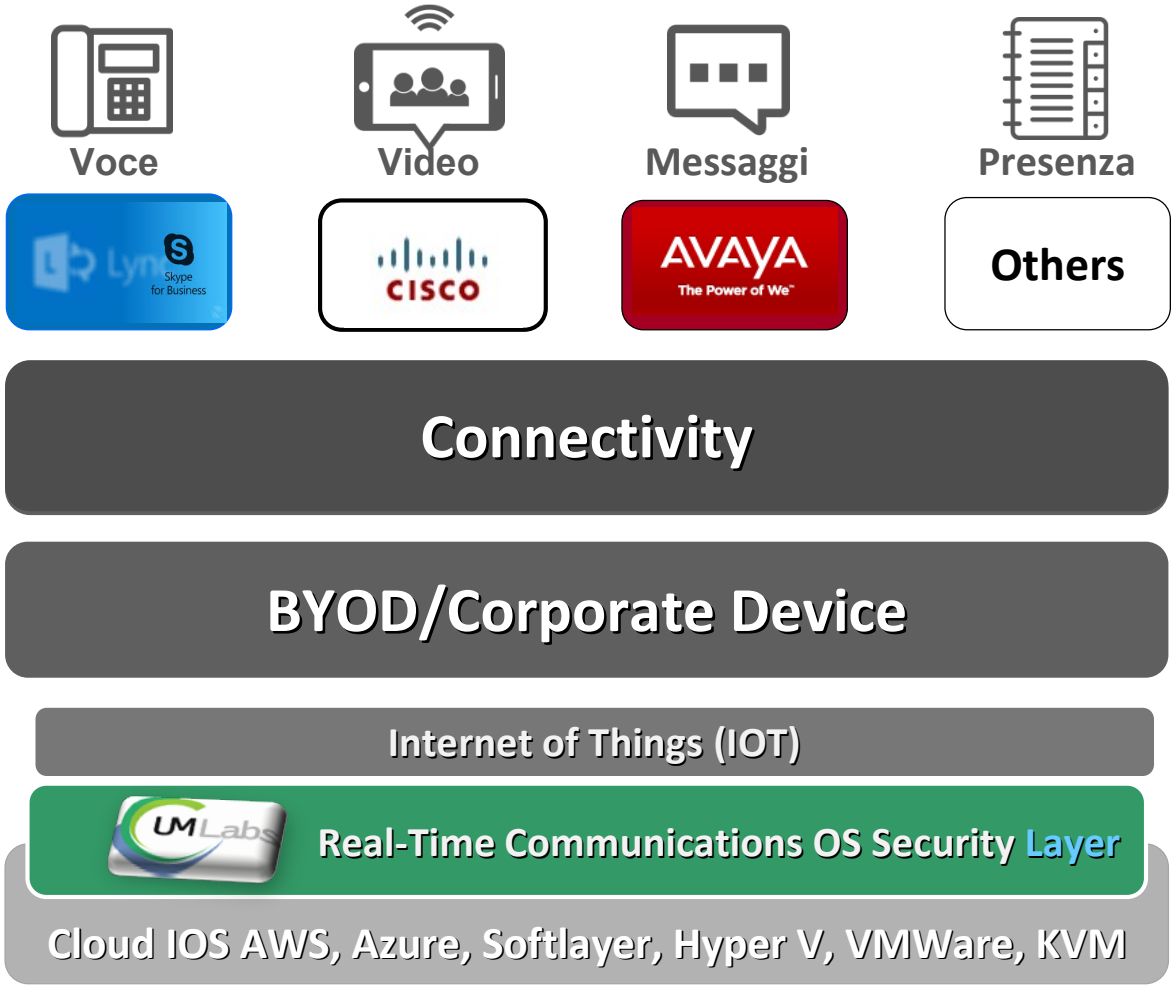
enisa
European Network and Information Security Agency

- ✓ "Industrializzazione" del cyber crime, attacchi multilivello
- ✓ GDPR 679/16 – Protezione dati e servizi, dalla progettazione alla esecuzione, autodenuncia 72 h, onere della prova, sanzioni (4% giro d'affari)
- ✓ Linee guida ENISA – difesa multilivello

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

UM Labs – uno strato di sicurezza a protezione delle UC



Contenuti UC

Livello applicativo UC

SIP Trunking

Mobile

Wi-Fi

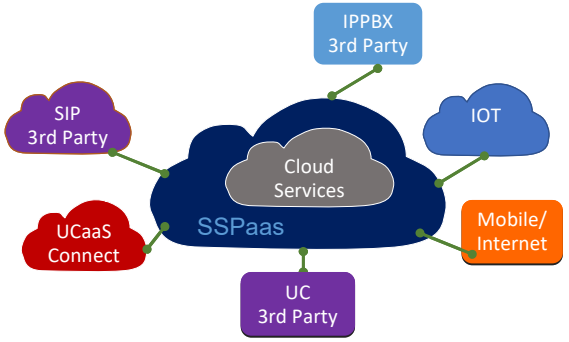
IPV4/IPV6,

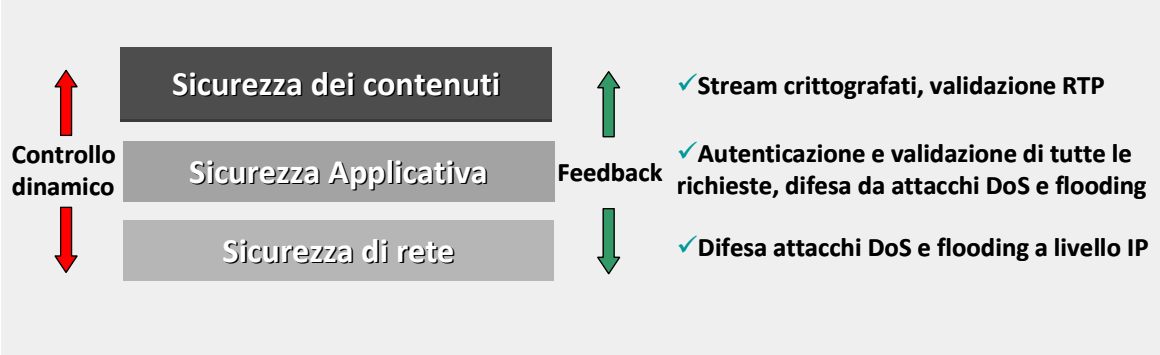
3G/4G/LTE, Wi-Fi

UM Labs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Servizio in Cloud - Sicurezza delle UC e delle Comunicazioni





- ✓ Assicura conformità e sicurezza ad ogni applicazione UC e comunicazione in tempo reale da un cloud pubblico, privato o ibrido
- ✓ Tre livelli di sicurezza integrati: Rete IP, Applicativo e Contenuti

Sicurezza IP	Sicurezza Applicativa	Sicurezza dei contenuti
Dos/DDoS	Malformed messages	Ascolto fraudolento
Flooding Attacks	Directory harvesting	Furto di chiamate
Port Scanning	Frodi telefoniche	Modifica dei contenuti

- ✓ Protezione dagli attacchi: DoS, DDoS, Harvesting, Hacking, etc.
- ✓ "Cattura" di Voce, Video & IM secondo normativa MiFID II
- ✓ Conforme alla normativa GDPR, ed alle linee guida ENISA e USA
- ✓ Supporto SOC/NOC Management
- ✓ Sicurezza IP per Internet of Things

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

La rilevanza del GDPR per gli operatori

"**(49)** Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata *per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere*, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a *impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica*."

