
IAUG
CONVERGE
NOVEMBER 2-4, 2026 | SAVANNAH, GA

Securing UC and CC from Deepfakes, Mythos, and AI-Powered Threats

DAVID MOORE

DIRECTOR, CX & ADVISORY SERVICES, **C1**


REAL
FAKE

How about now?



Cybersecurity awareness in the age of AI



Recognition alone is insufficient



Build consistent security habits



Adapt defenses to AI-assisted deception

AI changes how attackers target

Attacking systems

- Finding software weaknesses and developing exploits
- Frontier AI capabilities, including Mythos, accelerate vulnerability discovery
- Protect the platforms, integrations, and access

Deceiving people

- Impersonating customers, employees, and executives
- Synthetic voices and deepfakes are more convincing than ever
- Protect verification and business decisions

Frontier AI and Mythos

What's changing

AI can accelerate the discovery and exploitation of SW vulnerabilities

Why it matters

- Defenders can find and fix weaknesses faster
- Attackers can use similar capabilities to exploit them

Priorities for UC & CC

- **Keep platforms supported and current**
  Prioritize vendor advisories and internet-facing services.
- **Protect privileged access**
  Use phishing-resistant MFA where supported.
- **Limit access and connections**
  Review service accounts, permissions, and integrations.
- **Monitor and prepare**
  Watch for unusual access and configuration changes; rehearse response.

Deepfakes and AI-enabled fraud at scale

1 in 5

Deepfakes accounted for one in five biometric fraud attempts

Entrust

58% Increase

Deepfake selfie attempts increase 58% year over year in 2025

Entrust

$893 million

AI-related complaints reported to the FBI carried $893 million in losses in 2025

www.ic3.gov

INTESA SANPAOLO

Reuters

GOVERNMENT

September 25, 2026 3:51 PM UTC

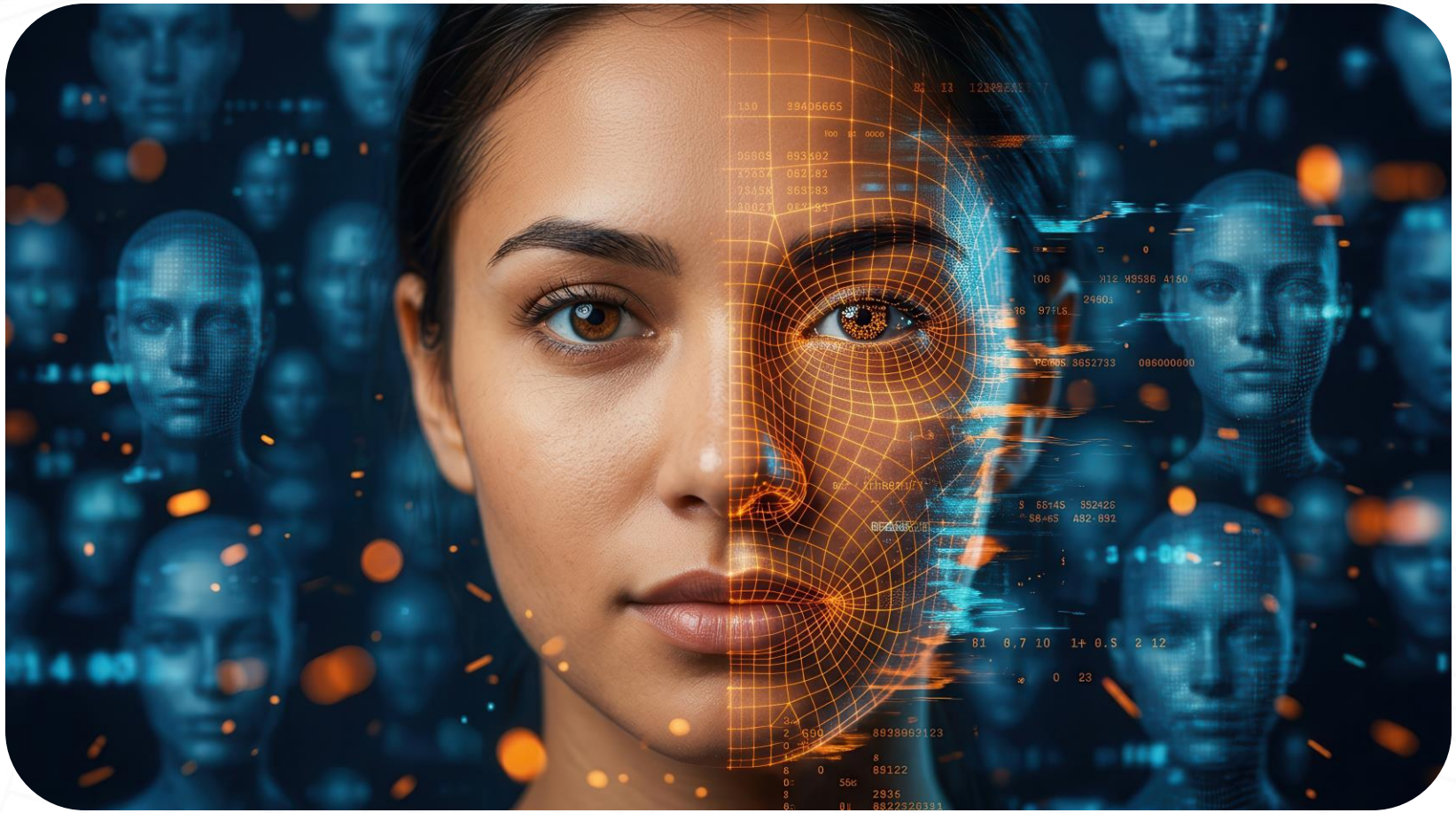
AI messaging scam costs Italy's top bank Intesa millions, sources say

