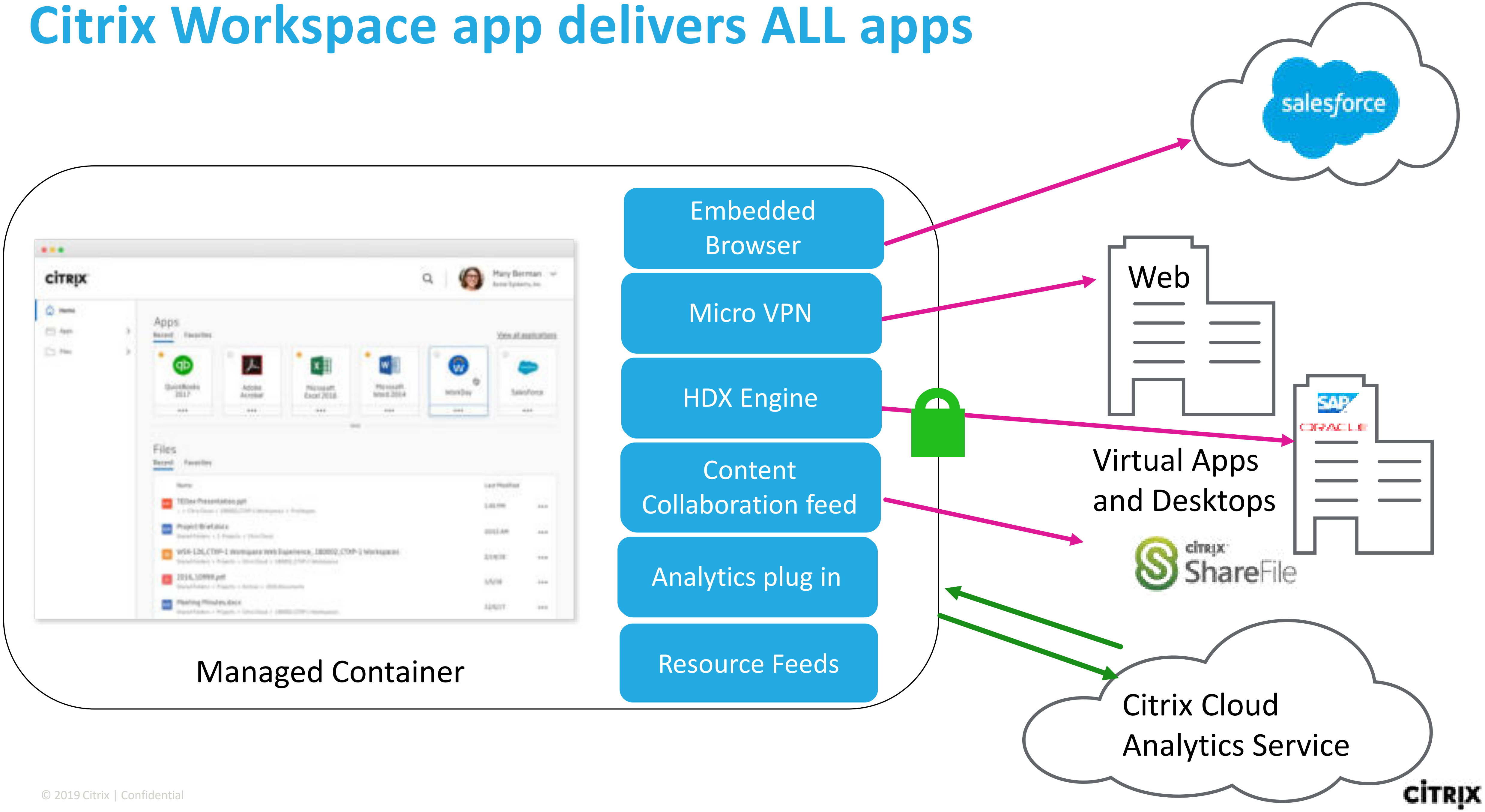
Citrix Security Analytics

Roman Kapitan, Market Development Engineer CZ/SK/HU

Citrix Workspace app delivers ALL apps



Embedded Browser

Micro VPN

HDX Engine

Content Collaboration feed

Analytics plug in

Resource Feeds

Managed Container

Web

Virtual Apps and Desktops

Citrix Cloud Analytics Service

The Rise of Dark AI

State of the Security Industry

- 1.8 million unfilled cybersecurity positions in next 5 years
- 70% of employers are planning to hire more cybersecurity experts
- Money cannot simply solve this problem

Empire Strikes Back!