"32. Sicurezza del trattamento

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e *la cifratura dei dati personali*; 4.5.2016 L 119/51 Gazzetta ufficiale dell'Unione europea IT…."

"33. Notifica di una violazione dei dati personali all'autorità di controllo

1.In caso di violazione dei dati personali, il titolare del trattamento *notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore* dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. …"

"83. Condizioni generali per infliggere sanzioni amministrative pecuniarie

……

5.In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a *sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo* dell'esercizio precedente, se superiore: …."

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Linee guida ENISA

L'**Articolo 13a della direttiva 2002/58/EC** ("Telecommunications Framework Directive") stabilisce che le autorità assicurino che i provider:

1. Intraprendano le opportune misure tecniche e organizzative per proteggere le reti di trasmissione ed servizi erogati.
2. Intraprendano i passi opportuni per garantire l'integrità delle reti, e riportino alle autorità le violazioni della sicurezza con impatto significativo sull'operatività delle reti.

"*ENISA has engaged national regulators from the different EU Member States in a number of meetings and workshops to develop a technical guideline concerning these security measures, called: Technical guideline for Minimum Security Measures*"

"*..the Technical Guideline for Security Measures, provides guidance to NRAs about the technical details of implementing paragraphs 1 and 2 of Article 13a: how to ensure that providers assess risks and take appropriate security measures*"

Il paragrafo SO11 (Security Objective 11) delle line guida specifica i requisiti di accesso e controllo per una protezione multi-livello:

Sono state condotte e riportate evidenze di rispondenza ai requisiti degli apparati legacy comunemente impiegati, quali Firewall e SBC

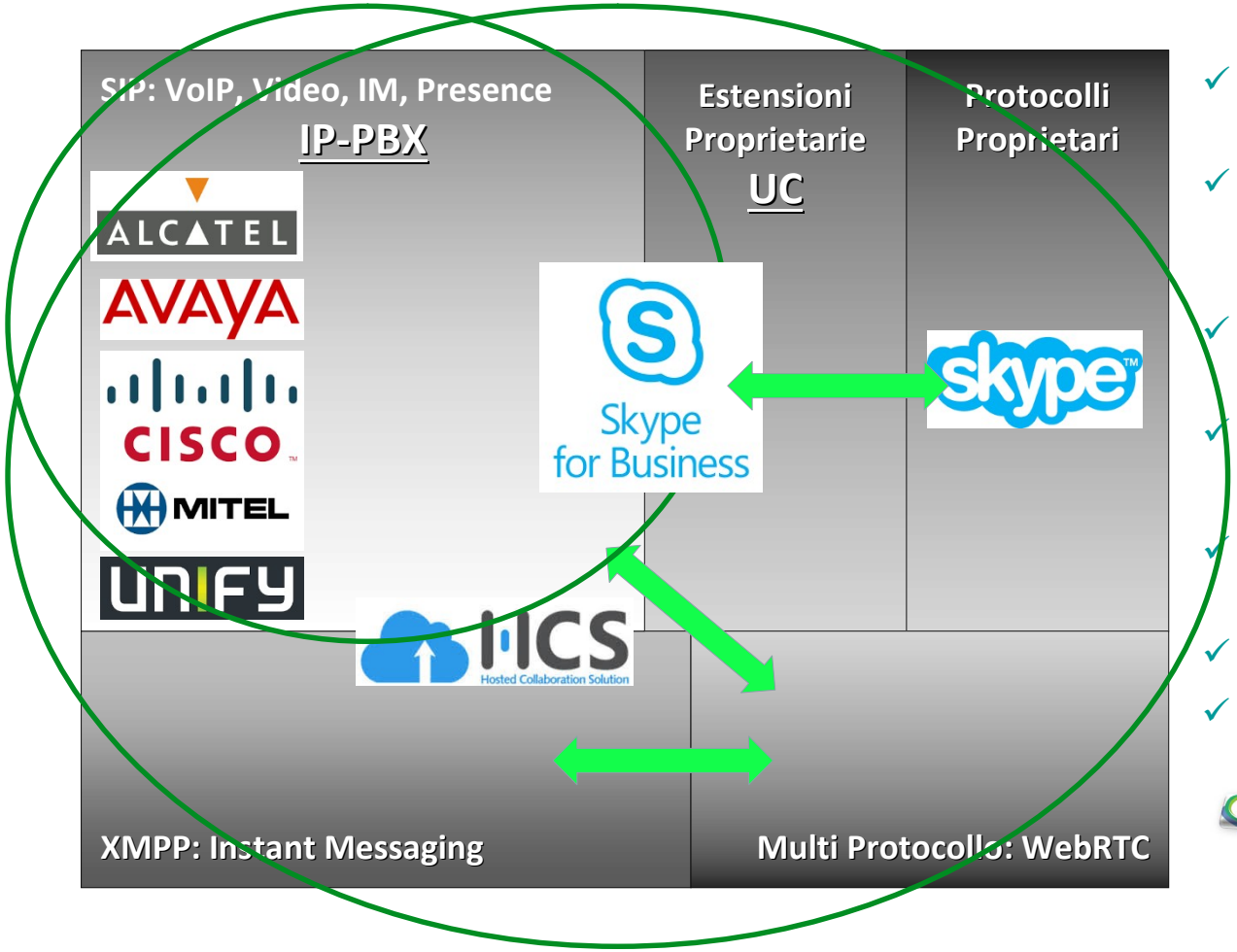
Security Feature	UM Labs	SBC
Multi-level security	✓	×
Specific defences against application level threats (e.g. DoS attacks)	✓	×
Block probe attacks used by fraudsters	✓	×
Real-time black list for call fraud control	✓	×
Signalling and media encryption services	✓	- (1)
Proven to meet GDPR compliance requirements	✓	×
Cloud deployment option with SDN/NFV support	✓	×