By Emilio Parodi



The real problem with deepfakes

Seeing is believing



Detection | Attack Surface | Attack Vector

Why impersonations work



Convincing faces and voices | Real-time responsiveness | Context hijacking | Multichannel consistency | Pressure to act

Attack Surface



Customer Support



IT Service Desk



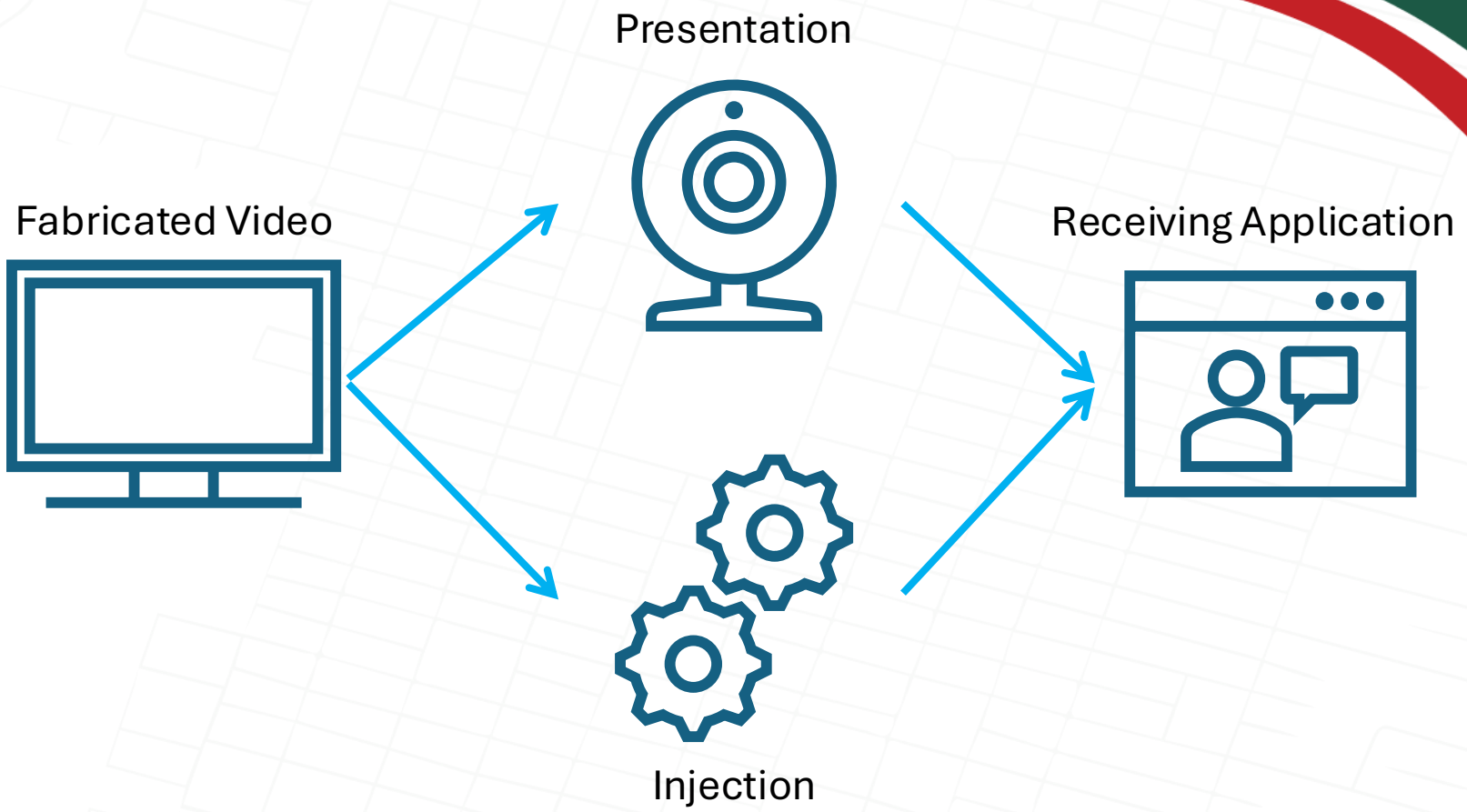
Direct to Employee

Attack surface

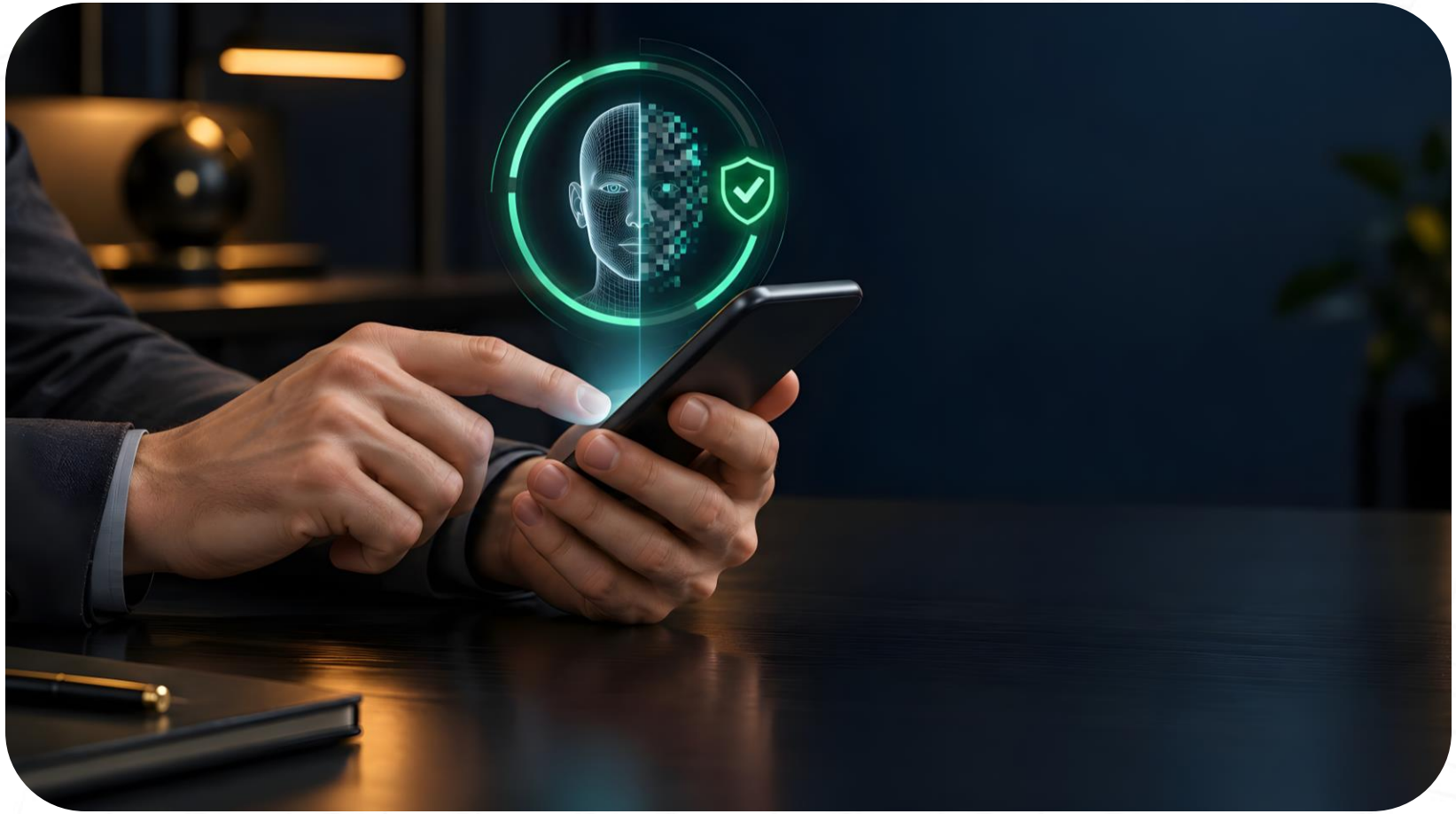


CCaaS Workflows | UCaaS Collaboration platforms | Corporate Devices Personal Devices (mobile phones) | Unsanctioned platforms (Facetime, WhatsApp)