- 73% of breaches are now financially motivated
- Estimated to be *at least* $1.5 trillion USD economy
- Malware service providers with complex supply chain

Srsly, how smart R attackers?

Subject: Nigerian Astronaut Wants To Come Home

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

AI Villain level #1

- Hybrid between spam and spear-phishing
  - Large volume, highly targeted
  - Context aware
  - 1st and 2nd line - Chatbots
- SNAP_R – Twitter spear-fishing experiment with 30% success rate
  - Rate 6.75 personalized tweets per minute
- In 2016, a Japanese AI program wrote a short novel that made it through the first round for a national literary prize
- Gartner predicts that in 2018, machines will create 20% of business content (report, legal documents)

AI Villain level #2

- **Today –** Cyberattacks are sophisticated, but require a lot of time and effort and attackers can focus on one target only. Attackers are soldiers in the battlefield.
- **Tomorrow –** Attackers are generals leading armies to multiple battlefields. They focus mostly on maintaining/developing the code.

AI Villain level #2

- Cyber Grand Challenge by DARPA
- AI will master evasion and stealth techniques
  - Ability to detect sandboxed environments
  - Ability to blend in to compromised environment
  - Ability to poison good AI
  - “Low and slow” will become more common
- Instead of building simple kill chain, attackers will arm their AIs with arsenal of different weapons
- Deep learning will be able to find new vulnerabilities in open-source projects

Is AI/ML really THE solution?

- Most of companies has adopted it already…
  - …in their marketing materials
- Do you think cybercriminals will just find job at <insert fast food chain name>?

Citrix Analytics – User Behavior

Citrix Workspace

“Employee Experience”

