



CHAPTERS

Montreal

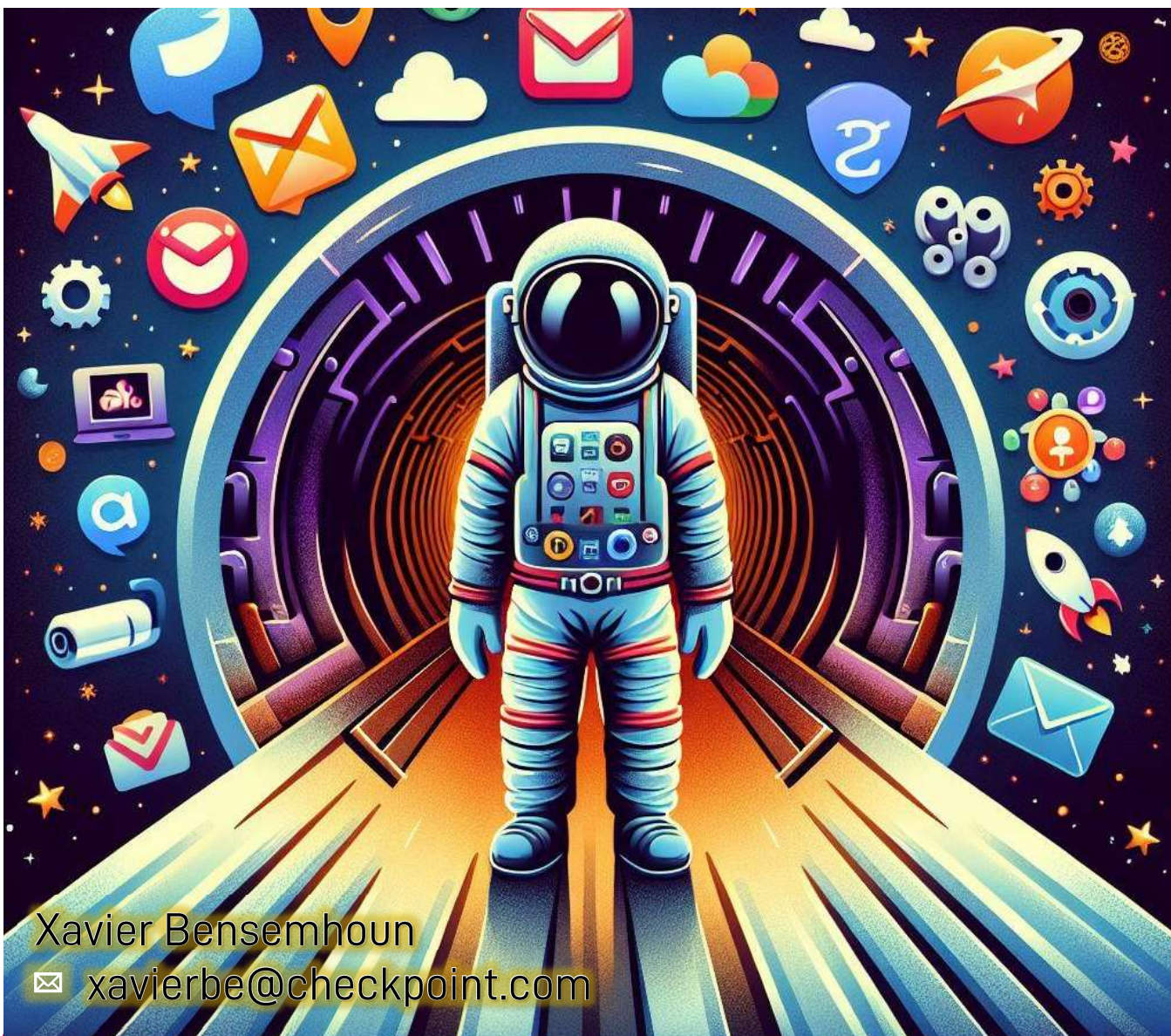
November 20, 2024

Welcome Xavier

Xavier is a Cybersecurity Evangelist and has been in the cybersecurity industry since the early 2000s. Throughout his tenure, he developed many technical solutions and helped mature the governance of many organizations.

