CHECK POINT™

The Executive Playbook for secure and responsible AI

Are you ready for the future of AI?

Rishi Muchalla, Field BISO and Evangelist, Office of the CTO

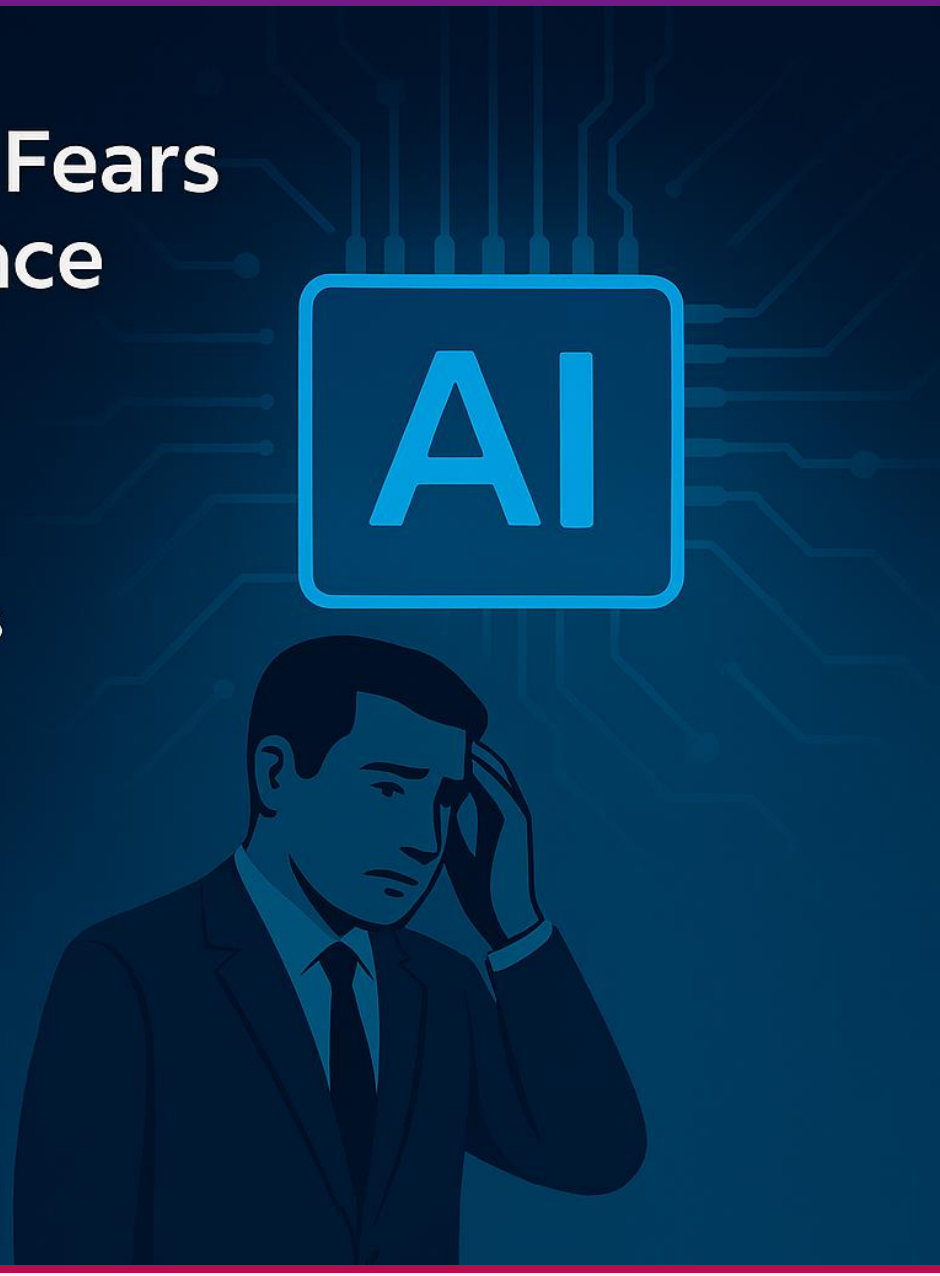
Check Point Software

What does AI mean to you?

Everyone has an opinion on how AI will affect our lives. There is no right or wrong..