- One Password (SSO)
- Fingerprint *
- Facial Recognition*

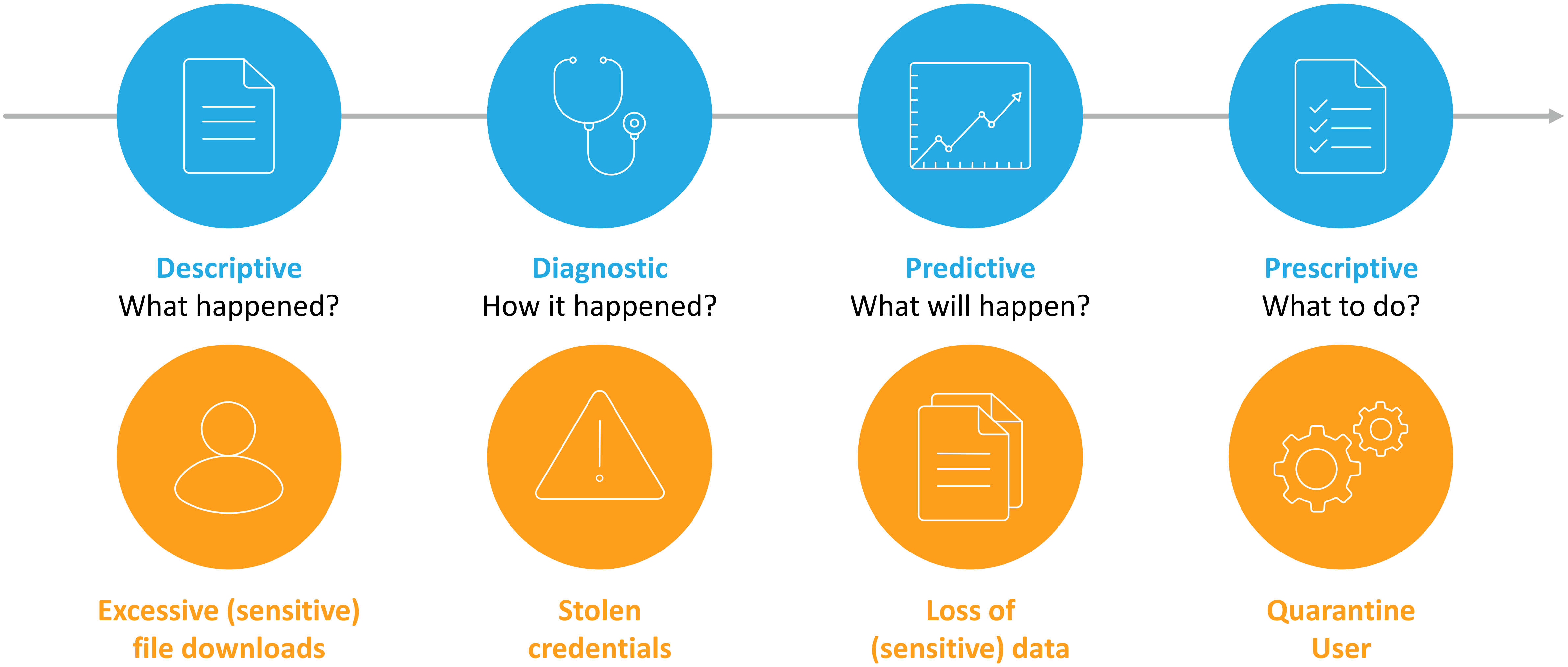
Comprehensive End-to-End security

- Multi-layer Encryption (FIPS)
- Containerized Workflows
- Packet Inspection/Filtering (Layer 7)
- Cloud App Control (SaaS)
- Secure Digital Perimeter
- Citrix Analytics/Machine Learning

* Dependency on operating system and device type

Citrix Security Analytics

What is it?



Descriptive
What happened?

Diagnostic
How it happened?

Predictive
What will happen?

Prescriptive
What to do?