Deepfake Attack Vectors



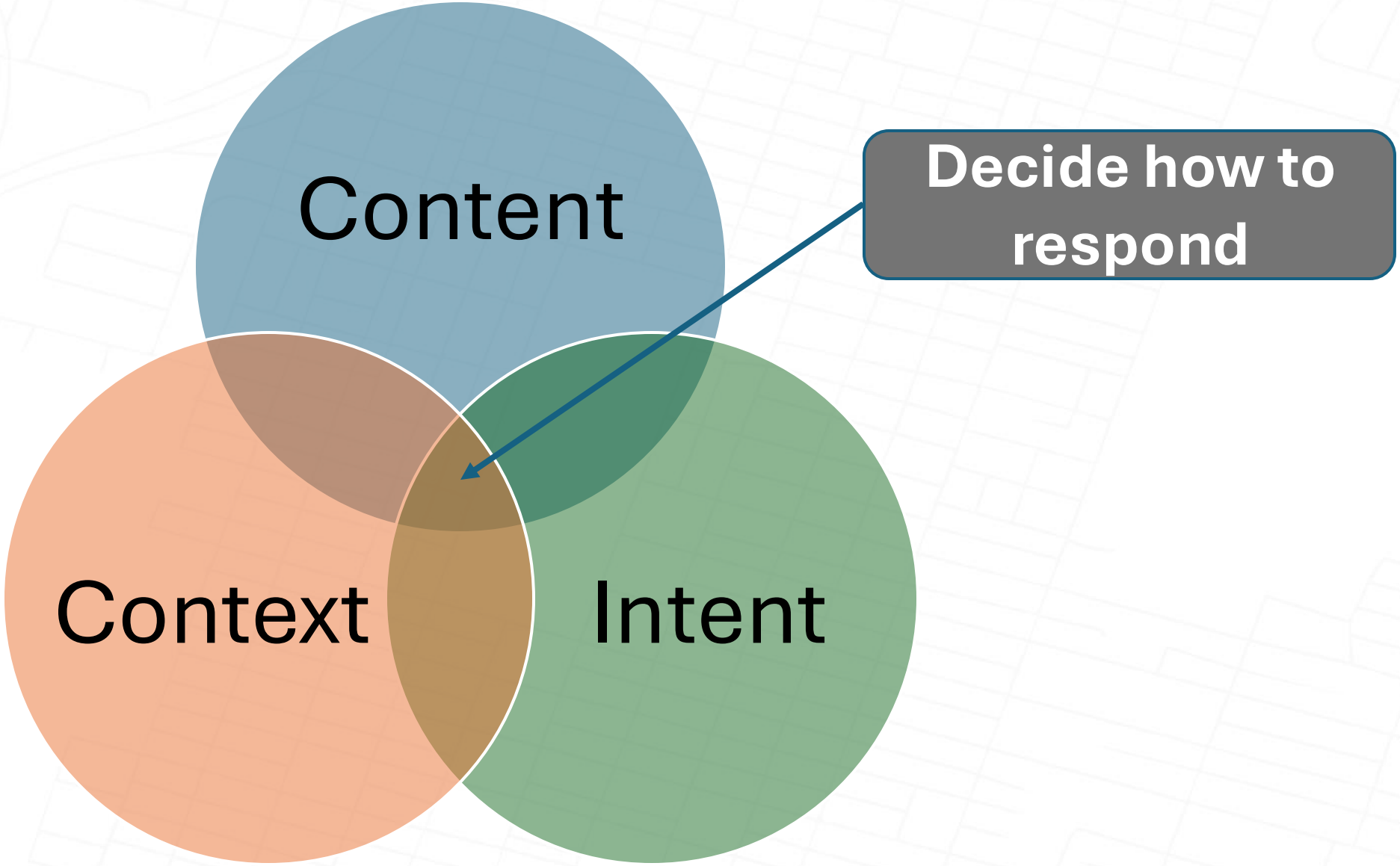
Defending against deepfake



People | Process | Technology

Is this real?

Does this make sense?


Content
Context
Intent
Decide how to respond

Zero trust architecture



Who? What? Where? When? Why?

Never trust | Always verify | Assume breach

Preparing people to respond

Verify identity through approved methods (never trust, always verify)