	Security measures	Evidence
1	a) Users and systems have unique ID's and are authenticated before accessing services or systems. b) Implement (logical) access control mechanism for network and information systems to allow only authorized use.	• Access logs show unique identifiers for users and systems when granted or denied access. • Overview of authentication and access control methods for systems and users.
2	c) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. d) Choose appropriate authentication mechanisms, depending on the type of access. e) Monitor access to network and information systems, have a process for approving exceptions and registering access violations.	• Access control policy including description of roles, groups, access rights, procedures for granting and revoking access. • Different types of authentication mechanisms for different types of access. • Log of access control policy violations and exceptions, approved by the security officer.
3	f) Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms. h) Access control policy and access control mechanisms are reviewed and when needed revised.	• Reports of (security) tests of access control mechanisms. • Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). • Logs of intrusion detection and anomaly detection systems. • Updates of access control policy, review comments or change logs.

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Unified Communications - Interoperabilità



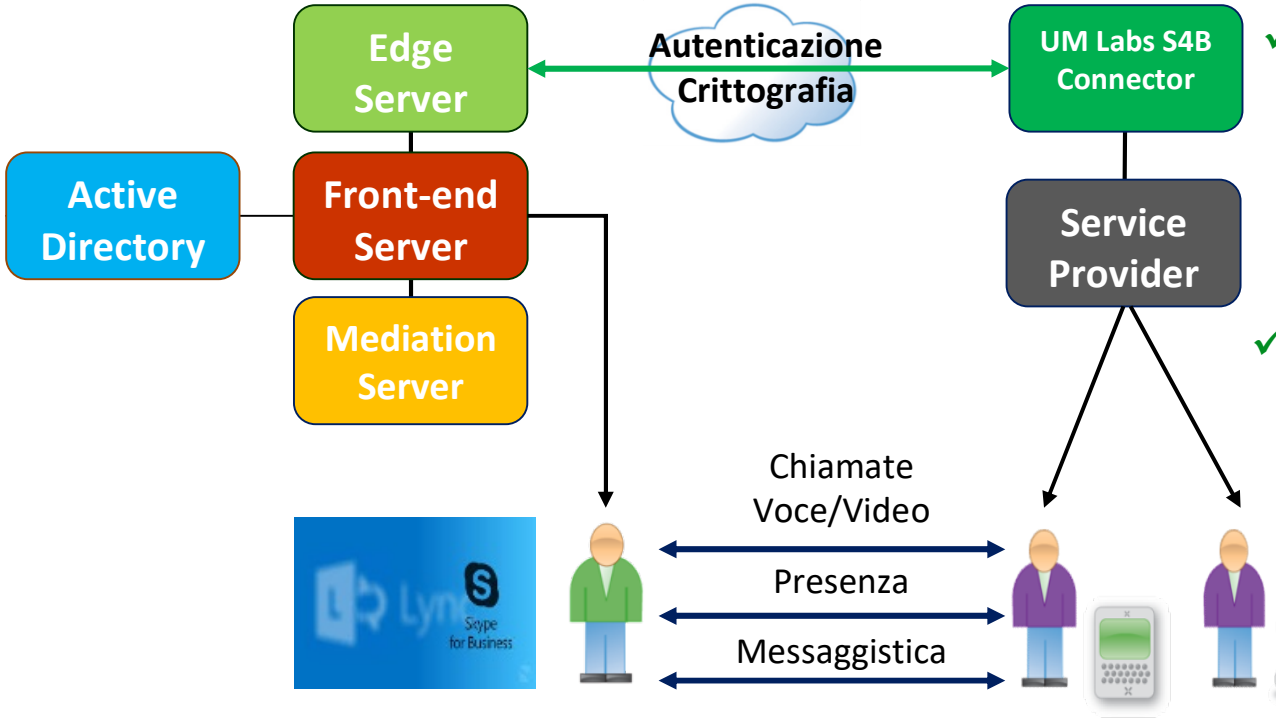
- ✓ I sistemi UC impiegano protocolli di comunicazione variegati
- ✓ Session Initiation Protocol (SIP): è il protocollo standard adottato dai maggiori player di sistemi IP
- ✓ Consolidate applicazioni impiegano protocolli proprietari
- ✓ o estensioni proprietarie del protocollo SIP
- ✓ La messaggistica istantanea dispone di un protocollo specifico
- ✓ Verso sistemi multi-protocollo
- ✓ Cresce l'esigenza di inter-connettere questi sistemi

UMLabs Garantendo la sicurezza in modo facile e immediato

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Funzionalità di integrazione avanzata per Skype for Business



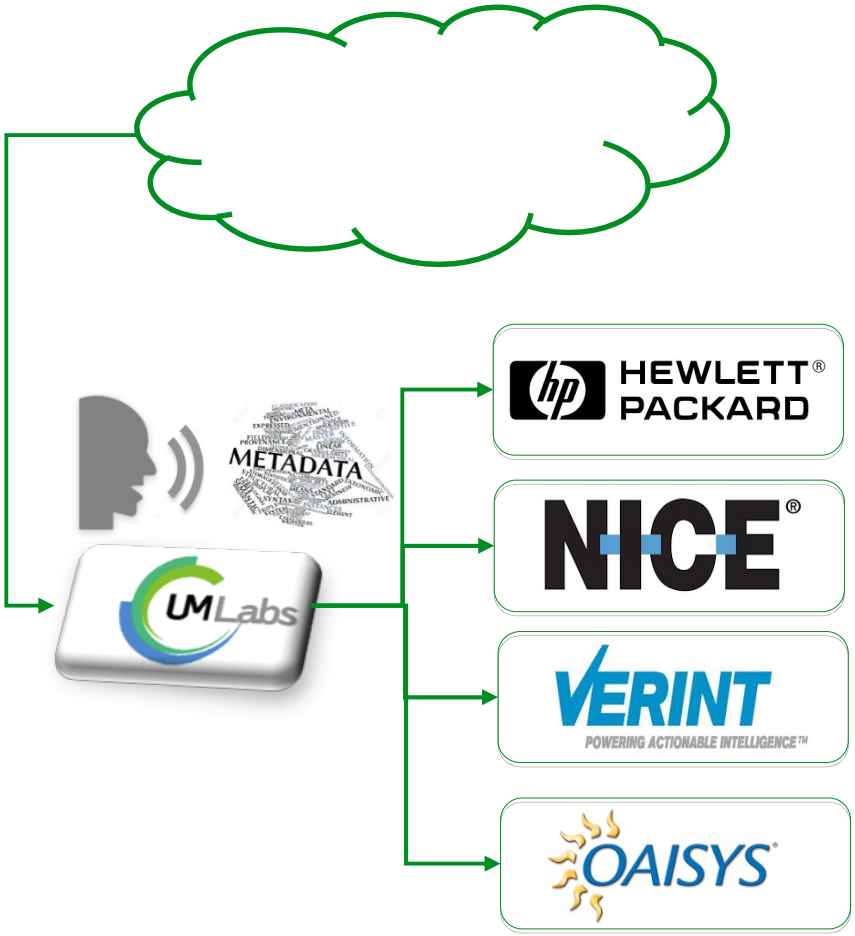
- ✓ UM Labs consente di connettere direttamente il server Edge ai servizi di un provider e/o di un sistema IP-PBX
- ✓ Abilita tutte le funzionalità native di Skype for Business agli utenti remoti ed agli utenti di servizi hosted

