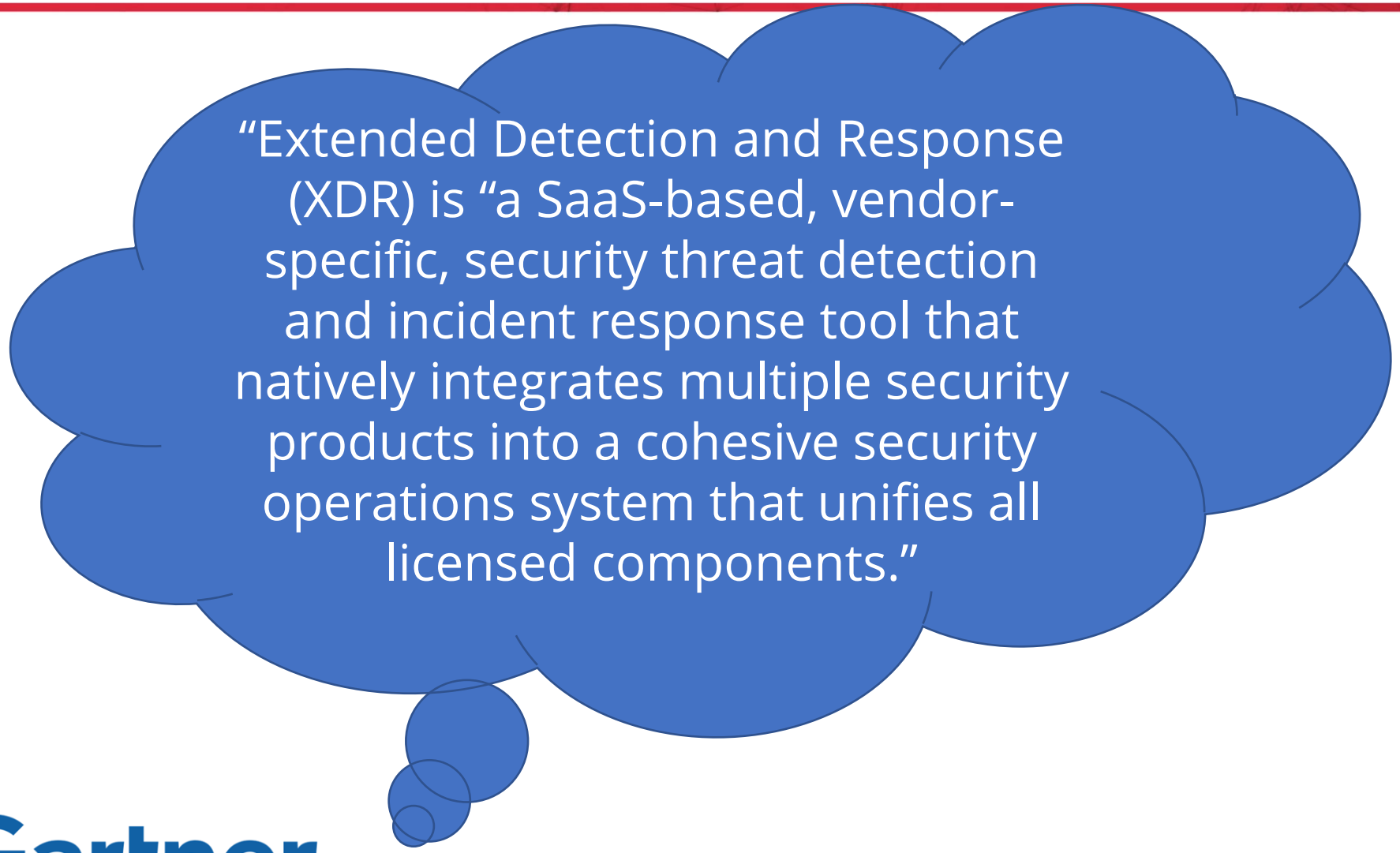
COMGUARD
communication security

InsightIDR – SIEM nebo XDR?

Jakub Mazal / Senior Technical Consultant

Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.

Gartner®


“Extended Detection and Response (XDR) is “a SaaS-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components.”