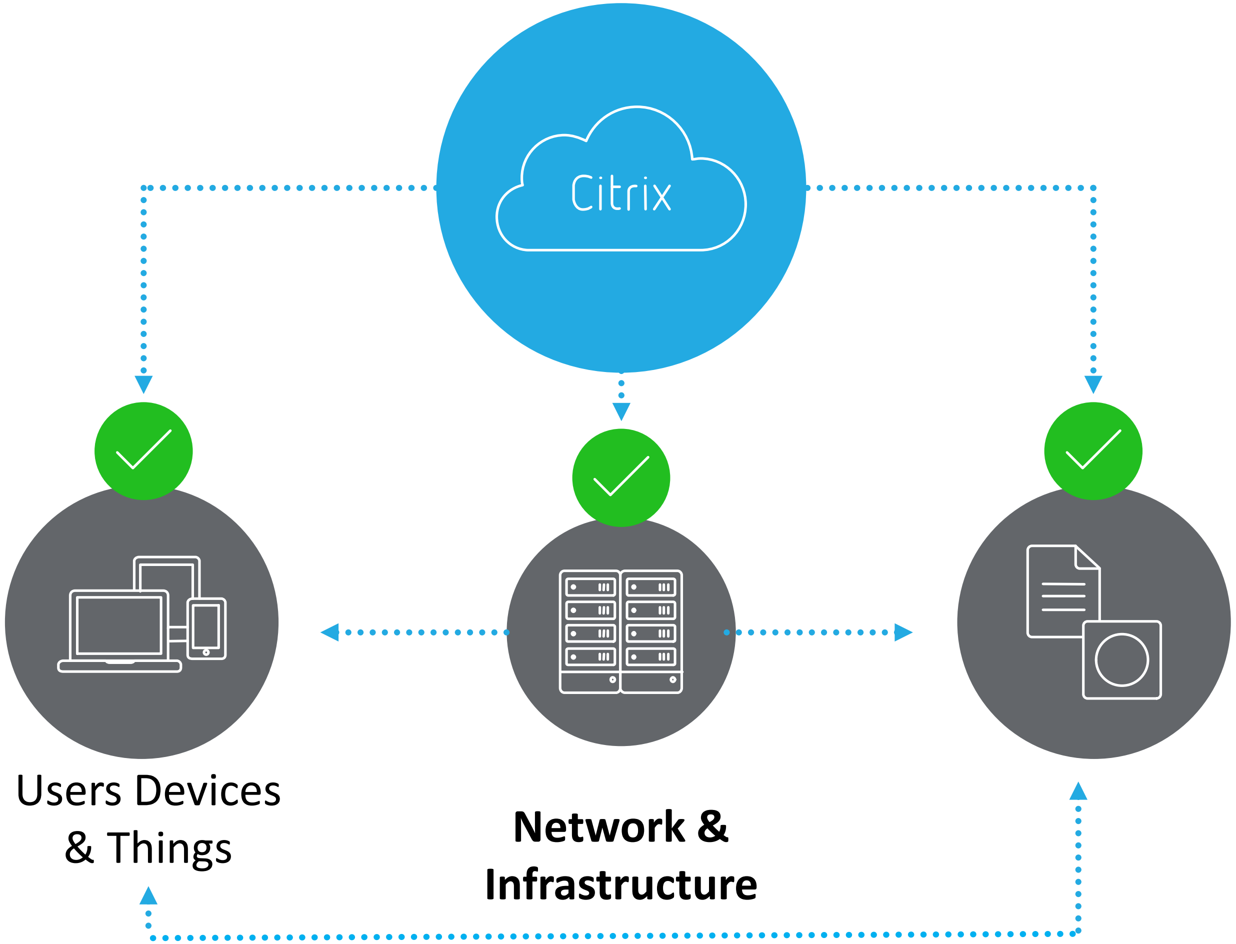
Excessive (sensitive) file downloads

Stolen credentials

Loss of (sensitive) data

Quarantine User

Diverse Comprehensive Data Sources