Misconceptions and Fears of Artificial Intelligence

- Job displacement concerns
- Loss of control
- Ethical implications and biases
- Threat to human autonomy



AI Deception

- AI Blackmails Engineers (2025)
- Fake Audio targeting Politicians (2025)
- Fake “Elon Musk” cryptocurrency scam (2024)
- Visual Trickery (OpenAI)

AI Generated Decepticon

More than ever before, organizations need to:

1. develop operating models
2. install guardrails
3. understand the value

This session will help reframe AI governance through the lens of *Leadership, Regulation and Cybersecurity.* It explores the need to protect AI systems from manipulation, data poisoning, model theft and misuse.

The need for control is NOW!!

Reframing AI Governance through 3 lenses:

Leadership	Regulation	Cybersecurity

“AI systems aren’t just tools we use to govern the state – AI systems are assets that must be governed and secured by the state” – co-pilot

Leadership

Transformation & Effective risk management starts with great leadership.

Our Leaders can reduce the “Fear Factor”

Source: Hyperight

Leadership in the era of AI

- *We are already seeing leaders starting the journey of securing AI transformation*

- Upskill staff
- Build “psychological safety”
- Re-design Roles for Agentic Orchestration
- Mandate AI Transparency and Explainability
- Incentivize “AI Literacy”

Possible roles in an AI augmented organization

- Chief AI officer
- Prompt Engineer
- Personality developer
- Content reviewer
- AI experience designer
- Ethics officer/specialist (Fair, Transparent, unbiased)
- AI security engineer
- AI Trainer/Instructor
- Human-AI collaboration specialist
- AI adoption Manager (Champion for new tools, use case development)

Regulation

As of January, 2026 Canada is transitioning from a “voluntary” phase to rigorous regulation!

Navigating Canada’s New AI Guardrails

- Canada moves from “if” to “how” we govern it.
- Compliance is no longer a “tech” issue
- The Federal Pivot: After the Artificial Intelligence and Data Act (AIDA) died in parliament in 2025, the new approach emphasizes Digital Sovereignty and a renewed AI strategy for the Federal Public Service (2025-2027)

AI Regulations – The intersect between AIDA and NIST

AIDA

A risk-based, harms focused approach for high impact AI. Risk mitigation, Fairness and Transparency.

As part of Bill C-27 **was** mandatory

NIST – AI RMF

A voluntary, guideline for trustworthy AI. Govern, Map, Measure and Manage. Has become de facto standard in Global Tech.

Alignment between regulations and standards

NIST's risk-based approach aligns with Canada's intended harms-focused AIDA. Identify, Protect, Detect, Respond, Recover.

Canadian entities, especially federal contractors, already require NIST compliance, to manage legal/ethical risk *before* AIDA becomes law!

Operationalizing trust: The RMF provides the tools to implement governance, throughout the AI lifecycle of Design, Development and Deployment