Tonight, he will share with us his experience with SaaS Application Security!





Xavier Bensemhoun
✉ xavierbe@checkpoint.com




MONTREAL

Off course my
users' SaaS
applications are
secured!

... sorry, **WHAT?**

*The SSPM practice and how
Check Point can help on that*

Who am I?

- Franco-Canadian
- Information Security professional
 - In the field since 2003 
 - Security Engineer since 2021 at Check Point
 - Evangelist at the Office of CTO since 2024
- Fan of astronomy and science
 - Hubert Reeves' books at public library
 - 🤪 1st Internet access few month after Mars Pathfinder landed on Mars on July 4th, 1997
 - APOD consumer
- CYBER&SPACE: ENG “cyber and space” or FRA “cyber espace”

Qu'est-ce que SSPM?

- SSPM stands for SaaS Security Posture Management
 - SaaS Security: how to secure data in SaaS application you do not master?
 - Posture Management: so much important in any cloud move
- In which CISSP domains do we talk about SaaS Security?
 - Risk management
 - Security Architecture and Engineering
 - IAM
- And what's a SaaS Application?

And what's a SaaS Application?

- Cloud based « As-a-Service » applications
- Personal or professional usage
- Free or under subscription

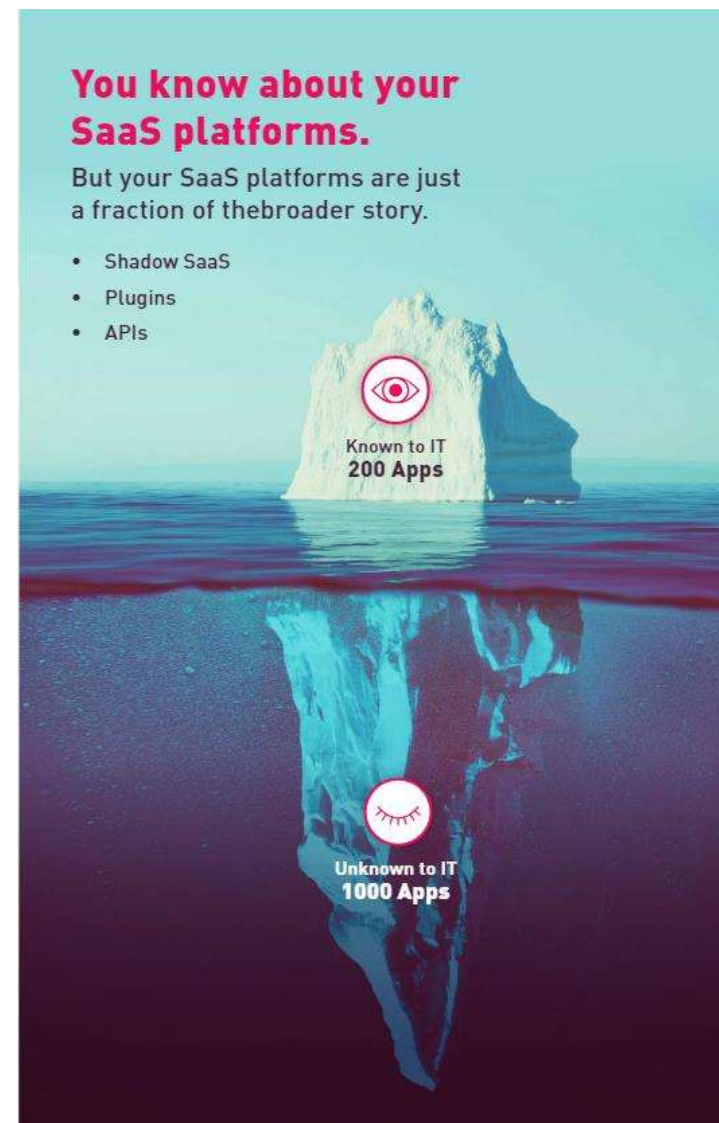
- Google Workspace, Microsoft 365 and Adobe Creative Cloud
- Salesforce, Zoom, Slack, Atlassian, Workaday, ServiceNow, Dropbox, DocuSign, Qualtrics, Mailchimp, Okta, ...
- Search engines and GenAi* (don't forget AI trainings aspects!)