- ✓ Autenticazione tramite Active Directory, single sign-on, dialling semplificato, common name space, integrazione nativa
- ✓ Sicurezza end to end per tutte le comunicazioni tramite autenticazione e crittografia

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Funzionalità di Call Capture per sistemi di registrazione

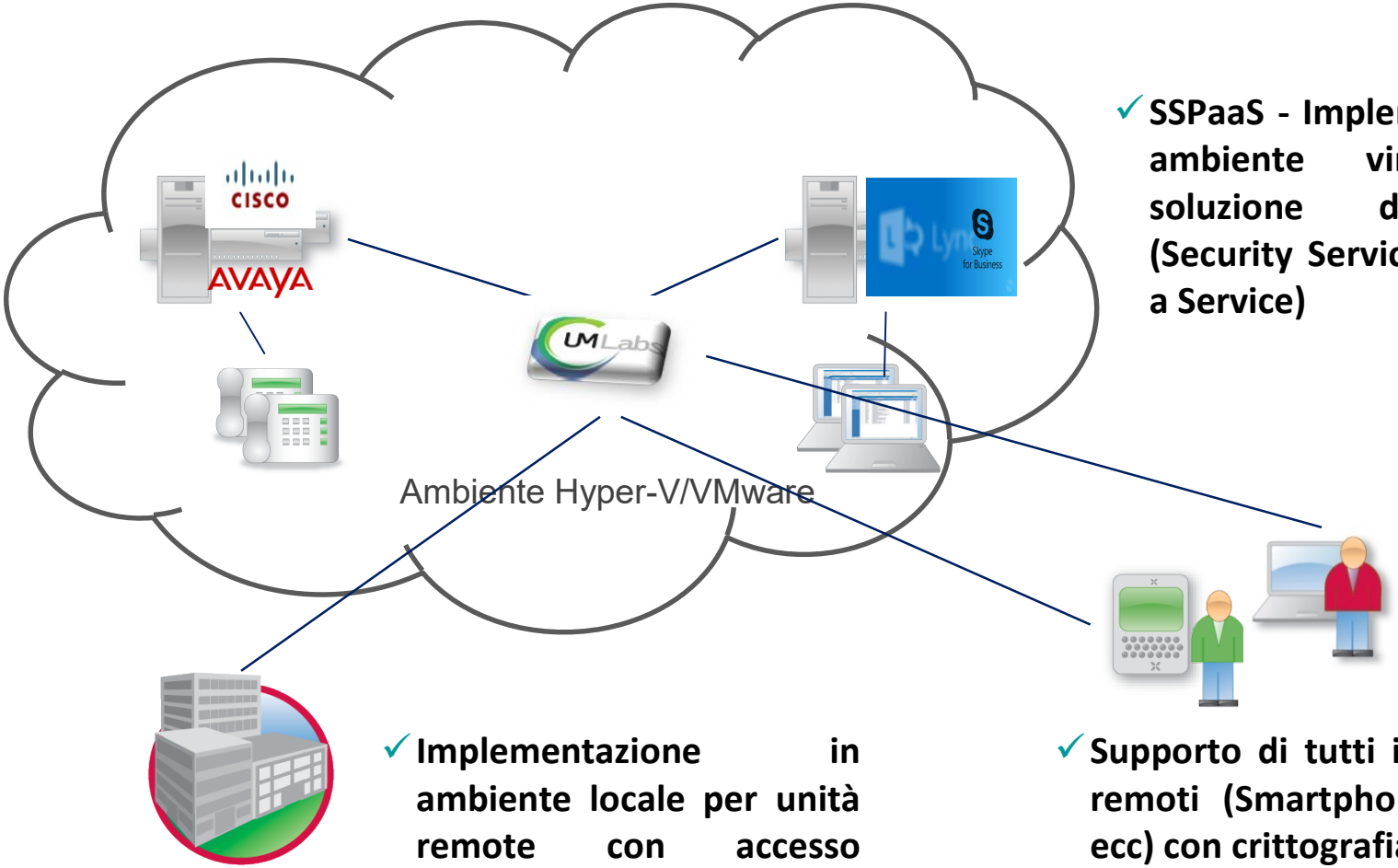


- ✓ **Le chiamate vengono catturate ed elaborate per rispondere ai requisiti specifici:**
  - ☑ **Separazione dei Media streams**
  - ☑ **Registrazione delle chiamate assemblate**
  - ☑ **Registrazione dei meta dati delle chiamate**
- ✓ **Cattura degli Instant Messages e dei relativi meta data**
- ✓ **Disponibili funzionalità base di lettura/ riproduzione web based**
- ✓ **Esportazione delle registrazioni verso sistemi di indicizzazione/ storage**
- ✓ **Rispetto dei requisiti legali**

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

UM Labs – Implementazione tipica



- ✓ **SSPaaS - Implementazione in ambiente virtuale della soluzione di sicurezza (Security Service Platform as a Service)**

