

# Logging and Security

---

- Logging is one of the most important parts of secure systems
- Documents security related incidents
- Can be streamed to SIEM tools for further analytics and mitigation

# Security Related Incidents

---

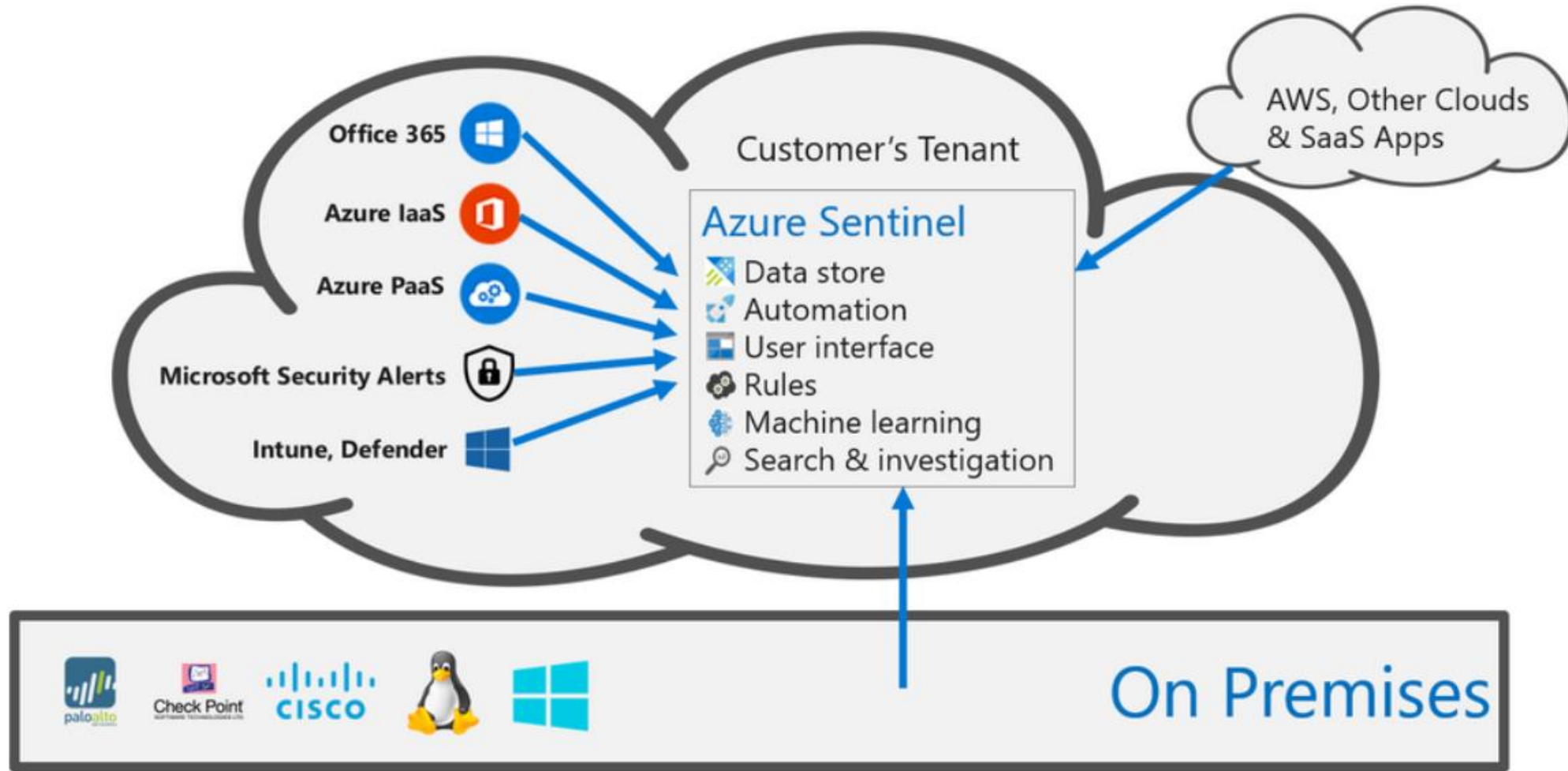
- Make sure to log security related events such as:
  - Unauthorized access
  - SQL injection attack
  - Excessive load on the system
  - And more...

# SIEM Tools

---

- Security Information and Event Management
- Offer holistic view of the organization's information security
- Connect to various sources to get security information
- Analyze, alert, mitigate
- Can be on-prem or in the cloud

# SIEM Tools



# SIEM Tools

---

- Add your own logs as a data source to the organization's SIEM
- Help build a unified view of the information security in the organization