So what's the current situation?

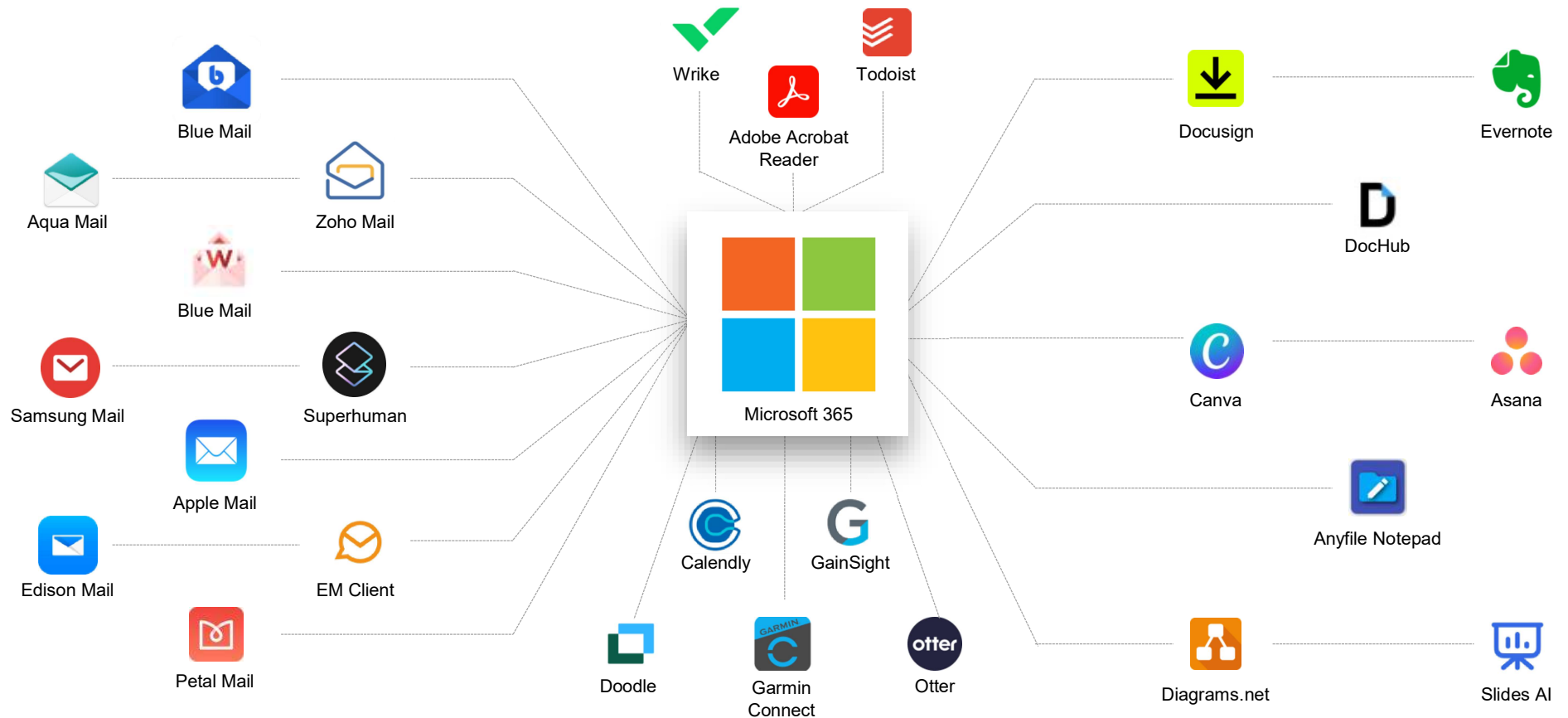
- Between 35 and hundreds of SaaS applications in every companies (and approx 30 per users)
- IT teams only aware of 20% of SaaS apps. used ¹
- 41% of app are used by a single user ; 63% of them were not accessed regularly ²
- Organisations: 85% with external users ; 20% with not fully offboarded employees ²
- Gartner's predictions:
 - Through 2025: 99% of cloud security failures: customer's fault and 90% of org. that fail to control public cloud use will inappropriately share sensitive data ³
 - Overall public cloud consumption: \$675 billion in 2024 (20% compared to 2023 ; 22% more in 2025) and driven by GenAI ⁴