Behavior | Context | Usage

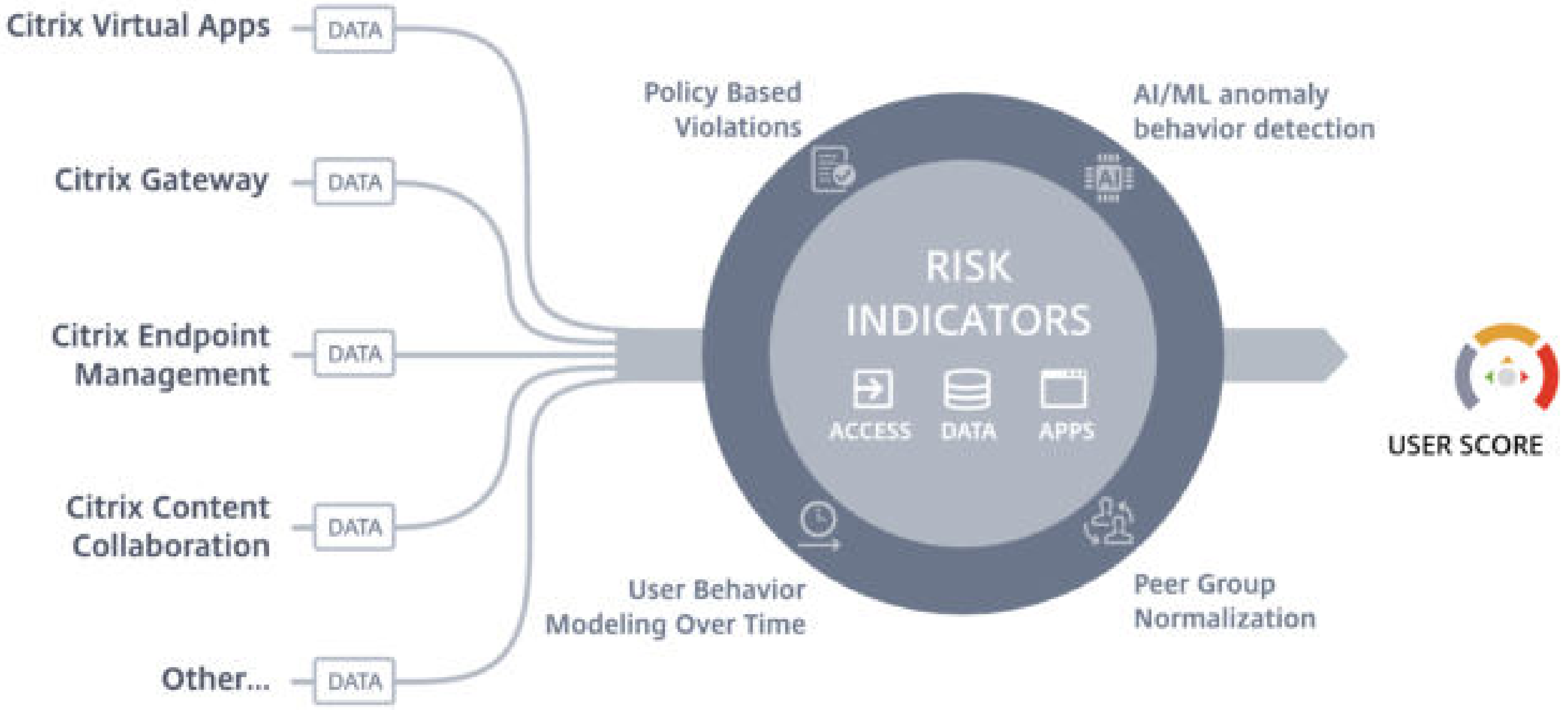
Track Access, Devices & Things
Track user access credentials, devices used for access, location (GPS), Time

