www.pipelinepub.com
Volume 22, Issue 1

Letter from the Editor
Security & Assurance - November 2025

By: Scott St. John - Pipeline

We live in an era where connectivity is no longer just an enabler — it's the very backbone of business, society, and the global economy. Today's enterprises and service providers are locked into a relentless race: not only to connect — customers, devices, and networks — but to secure, assure, and trust those connections. Every mesh of cables, every wireless hop, every cloud-based service is now a potential target and potential battleground.

In the last decade, we have witnessed two competing forces. On one hand: the explosion of possibilities — rampant adoption of artificial intelligence (AI); launch of wireless, terrestrial, satellite, and extraterrestrial network deployments; edge computing; hybrid-cloud infrastructures; and IoT driving everything from manufacturing to healthcare. On the other hand, the dark side of that expansion includes sophisticated cyber-attacks, service disruptions, fraud schemes, and an ever-growing regulatory burden. The convergence of these forces means that building, managing, and monetizing networks is no longer just about throughput and latency; it's about resilience, integrity, and assurance.

That shift is especially acute at the intersection of enterprise and communications technology. Service providers have become a custodian of trust, not just connectivity providers. Enterprises are rethinking connectivity as a business asset and fundamental driver of innovation. Both face a constantly changing myriad of evolving threats, audits, regulatory scrutiny, and customer expectations.

Throughout this issue, we examine the evolving security landscape and the threats that are lurking on the horizon. We examine how to mitigate AI and quantum risks and prepare networks for the eventuality of Q-day, the day when quantum computing can crack government-level encryption. And that day is near, if not already upon us. Meanwhile, some of the world's smartest minds are warning of the threat of an AI-driven global human extinction event if guardrails aren't put in place before the advent of Artificial General Intelligence (AGI), or superintelligence.

This issue also provides perspectives that drill deep into both securing the network and assuring the business. We explore how assurance isn't just about preventing a breach — it's about assuring service continuity, brand trust, regulatory compliance, and the customer experience. We dig into fraud prevention, where the network and the business process meet; into how telecommunications networks must defend against service-level attacks as much as

data theft; and into how operators and enterprises must shift from reactive defense to proactive security posture.

The days when you can simply check the boxes of whether you have the right cybersecurity tools or components installed are gone. The key consideration has now become whether your security operations can detect threats, fraud, and risks in real time. Can you – and your partners – guarantee the chain of trust from device to cloud to customer? Are you prepared for what's to come? The old boundaries between IT, OT, telecom, business risk, compliance, and customer experience are dissolving — and security (and trust) must traverse them all.

A network outage or fraud incident today can cripple brands, evoke significant Service Level Agreement (SLA) penalties, ripple into massive customer churn, and incur steep regulatory fines. But business leaders must also learn how security and assurance are becoming key strategic and competitive differentiators. As our global society becomes ever more interconnected, the imperatives grow sharper: resilience becomes revenue protection; security a revenue enabler; trust becomes your brand; and assurance a business imperative.

We've come a long way from the time when a network outage meant that only a handful of users couldn't access email. Today, a network failure can cascade across continents, impact financial systems, break trust, and even endanger lives. The flip side is that by turning connectivity into a resilient, trustworthy asset, organizations can unlock growth, new services, smarter monetization, and stronger customer relationships. Our industry sits at a pivotal moment where connectivity, cybersecurity, and business assurance converge in ways we have only begun to realize. The choices you make today will set the foundation not just for your network, but for your service, your brand, and your customers. Which is what makes this edition — the first issue of our 22nd volume — so important.

In this issue of *Pipeline*, we explore the evolving world of cybersecurity and assurance. Nokia examines next-generation quantum network security strategies that scale globally. Dispersive exposes unseen operational and enterprise network risk factors, and contributing editor Mark Cummings, Ph.D., examines the hidden risk vectors in AI-driven support systems. Belden examines how industrial-network environments demand both deep visibility and hardened assurance. TransUnion explores how fraud-intelligence data is strengthening network-level protection. AB Handshake reveals how verifying device and user identities can help prevent fraud across global communications, and Tollring explores call-data analytics and voice-fraud assurance. Exabeam demonstrates how to integrate security-information platforms with network telemetry for real-time risk visibility. We hear from Cynomi on how enterprise fraud prevention and network assurance are merging to protect both services and customers. Finally, Stellar Cyber shares how autonomous security platforms are evolving to deliver scalable, intelligent assurance across the enterprise-telecom landscape. All this, plus the latest enterprise and telecommunications technology industry news and more.

We hope you enjoy this and every issue,

Scott St. John
Managing Editor
Pipeline

Follow on X | Follow on LinkedIn | Follow Pipeline