Source:

1. <https://www.checkpoint.com/resources/items/the-cisos-definitive-guide-to-saas-security>
2. <https://wing.security/wp-content/uploads/2024/02/2024-Report.pdf>
3. <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure>
4. <https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024>

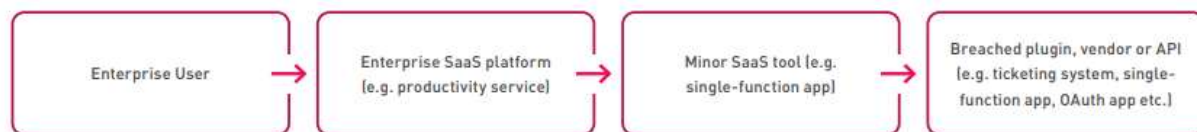


But do you know what they're connected to?



How prevalent are SaaS breaches?

- SaaS Supply Chain attacks
 - 98% of org. globally linked to compromised 3rd party vendors ¹
- SaaS Data Leakage
 - 81% of org. Experienced data exposure due to SaaS apps ¹
- SaaS Misconfiguration
 - 43% of org. experience security incidents directly traced to SaaS misconfiguration ¹



Example of SaaS Interconnections in a Fourth-Party Supply Chain Attack

- ...In 2023, more than 30 major breaches impacted > 220 millions of people (consumer data or profiles, employee's data) ²

Source:

1. <https://www.checkpoint.com/resources/items/the-cisos-definitive-guide-to-saas-security>
2. <https://cloudsecurityalliance.org/blog/2023/12/22/2024-saas-security-predictions-a-look-at-the-saas-threat-landscape-in-the-year-ahead>

Are most of SSPMs and CASBs sufficient for preventing SaaS breaches?

- CASBs secure User-to-App and In-App Activity
 - API and Inline
- SSPMs focus on App Security Posture and Remediation
 - Access and manage the app: uncover SaaS app settings
- Uncovering SaaS-to-SaaS Connections
- Preventing Risky SaaS-to-SaaS Connections in Real Time




Capability	SSPM	CASB
Shadow IT Discovery	●	●
Posture Management	●	●
Uncover SaaS-to-SaaS Connections	●	●
Security long tail of SaaS apps (inline security)	●	●
Security sanctioned SaaS apps (API-based security)	●	●
Prevent risky SaaS-to-SaaS connections in real time	● *	●

*The vast majority of SSPMs do not prevent Risky SaaS-to-SaaS connections in real time. More on this in the next few pages.

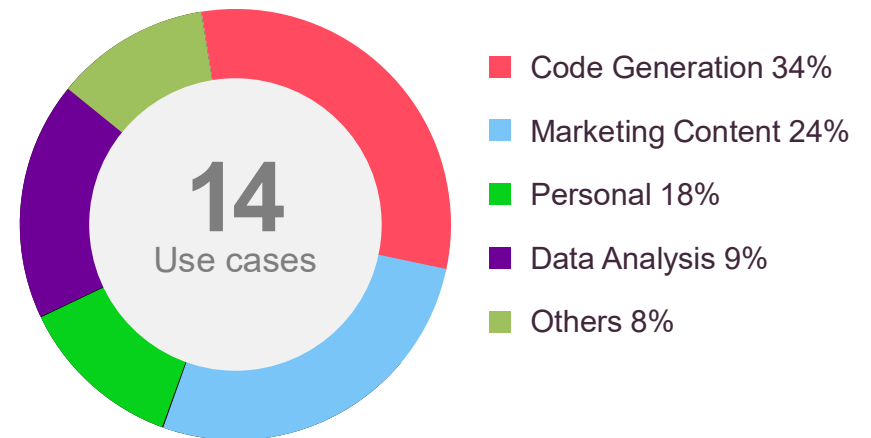
While SSPMs and CASBs complement each other and considerably improve SaaS security, the above blind spots make it challenging for a CISO to maintain comprehensive oversight and control over the organization's entire SaaS landscape.