Gather Apps & Data
Gather granular Applications & Data usage related information

Tap into Network Traffic
Access to user access data & encrypted network traffic on the wire

Build End-to-end User Behavior with Context
Presence in strategic locations (without any additional instrumentation) for visibility across all the hops from data center to the end-user

HOW THE USER RISK SCORE WORKS



91 - 100 High

Highest risk. Inmediate complex threats or use cases as defined by policies or detected by AI / ML model agregated over a short period of time. **Should be addressed inmediately.**

71 - 90 Medium

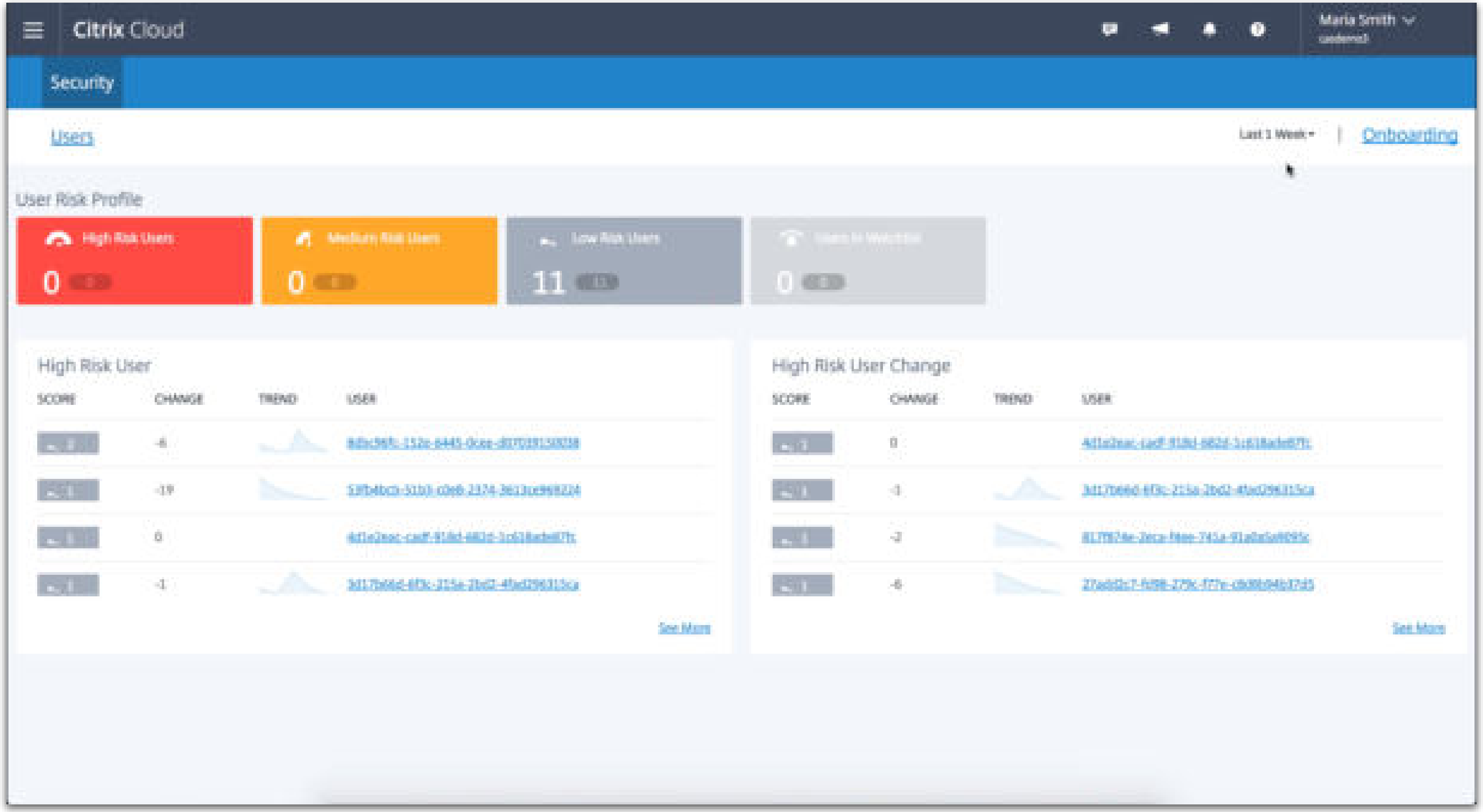
Medium risk. Possible complex threats on the rise or multiple serious violations as defined by policies or detected by AI/ML model found over a short time. **Should be investigated as soon as possible.**

0 - 70 Low

Low risk. Some violations as defined by policies or detected by AI / ML model. Maybe previously high score being reduced over time.

User Behavior Security Analytics

- Detect & mitigate threats from trusted internal users with malicious intent
- Easily identify high risk users with drill-down capabilities on behavior
- Apply corrective actions



User Risk Profile

High Risk Users 0

Medium Risk Users 0

Low Risk Users 11

Users in Watchlist 0

High Risk User

SCORE	CHANGE	TREND	USER
[illegible]	-6		8dbc96fc-152e-6445-0cee-d07039130038
[illegible]	-19		53fb4bcb-51b3-c0eb-2374-3613ce968224
[illegible]	0		4d1e2eac-cadf-918d-682d-1c618adeb87fc
[illegible]	-1		3d17b66d-6f3c-215a-2bd2-4fad296315ca

See More

High Risk User Change

SCORE	CHANGE	TREND	USER
[illegible]	0		4d1e2eac-cadf-918d-682d-1c618ade87fc
[illegible]	-1		3d17b66d-6f3c-215a-2bd2-4fad296315ca
[illegible]	-2		817f874e-2eca-f4ee-741a-91a0a5a9095c
[illegible]	-6		27addc7-fd98-279c-f77e-c8d8b94b3745

See More

Citrix Analytics is Unique

Sense

1

TURN-KEY

Turn-key data collection

User behavior & context based

Analyze

2

ACCURATE

Correlation from multiple vantage points for accuracy

Machine Learning based models

Respond

3

AUTONOMOUS

Closed-loop autonomous actions

Granular policy control

CITRIX®