Consistent scripts and playbooks

Regular simulation and drills

Recognizing red flags

Pause, verify and escalate

Process: Verification before action

Verify through trusted route

- Independently sourced callback or approved authenticated channel

Escalate and obtain approval

- Additional review for sensitive actions or unresolved concerns

Limit exposure

- Transaction limits and holds where appropriate

Record and report

- Document verification, decisions and suspicious activity

Deepfake defense controls

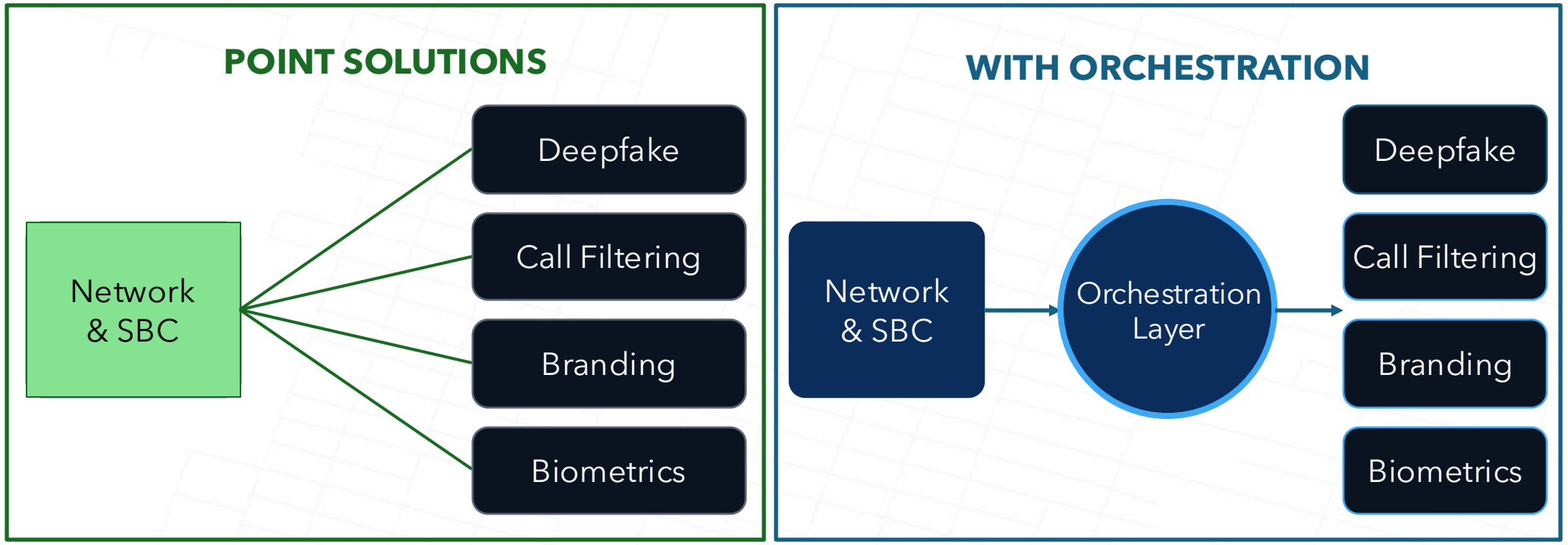
	PRESENTATION ATTACK Fake material in front of the camera	INJECTION ATTACK Substituted media in the digital capture path
1	Context & Risk Assessment	
2	Media & Liveness Analysis	
3	Interactive Challenges	
4	Screen Replay & Physical Spoof Detection	
5		Camera & Device Validation
6		Session Metadata Analysis
7		Application Tamper Protection
8		Capture & Transmission Integrity

Synthesis based on NIST SP 800-63A-4 and ENISA Remote ID Proofing Good Practices (2024).

One orchestration layer harnesses the AI tool explosion

Orchestration architecture

Plug each tool into the control plane once. Add, swap, or retire apps without rebuilding the core.



Signals don't share. Reintegration repeats.

Apps share signals in real time. Core network untouched.

EXAMPLE Deepfake detection flags an anomaly; orchestration updates shared treatment data so the next call is flagged for additional scrutiny.

C1 AI-powered portfolio

CX

EMPLOYEE EXPERIENCE
- Voice, Messaging & Video
- Meetings
- C1CX Hosted UC

CUSTOMER EXPERIENCE
- AI-Infused Omnichannel Engagement
- Integrated Customer Journeys
- Digital Orchestration AI/IVA
- Next Generation 911
- C1CX Hosted CC

VOICE CONNECTIVITY
- Carrier Services
- Trusted Voice

IX

ENTERPRISE NETWORKING
- Wired (LAN, WAN)
- Wireless (Wi-Fi, 5G)
- SD-WAN

MODERN INFRASTRUCTURE
- Compute, Storage & Virtualization
- Data Protection (Backup, DR, CR)
- C1CX Hosted Infrastructure

RAPID DEPLOYMENT
- Device as a Service
- Mobile Device Management
- Configuration, Kitting, Warehouse