And what about GenAI apps

Sanctioned and shadow GenAI apps

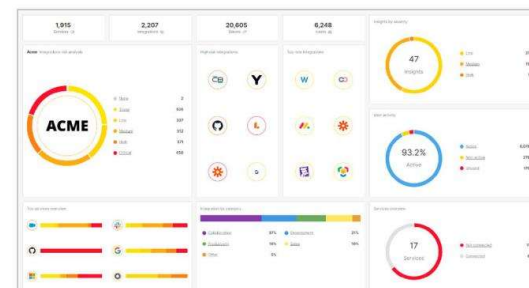
App Name	Risk	Sessions	Users
 Gemini	Low	6,433	3,045
 ChatGPT	Low	4,600	2,258
 Poe	High	1,565	690

Top GenAI app use cases



SaaS Security Must-Haves (1/2)

- Rapid SaaS Application Discovery
- Visibility into SaaS-to-SaaS connections
- Simplified Remediation of Configuration Drift
 - Find applications that require permissions they don't use and revoke those permissions (zero trust for app-to-app communication)
 - Find malicious, breached, abandoned, legacy and deprecated services in your environment
 - Find and fix configuration inefficiencies and configuration drift
 - Find unused SaaS services, stale API keys or tokens, and stale users in those services and disable them.



Prefer rapid SaaS discovery and standardized insights



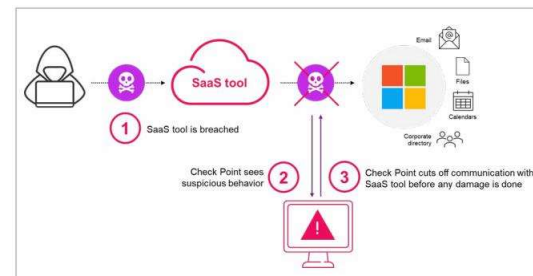
Ensure Visibility into SaaS-to-SaaS Connections

Insight	Risk	Host service
Enforce MFA	Medium	
Configure user consent for applications	Medium	
Force logout session timeout in security settings	Medium	
Check large amount of system administrators	Medium	
Check the number of administrators	Medium	
Finish up installation for connected applications	Medium	
Remove application specific passwords (ASP)	Medium	
Remove legacy apps	Medium	
Remove deprecated apps	Medium	

Seek a Solution that can Identify Security Gaps and Prioritize their Remediation

SaaS Security Must-Haves (2/2)

- Behavior-based Threat Prevention
- Attribute-based SaaS Risk Assessment
- Intuitive Rollout and Management
- Alerts on Changes affecting Regulatory Compliance
- A Zero Trust Approach to App Access



Machine Learning is Essential for Automatically Preventing SaaS-based Threats in Real Time

Description	Risk	Category	Date & time	
Microsoft 365 EmailMarketing integration performed an unexpected action EmailMarketing API key was used to call the method "MailboxAccess". This method is unexpected for this API key, and is of higher risk than normal.	Critical	Potential Data Exfiltration	Jan 6, 2024, ...	More Info
Salesforce integration attempted a method call from an unexpected location	Critical	Security hygiene	Jul 21, 2022, ...	More Info
Malicious API key performed an unexpected action	Critical	Suspicious Service Behavior	Feb 6, 2022, ...	More Info
Potentially dangerous Microsoft app "Upgrade" requires excessive permissions	Critical	Potential Breach	Feb 6, 2022, ...	More Info
Slack application performed an unexpected write	Critical	Phishing Attempt	Feb 6, 2022, ...	More Info

Evaluate the flexibility of a solution to provide fully automated or approval-based prevention

And again, what about GenAI and the need for real-time DLP

Hi, what can I do for you today?