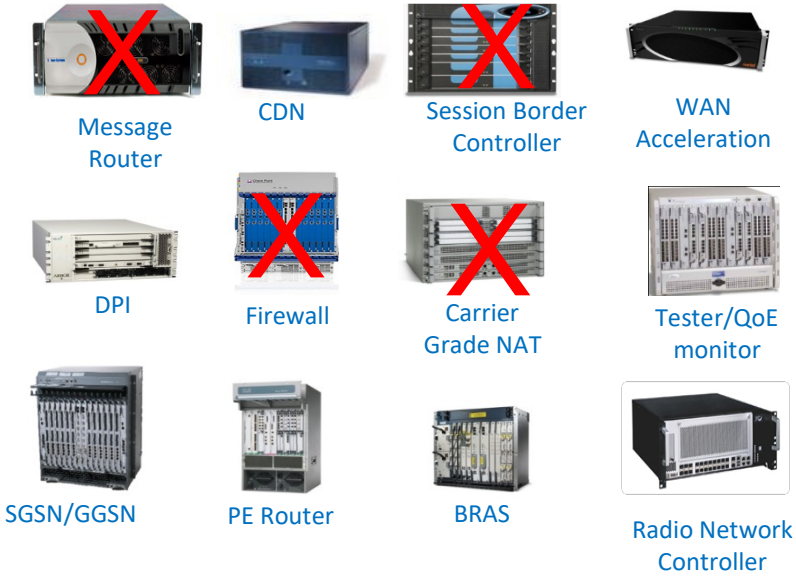
- ✓ **Implementazione in ambiente locale per unità remote con accesso crittografato**

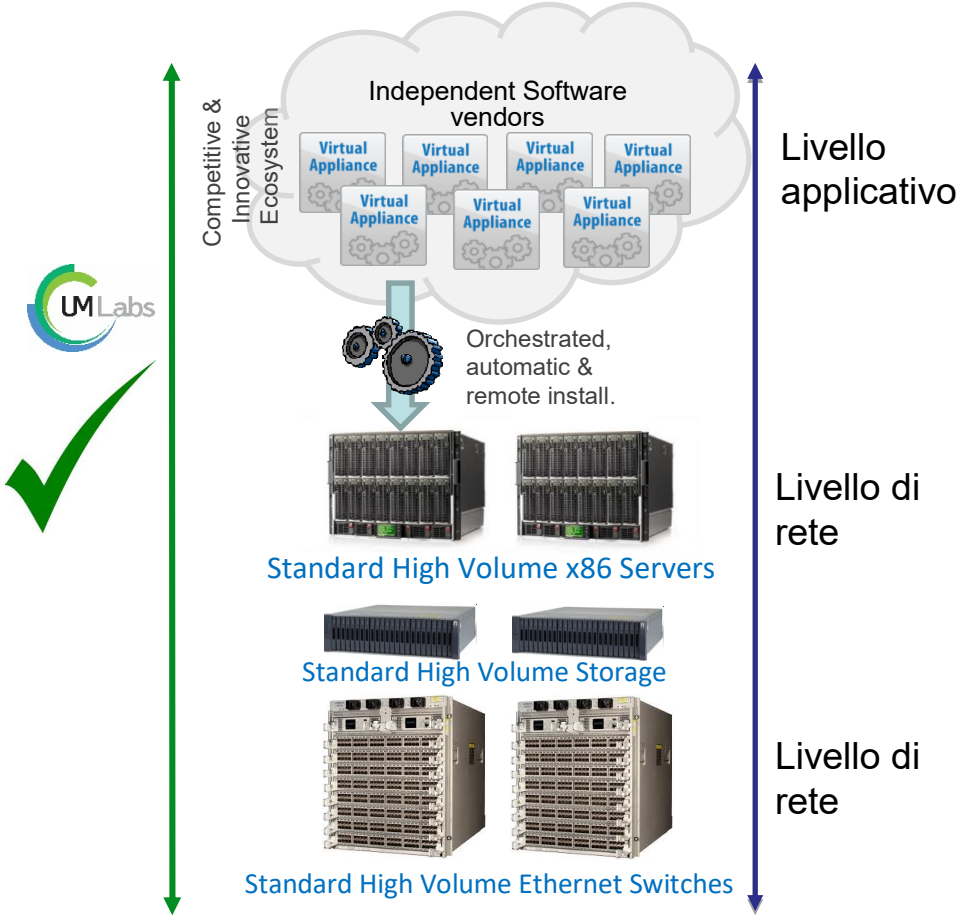
- ✓ **Supporto di tutti i dispositivi remoti (Smartphone, Tablet, ecc) con crittografia**

UM Labs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Evoluzione delle infrastrutture e implicazioni sulla sicurezza





Approccio classico:

Dispositivi Hardware frammentati e non commodity
Installazione/configurazione fisica per apparato e per sito
Sviluppo dell'HW: forte barriera all'entrata di nuovi vendors, limite all'innovazione e alla competizione

Sicurezza Multi-Livello

Progettata per implementazioni con tecnologia SDN/NFV

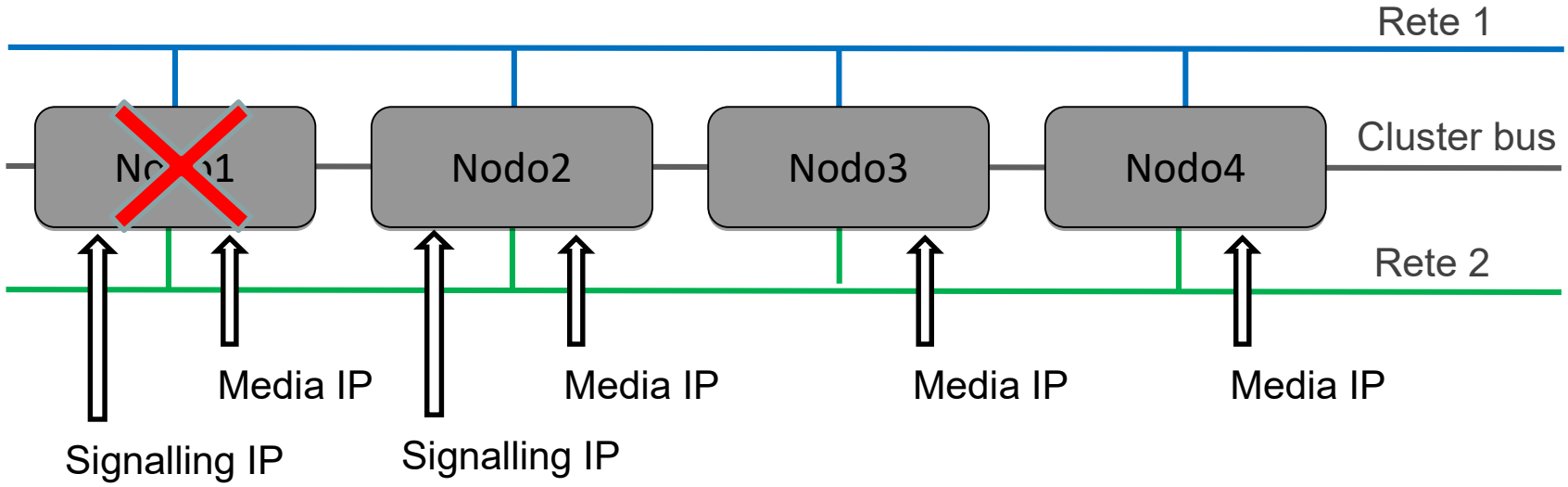
Nessuna integrazione in termini di sicurezza