Gartner®

Historie InsightIDR

- 2013 – Rapid7 odstartoval vývoj InsightIDR
- 2015 – Produkt uveden na trh
- 2017 – Poprvé v GARTNER jako SIEM
- 2018 – CTO Palo Alto Networks poprvé použil výraz XDR

https://www.rapid7.com/blog/post/2021/11/09/insightidr-was-xdr-before-xdr-was-even-a-thing-an-origin-story/

Source: Gartner (February 2020)

InsightIDR:

- Běží v cloudu s garantovanou dostupností a podporou.
- Sbírá logy z různých technologií a dále je zpracovává a uchovává.
- Má endpoint agenta sbírajícího informace, který umožňuje provádět reakce.
- Lze nasadit a nakonfigurovat **během několika dnů.**
- Vše probíhá přes webovém rozhraní.

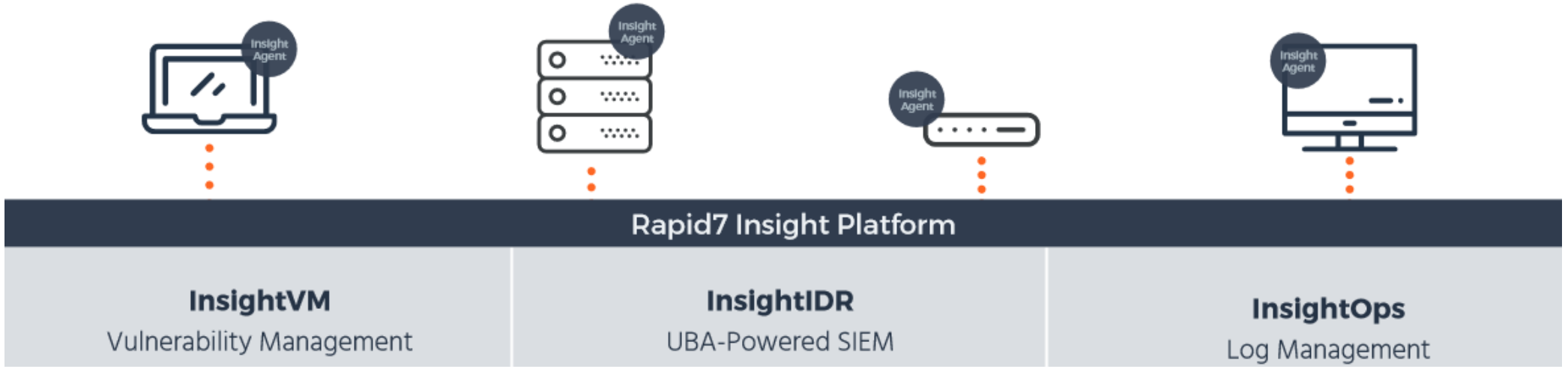
- **Jeho cílem je rychlé vyšetřování incidentů a reakce na ně**

Komponenty

- User Behavior Analytics
- Attacker Behavior Analytics
- Endpoint Detection and Visibility
- Network Traffic Analysis
- Centralized Log Management
- Visual Investigation Timeline
- Deception Technology
- File Integrity Monitoring (FIM)
- Automation
- Custom parsing rules