Prompt blocked due to data policy. Please reconsider.

Please prepare a press release with the following data:

First Quarter 2024:

- Total Revenues: \$599 million, a 6% increase year over year
- Security Subscription Revenues: \$263 million, a 15 percent increase YoY
- GAAP Operating Income: \$194 million, representing 32 percent of total revenues
- Non-GAAP Operating Income: \$252 million, representing 42% of total revenues
- GAAP EPS: \$1.60, a 5 percent increase year over year
- Non-GAAP EPS: \$2.04 a 13 percent increase year over year

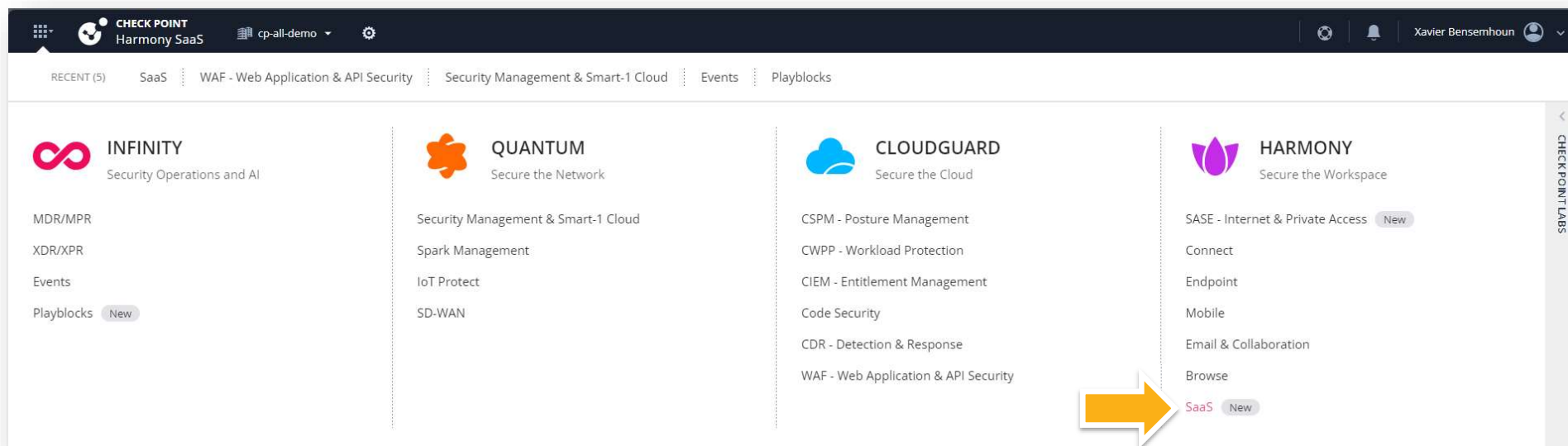
Yours,

Sara Harris
CFO

- AI-powered classification of unstructured data
- Copy/paste restrictions
- Customizable policy
- Keeps intellectual property safe
- Addresses privacy concerns

Place à la démo Harmony SaaS!

👉 <https://portal.checkpoint.com/dashboard/saassecurity#/overview>



Demo Time



Thank you! Merci!

Xavier Bensemhoun

✉ xavierbe@checkpoint.com





CHAPTERS

Connect | Educate | Inspire | Secure

Thank you!

<https://isc2mtl.ca>, communication@isc2mtl.ca, LinkedIn

© 2023 ISC2. All rights reserved. This presentation's images are subject to copyright protection and used under license from third parties. Do not use images from this presentation in other presentations or documents without first consulting with the creative team. The use of copyrighted images outside the licensed scope constitutes copyright infringement and subjects the user to monetary damages and other penalties.