

Canada CISO

Expert Exchange

Q3 Executive Summary
September 24, 2026

kyndryl.



Overview

Frontier AI is compressing the time between vulnerability discovery and exploitation, increasing the value of speed, visibility, and foundational security discipline. Key takeaways included enabling responsible experimentation, strengthening segmentation and credential hygiene, modernizing authentication, governing agentic access, and using clearer executive measures of accumulating exposure.

Host

Denis Villeneuve
Kyndryl, Canada Cyber Resilience
and Connectivity Practice Leader

Special guest

Kate Yamashita
Global Consult Leader, Kyndryl
Cybersecurity

Key topics

PAGE

- 03 Enabling Frontier AI without outrunning governance
- 04 Reinforcing foundational controls for faster threat cycles
- 05 Modernizing authentication while managing access friction
- 06 Governing agentic AI and measuring accumulating exposure

Enabling Frontier AI without outrunning governance

- Frontier AI is changing the speed of cyber risk more than its underlying mechanics. Familiar techniques can now be discovered, chained, and executed in days or weeks, compressing the time available for detection, testing, and remediation.
- Organizations are managing uneven adoption. Experienced users can quickly build models, code, and agents, while enterprise environments require stronger controls than personal labs. Scalable governance should define approved environments, data boundaries, and oversight without forcing every use case into a slow, one-off approval process.
- The same capabilities accelerating offensive activity can strengthen defense. Internal teams are using AI-assisted scanning to identify technical and business-logic vulnerabilities, locate likely exploitable paths, and help develop patches before weaknesses can be repeatedly abused.
- Board communication must avoid both complacency and alarm. Mapping existing controls and gaps to recognized frameworks creates a clearer investment case, while describing AI as an accelerator of known risks helps leadership understand why identity, segmentation, and automated response require renewed attention.

“Frontier AI cannot do the impossible. It does the possible at machine speed, which can look impossible to us.”

– CISO Expert Exchange Member

Reinforcing foundational controls for faster threat cycles

- Micro-segmentation programs expose how little application teams may know about actual network dependencies. Successful deployments begin with discovery and observation, keep application owners closely involved, and validate prerequisites before moving from visibility into blocking.
- Read-only deployment modes and well-defined test cases allow teams to map traffic, identify process gaps, and test whether controls stop real attack paths without disrupting production. Continuous testing can help confirm that segmentation policies operate as intended.
- Static access tokens, personal access keys, hardcoded credentials, and dormant accounts remain high-value entry points. Organizations are purging long-lived tokens, moving toward time-bound and granular access, scanning repositories and files for secrets, and strengthening remediation requirements when exposures are found.
- Automated access reviews, dormant-account discovery, and data loss prevention can reduce the burden on lean security teams while shrinking the attack surface. Foundational hygiene must become continuous and machine-assisted if defense is expected to keep pace with machine-speed discovery.

“Let’s not forget about the fundamentals as well.”

— CISO Expert Exchange Member



Modernizing authentication while managing access friction

- Adversary-in-the-middle techniques are eroding confidence in SMS and traditional authenticator workflows. Passkeys and hardware-backed FIDO2 keys are emerging as the preferred direction, particularly for privileged administrators and other high-risk access paths.
- Public-facing authentication requires a different migration approach from workforce access. Extensive user-experience testing, tailored login journeys, clear education, and practical recovery options are essential when serving users with varied levels of technical comfort.
- Shared accounts remain difficult to eliminate in operational settings such as training centers and meeting rooms. Where business processes require them, risk can be reduced through local or device-bound authentication, conditional access, restricted external communication, and tightly limited permissions.
- A tiered migration is more practical than a universal cutover. Stronger methods should be prioritized for privileged roles, remote access, unmanaged devices, and high-value transactions while organizations redesign workflows that cannot yet support individual phishing-resistant authentication.

“Authenticator app is now no longer good enough, and you have to go to a phishing-resistant MFA.”

— CISO Expert Exchange Member

Governing agentic AI and measuring accumulating exposure

- Agent permissions, credentials, data access, and behavior require a coordinated control plan as adoption expands. The immediate priority is inventory and visibility, followed by the ability to restrict unapproved tools, redact sensitive data, and monitor how agents interact with enterprise systems.
 - Agent governance is more sustainable when it integrates with existing identity, endpoint, network, data protection, and service-management platforms. Leaders remain cautious about adding standalone controls that create another operational island and introduce additional cost and administrative effort.
- The exchange did not identify a mature, universally accepted method for proving that models cannot escape intended boundaries. Organizations are limiting broad deployment, testing controls through proofs of concept, and expanding only when monitoring and containment capabilities are credible.
 - Vulnerability arrival rate compared with remediation burndown rate gives executives a concise view of whether exposure is accumulating. Framing the gap as self-insured risk is more actionable than isolated severity counts and better connects operational capacity to investment decisions.

“One of the most important things is being able to inventory and know what’s running in your environment.”

— CISO Expert Exchange Member





To learn more about the Kyndryl
Canada CISO Expert
Exchange or to become a member of
this community, please
visit this [site](#).

© Copyright Kyndryl, Inc. 2026

Kyndryl is a trademark or registered trademark of
Kyndryl Inc. in the United States and/or other
countries. Other product and service names may
be trademarks of Kyndryl Inc. or other companies.

This document is current as of the initial date of
publication and may be changed by Kyndryl at
any time without notice. Not all offerings are
available in every country in which Kyndryl
operates. Kyndryl products and services are
warranted according to the terms and conditions
of the agreements under which they are provided.