Cybersecurity

Revalidate existing Security

Continuously update security solutions

Secure the new AI attack surfaces

Leverage AI to simplify and automate security management and operations

The Fastest Technology Shift in Our Lifetime

AI is Fundamentally Changing the Threat Landscape

SECURING NON-HUMANS

AI SECURITY

The Security Challenges of AI Adoption

Data Leakage

Via prompts, uploads and integrations

AI-specific Threats

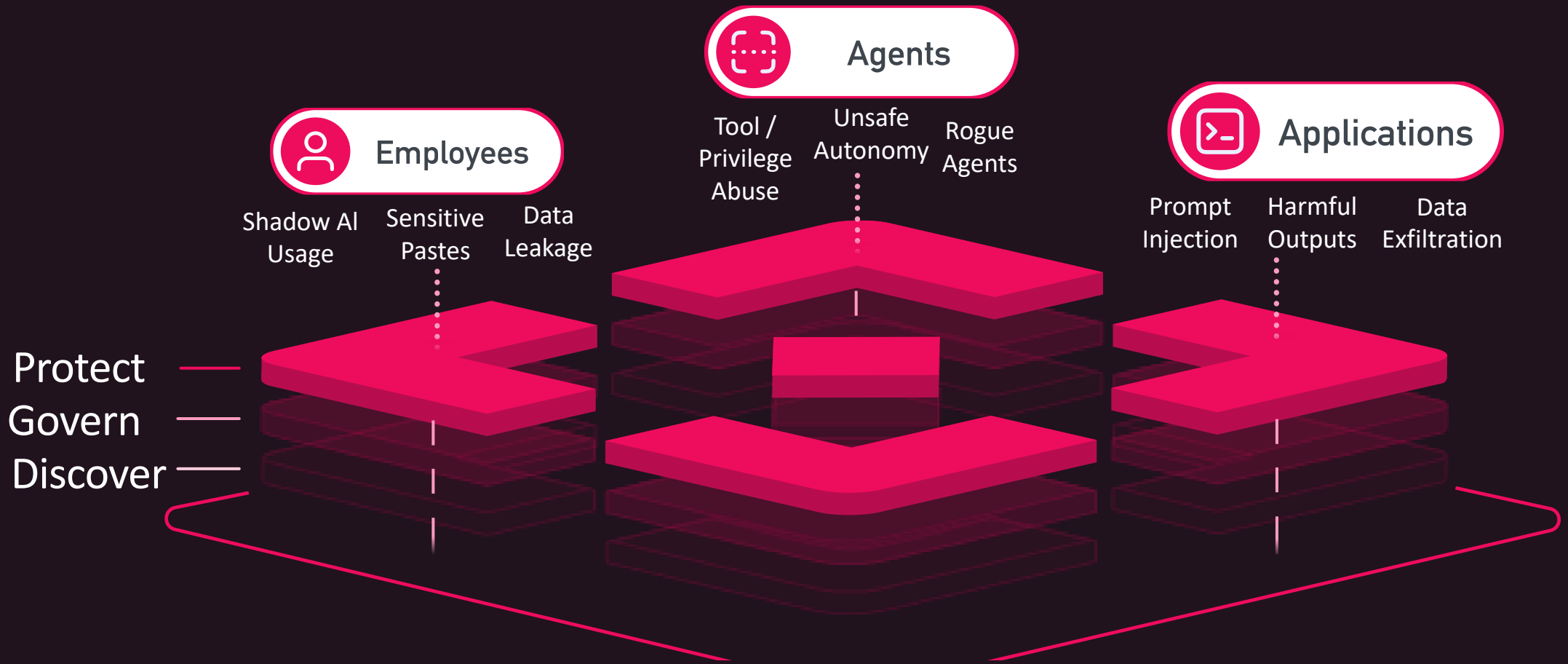
Prompt injection, model inversion, data poisoning, insecure output handling

Uncontrolled Autonomy

From agents acting beyond intended scope with unclear accountability

The AI Defense Plane

A Unified Security Model for Employees, Applications, and Agents



One platform. One lens.


Four Security Pillars
to Secure Your AI Transformation

CHECK POINT™


HYBRID MESH
NETWORK SECURITY
WORKSPACE
SECURITY
EXPOSURE
MANAGEMENT
AI
SECURITY

The Challenges of Hybrid Mesh Network Security

In the AI Era

01

The Perimeter is Everywhere

Autonomous AI expands the blast radius

02

Security Efficacy

AI Traffic hides risk inside normal-looking connections

03

Complexity Impacts Efficiency

AI Exploits permitted network access to take actions

The Challenges of Workspace Security

01 AI attacks can be launched from anywhere

02 Faster, personalized, AI-based attacks

03 Disjointed tools

The Challenges of Exposure Management

01 Overwhelming vulnerability volume with limited context

02 Disconnected intelligence and enforcement

03 Shrinking remediation windows

In an AI-Era, weeks-long resolution times **are no longer sustainable**

Final thoughts for leaders adopting AI

1. Start by aligning your stakeholders – secure buy-in, involve them in ideation and build consensus around responsible AI usage

2. Establish an AI Governance committee: Bring together cross-functional groups (legal, privacy, compliance, IT and business leads).

3. Encourage them to build an operating model that captures organizational goals, builds value cases and defines risk tolerance.

4. Manage Technical & Operational Risk: Adopt and implement “zero-trust” – Use an “identity-based access management strategy”. Foster collaboration through a consolidated, comprehensive AI Ready security platform

Thank You!

Please reach out to discuss your AI Transformation journey – rishim@checkpoint.com