SX

DATA & INFRASTRUCTURE SECURITY
- Virtual CISO/ GRC
- Managed Detection & Response
- Vulnerability/ Asset Intelligence
- Firewall
- Observability

USER & DEVICE PROTECTION
- Zero Trust (Identity, Network, System, Application, Monitoring)
- Mobile Device Management
- Operational Technology

PHYSICAL SECURITY
- Cameras & Access Control

AVAYA CISCO DELL Extreme networks GENESYS HPE paloalto NETWORKS

Resell | Advisory Services | Lifecycle Services | Professional Services | Total Care Managed Services | Maintenance Services | C1CX Hosting

Education | State & Local Gov | Healthcare | Finance

How C1 can help

- AI-Driven Security Controls & Solutions
- Zero Trust Architecture & Deployments
- Infrastructure & Data Protection
- Identity & Device Security
- Voice & Deepfake Defense
- Cyber Recovery & Resilience
- Vulnerability Management
- Managed Detection & Response (MDR)

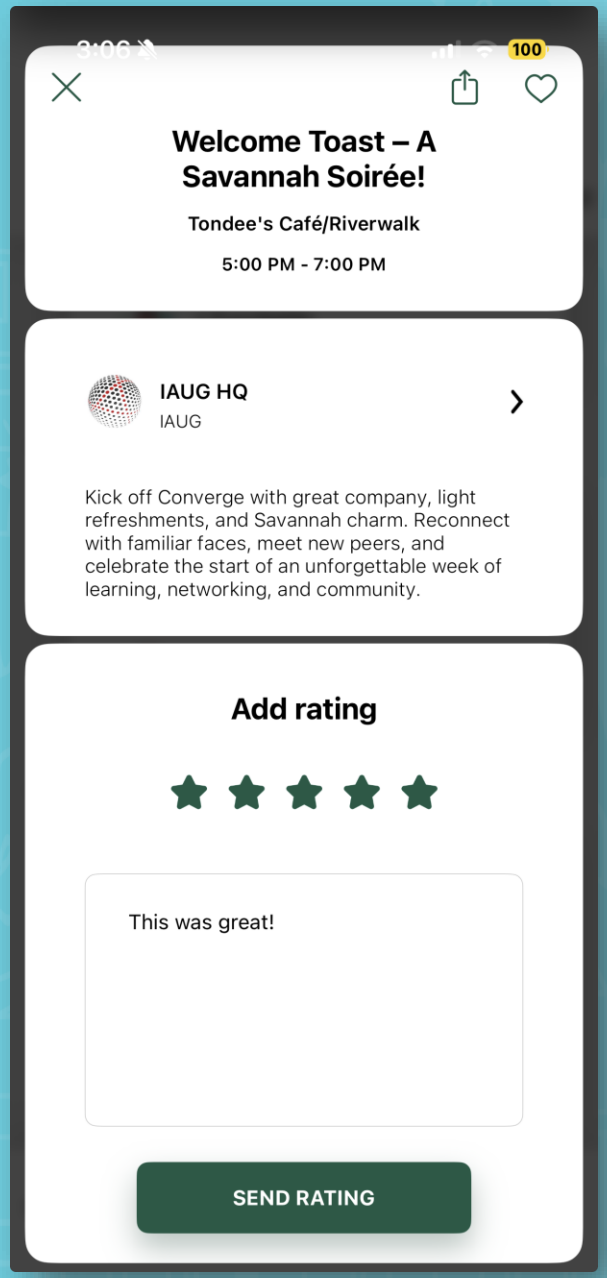


Join the IAUG Community + download the app!

International Avaya Users Group

International Avaya User Group (IAUG)

SCAN HERE



Thank you!

Please take a moment to provide a rating and feedback in the IAUG Converge App.

All feedback is hidden and anonymous.

1. Click on this session.
2. Scroll to the bottom and find "Add rating."
3. Select between one (low) to five (high) stars.
4. Leave an optional comment explaining your rating.
5. Click, "Send Rating."

Thank You