UM Labs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Scalabilità e flessibilità

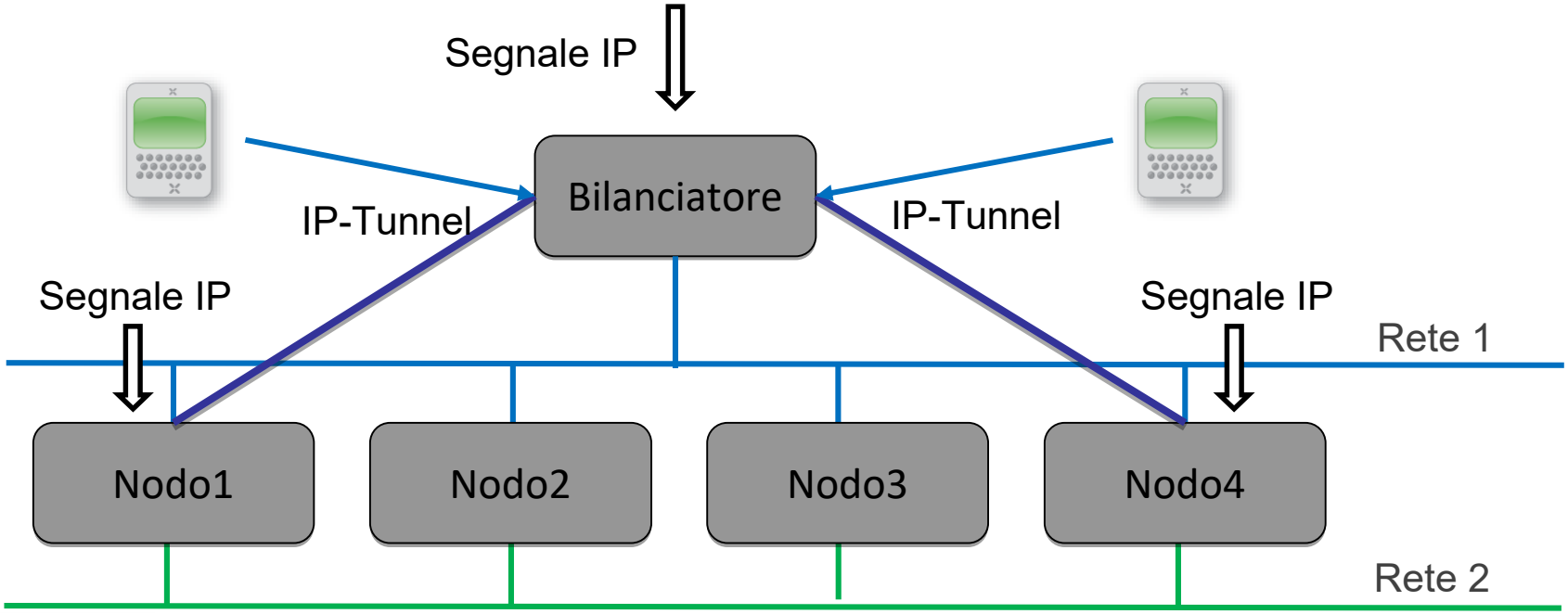
- ✓ La soluzione supporta la clusterizzazione con indirizzi IP variabili
- ✓ Segnalazione: Attiva/Passiva
- ✓ Media stream: Attiva/Attiva



CONCEPT

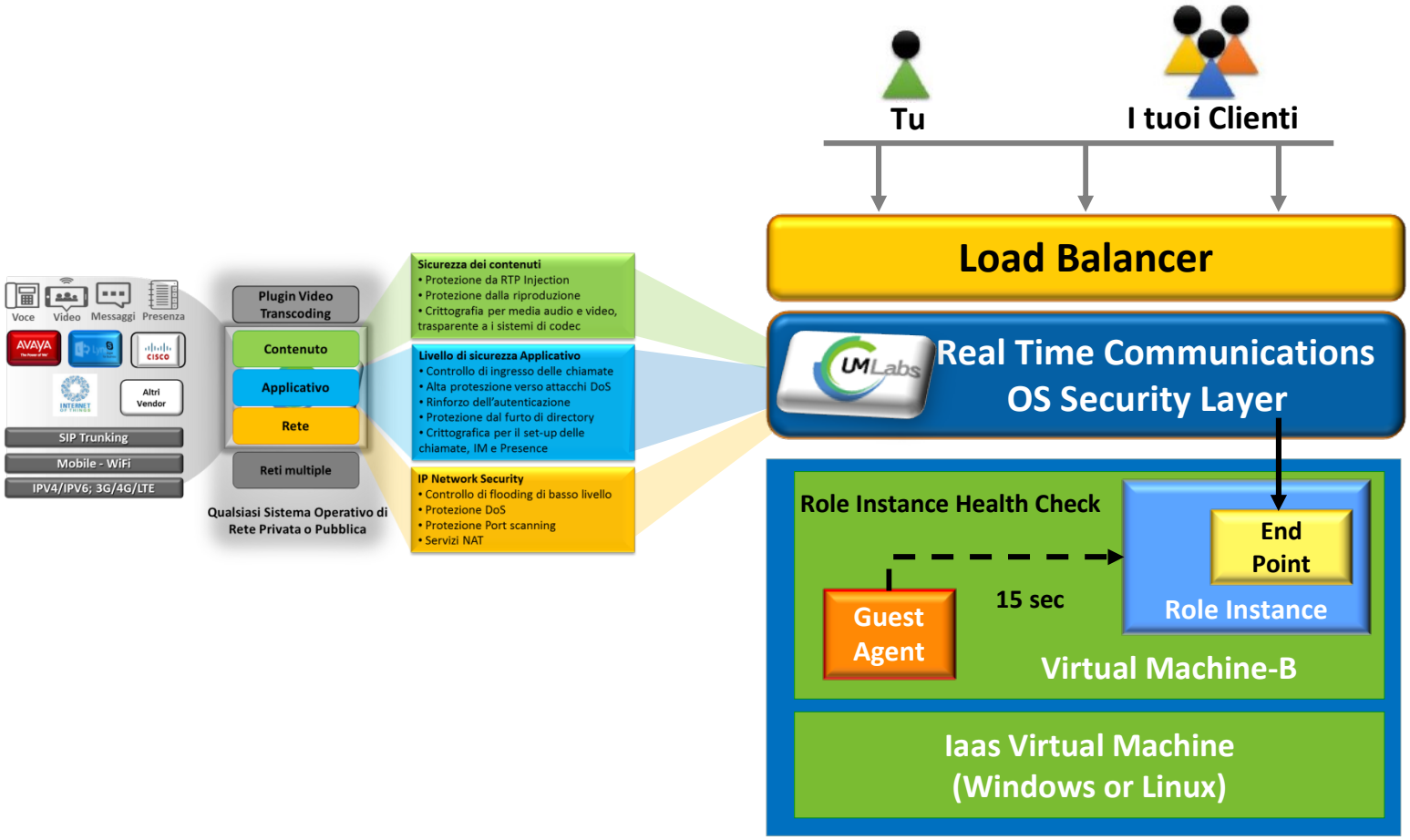
Scalabilità e flessibilità – bilanciamento