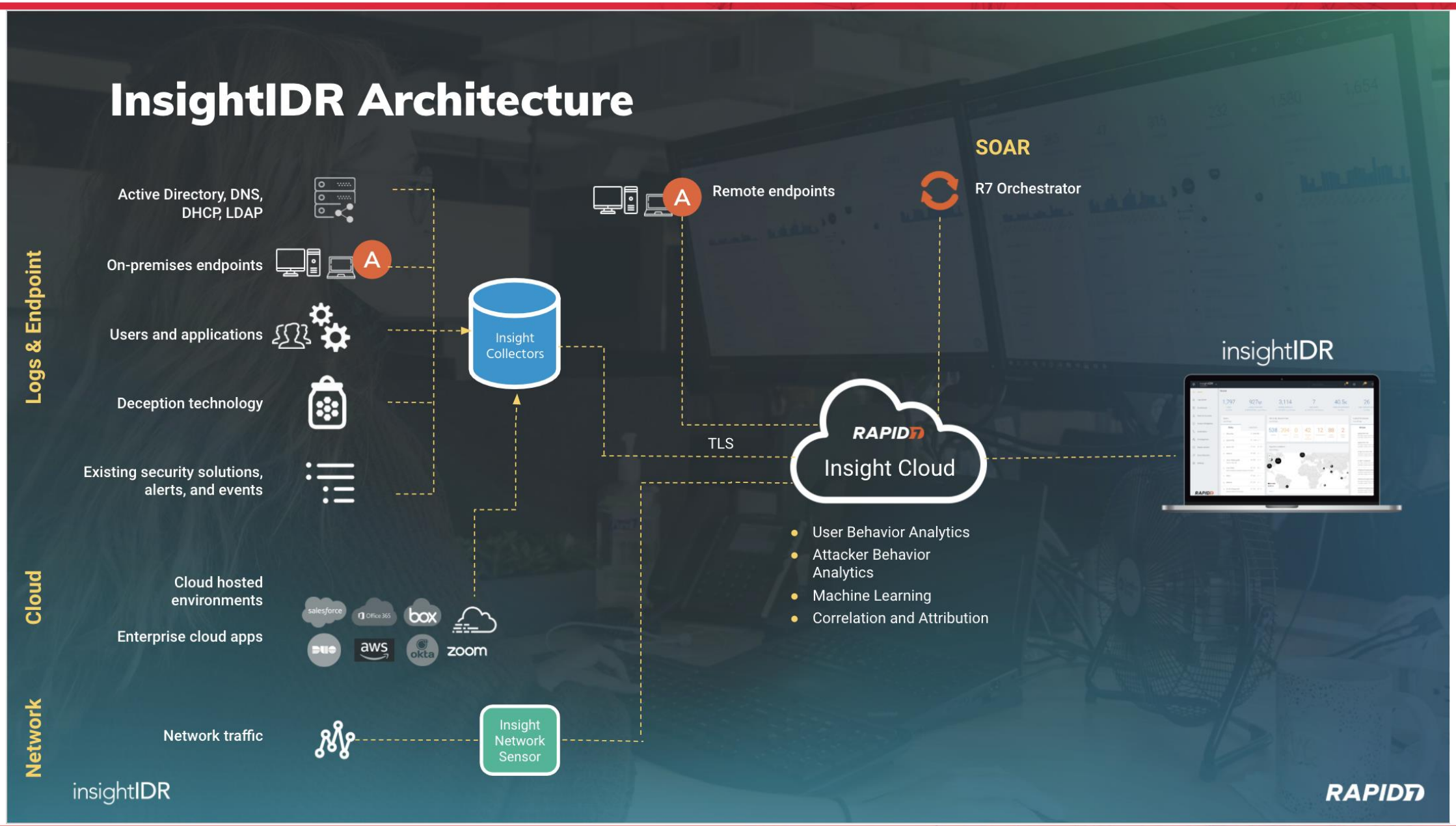
Insight Agent

- One Agent to Rule Them All (Jeden Agent vládne všem)
  - Produktům na platformě Insight



Insight Agent

- Local user activity
- Windows logon activity
- Event log tampering
- Process hash identification
- Process commonality analysis
- Process malware analysis
- File integrity monitoring


InsightIDR Architecture
Logs & Endpoint
Active Directory, DNS, DHCP, LDAP
On-premises endpoints
Users and applications
Deception technology
Existing security solutions, alerts, and events
Cloud
Cloud hosted environments
Enterprise cloud apps
Network
Network traffic
Insight Collectors
Insight Network Sensor
Remote endpoints
SOAR
R7 Orchestrator
TLS
RAPID7
Insight Cloud
User Behavior Analytics
Attacker Behavior Analytics
Machine Learning
Correlation and Attribution
insightIDR
insightIDR
RAPID7

InsightIDR: It was XDR before XDR was even a thing

COMGUARD
communication security

Ukázka z Kompetenčního centra COMGUARD

InsighIDR – Investigace incidentu

Další funkcionality

- Insight Network Sensor
  - Síťová sonda od Rapid7
- Insight Orchestrator
  - Možnost definice workflow při detekci hrozby
  - Definice automatizovaných akcí
- Honeypots, Honey users, Honey files
  - Předpřipravené balíčky
- Možnost napojení na SOAR – InsightConnect

COMGUARD
communication security

Děkuji za pozornost

jakub.mazal@comguard.cz
+420 777 366 338