- ✓ **Decisioni di bilanciamento basate solamente sulla richiesta iniziale della segnalazione**
- ✓ **Ideale per connessioni di agenti remoti multipli**



CONCEPT

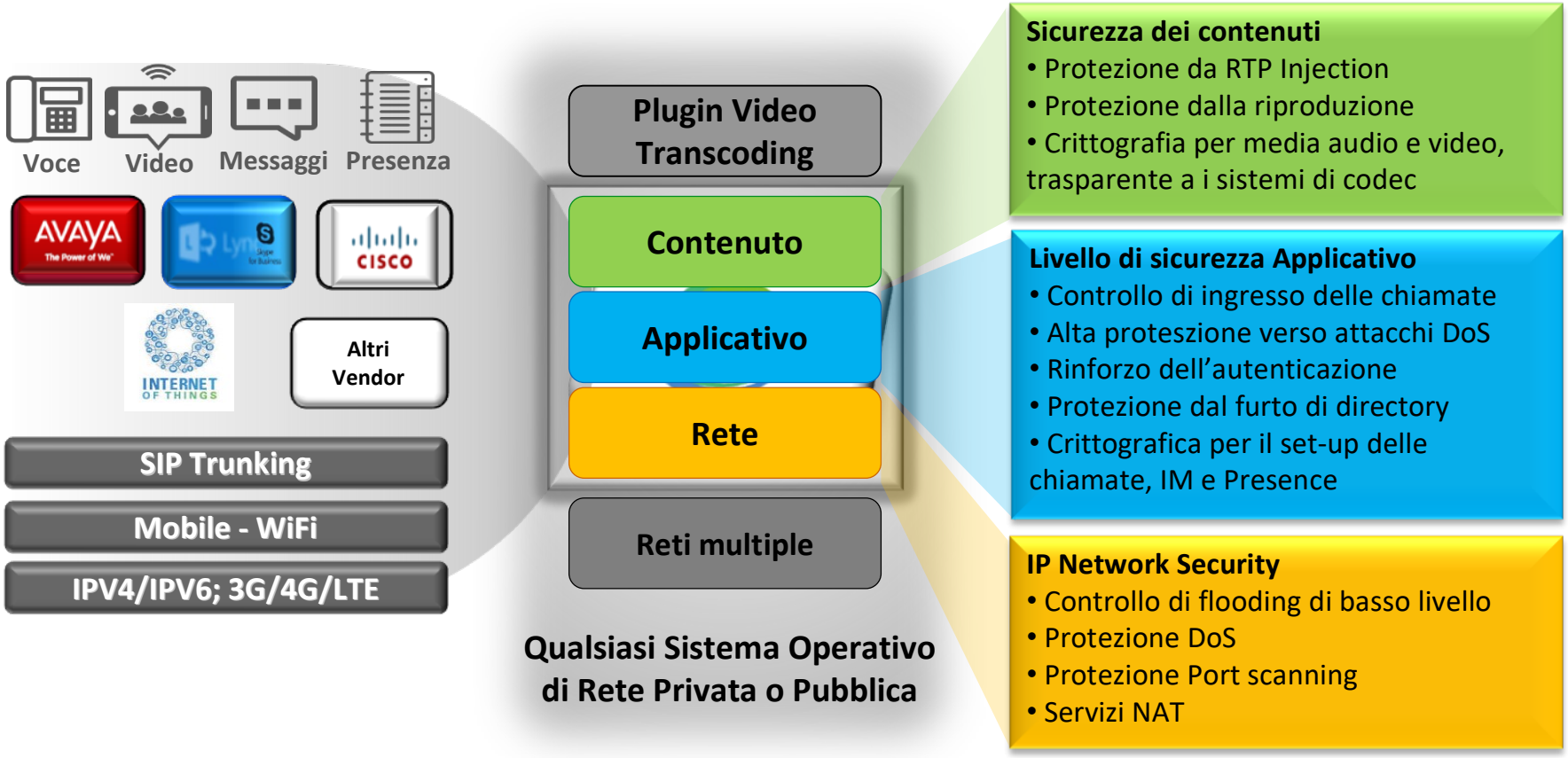
Azure - Lo strato di Sistema Operativo di sicurezza informatica per le Comunicazioni in Tempo Reale



UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

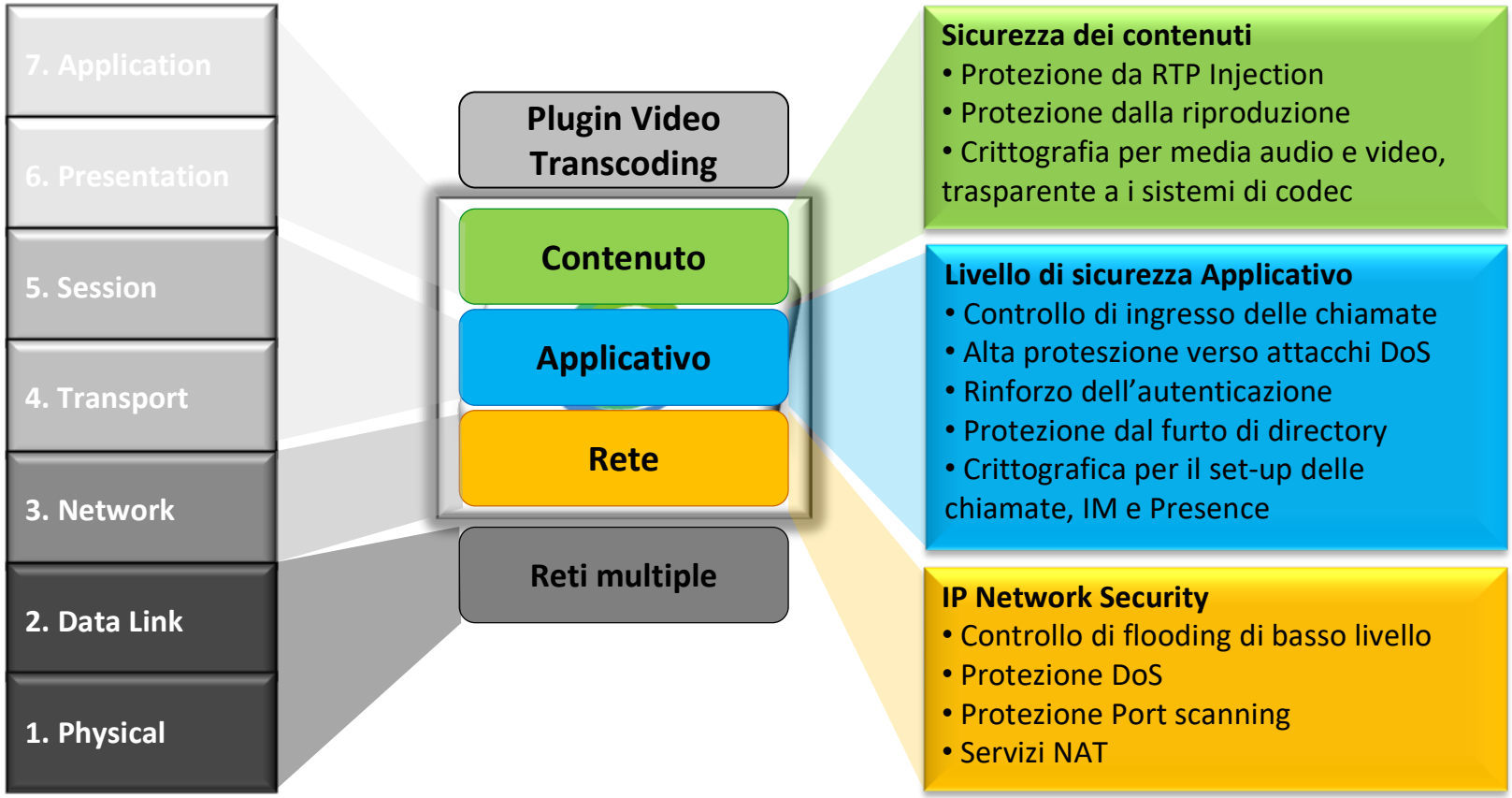
Lo Stack UM Labs



UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Corrispondenza tra le Stack ISO e UM Labs

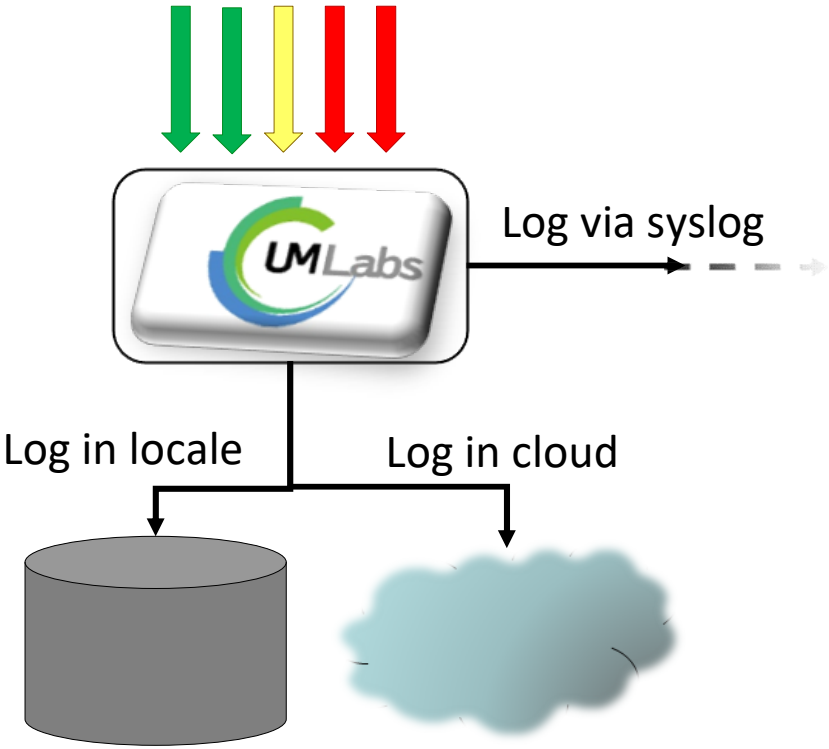


UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Funzionalità di log e controllo per Service Providers

Eventi: Normali e Anomali



- ✓ Log da sotto-sistemi multipli
- ✓ Funzionalità di log di default
  - ✓ Ogni Transazione SIP, sia a buon fine che rifiutate; indicazione dello stato di crittazione
  - ✓ CDRs (Registrazione Dettagli chiamate)
  - ✓ Blacklist e azioni di blacklist
  - ✓ Filtraggio IP
- ✓ Funzionalità di Log personalizzate
  - ✓ CDRs Personalizzate
  - ✓ Eventi speciali
  - ✓ Trigger per azioni specifiche

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Reference e Partnership

UM-Labs R&D and KPN describe their collaboration for Real-Time Communications Cyber Security at the UK Department of International Trade session in Cyber Week at the Fokker Terminal

London and Den Haag, 4th October Cyber Week – UM-LABS R&D, a leader in RTC Cyber Security UOS (Unicus) for Real-time communications (RTC) jointly described the developments of its partnership with KPN to combat major Data in Transit fraud and RTC cyber-attacks.
"Fraudulent activity is one of the many security threats facing IP based real-time communication services. The technology used in this new cyber security service by the Dutch National Telecom provider-KPN, compliments our RTC Cybersecurity technology and provides a complete security package benefiting both service providers and enterprises" said Peter Cox- CEO and inventor at UM Labs R&D.

To control this growing problem, UM Labs R&D and KPN have worked to test, audit and deliver a new model where Data in Transit cyber-attacks are protected, the addition of KPN cloud services around this, allow for full Data in Transit compliance set against GDPR, ENISA Guidelines and other regulations such as MiFiDII.
"**KPN NGSS as a service' based upon the UM-LABS technology will be available to all KPN Enterprise Market** customers for Data in Transit RTC Cyber Security which is now a huge challenge for our customers and it provides a valuable over the top service, enabling detection and blocking of fraudulent voice, video and instant messaging calls, while protecting both our customers and their own bottom line" said Johan Camps-Director of Consulting at KPN Enterprise Market.

UMLabs

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI