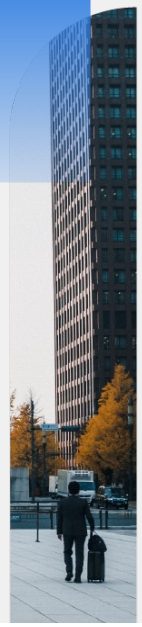
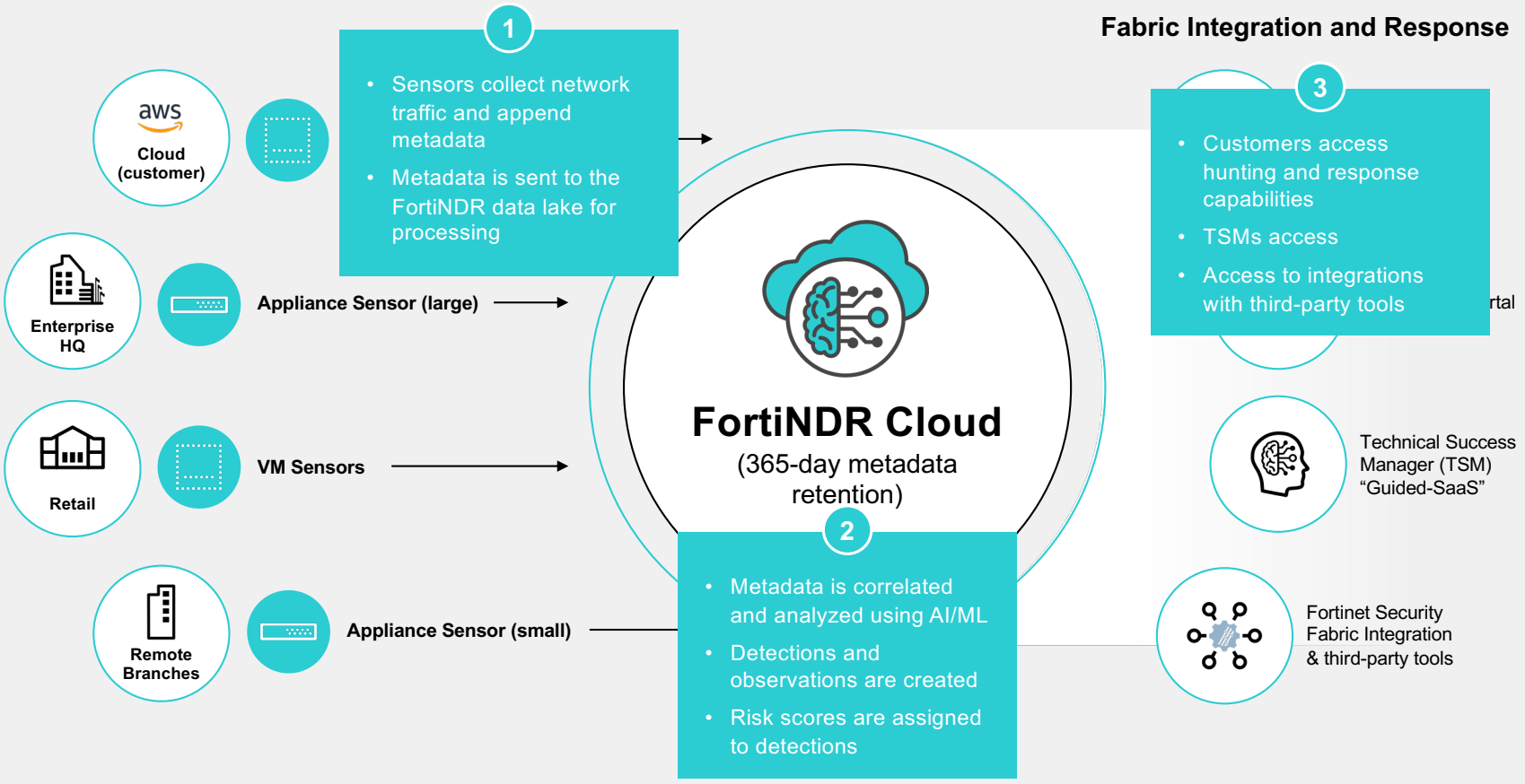
FortiNDR Network Detection and Response

Tony Molica, Systems Engineer, Northeast USA

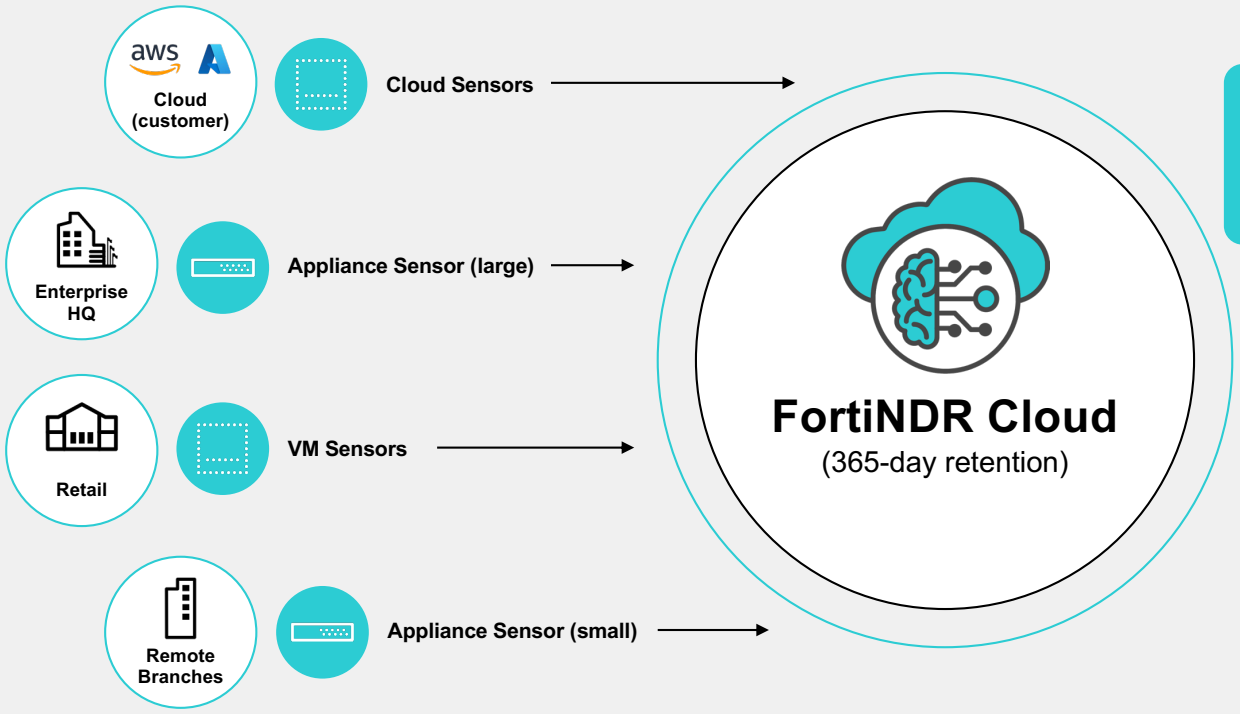


October 2024

FortiNDR In Action



Technical Success Managers In-Depth

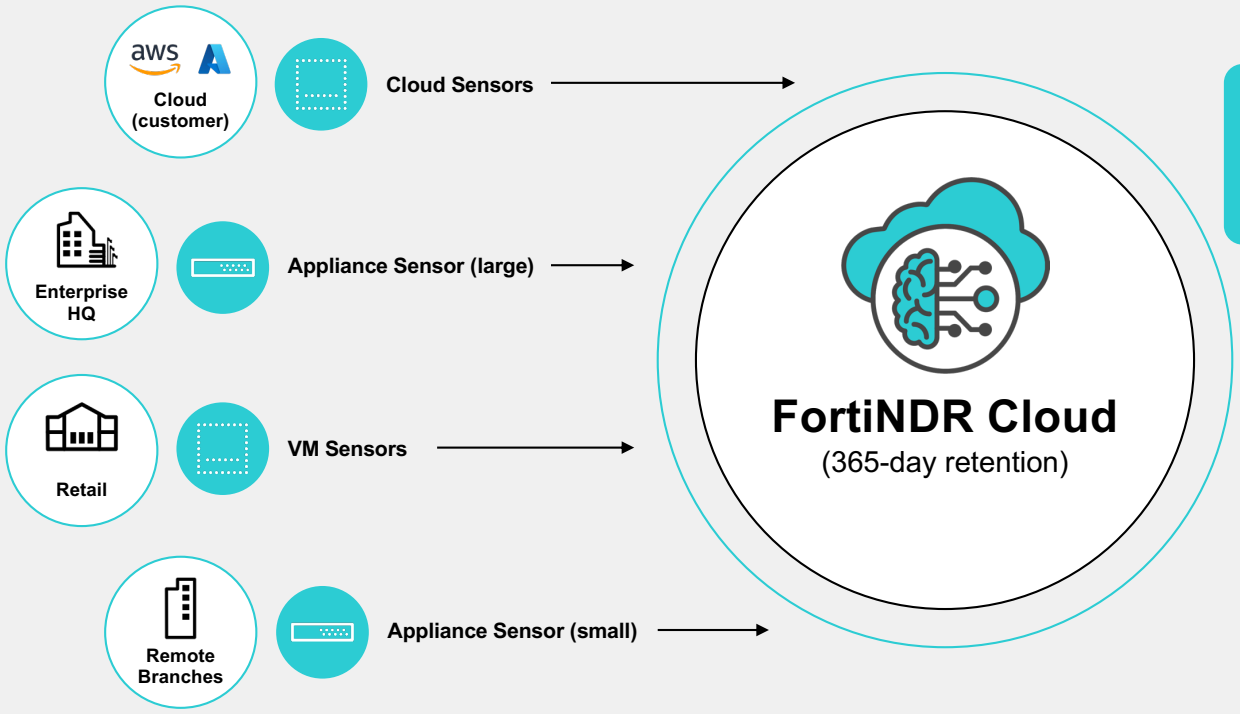


Technical Success Manager (TSM) "Guided-SaaS"

Experienced incident responders & security analysts that:

- Enable teams
- Set up and optimize deployments
- Drive industry best practices
- Provide advice when it matters

FortiGuard Applied Threat Research In-Depth



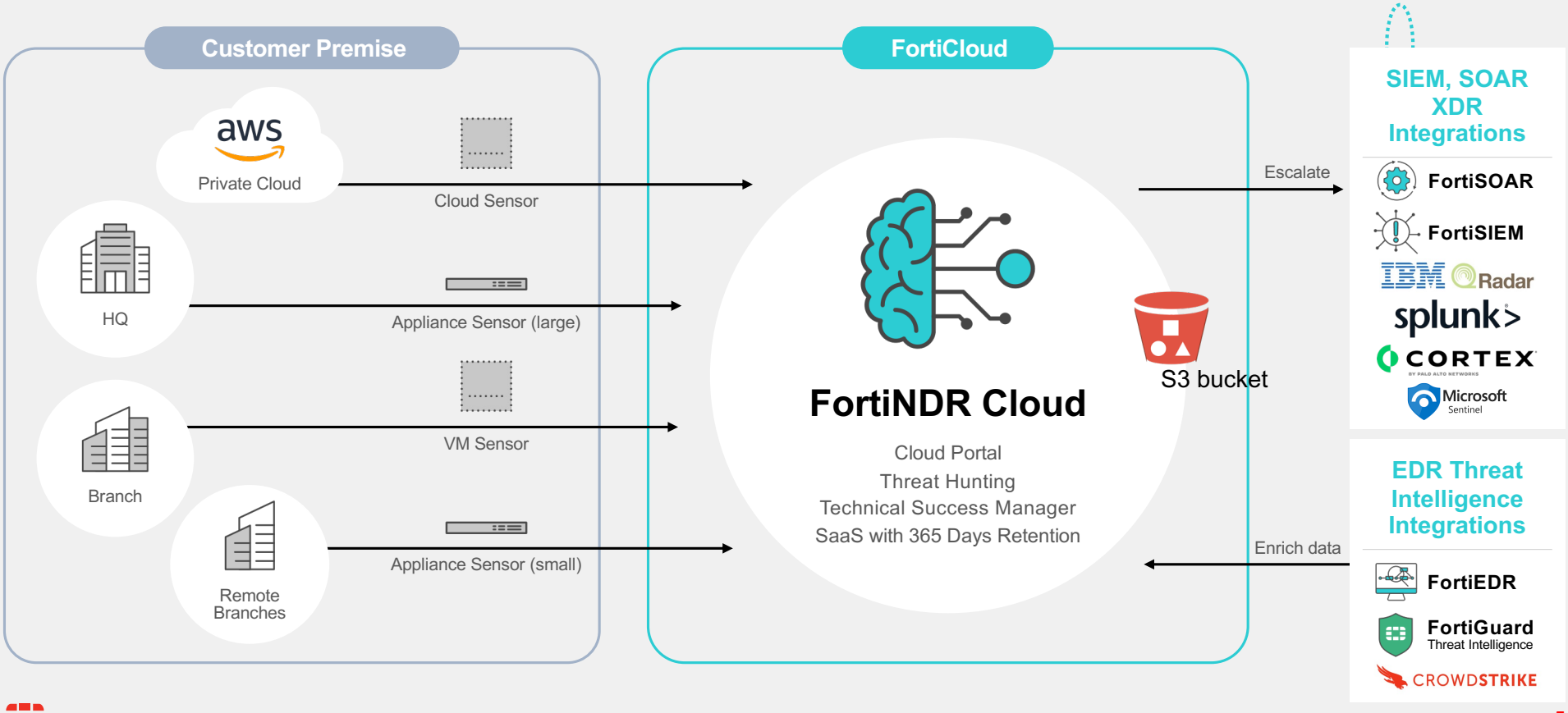
FortiGuard Applied Threat Research (ATR)

Complements FortiNDR Cloud threat intel and detection engines:

- Create low false positive/high-fidelity detections
- Create AI/ML-based observations
- Continuous detection tuning
- Incorporating FortiGuard Labs outbreak alerts

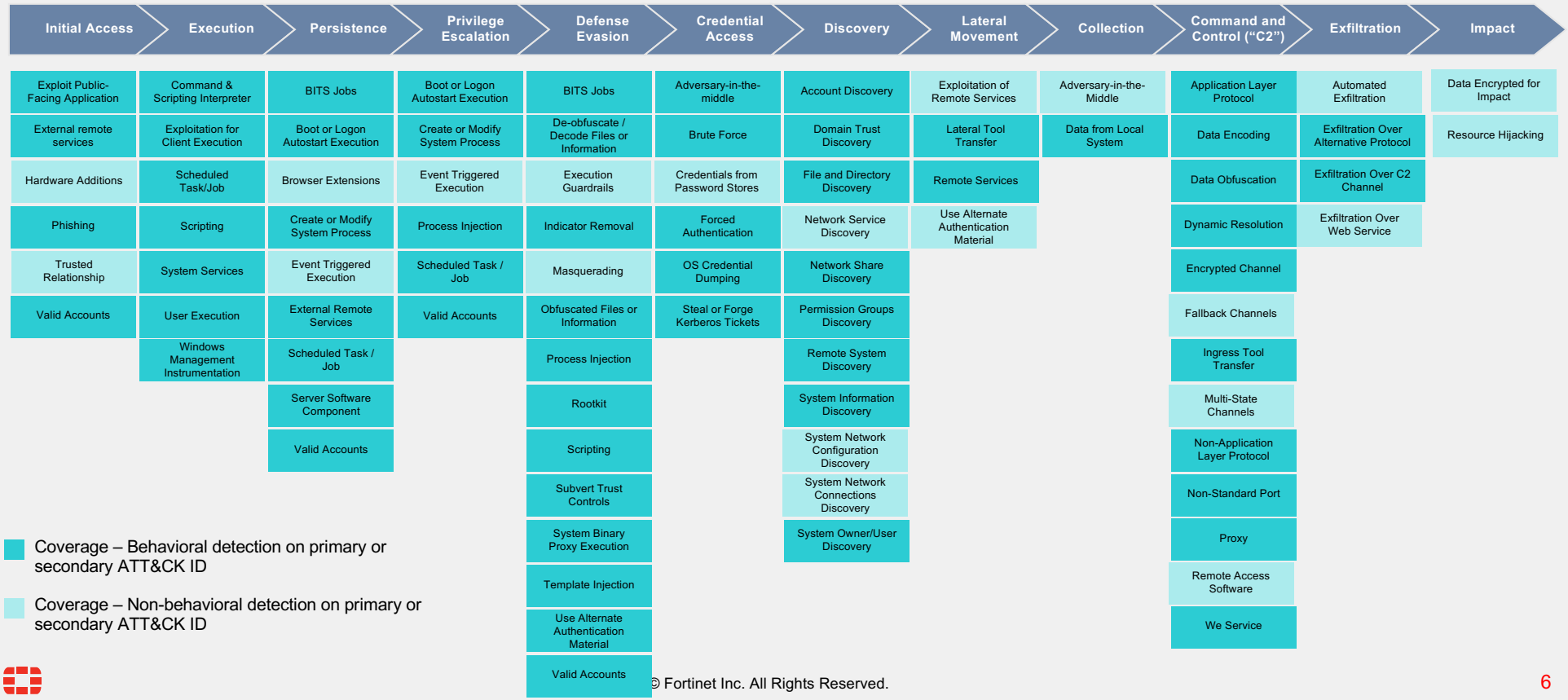
FortiNDR Cloud Integration Capabilities

SaaS deployment



Over 90% MITRE ATT&CK Coverage

All **FortiNDR Cloud** detections are mapped to the MITRE ATT&CK lifecycle with actionable, expert guidance



Coverage – Behavioral detection on primary or secondary ATT&CK ID

Coverage – Non-behavioral detection on primary or secondary ATT&CK ID

FortiNDR OT Protocols Coverage

Protocols and Vendor Applications Supported (as of 2024.5 release)

- 3S-Smart
- Allen-Bradley
- BACNet
- Beckhoff
- Broadwin
- CODESYS
- CitectSCADA
- Cogent
- DATAC
- DNP3
- ETHERNET_IP
- GE
- IEC104
- Iconics
- Measuresoft
- Microsys
- MODBUS
- Movicon
- Moxa
- mySCADA
- OPC
- PcVue
- Promotic
- RSLogix
- RealFlex
- Rockwell
- Schneider
- Schweitzer Engineering
- Siemens
- Sunway
- Tridium Niagara
- Sielco
- Sinapsi
- ScadaTex Scadaphone
- S7

Green = investigation/query support
Blue = IDS signatures support

Useful Links

Video Demo of FortiNDR Cloud. https://video.fortinet.com/products/fortindrcloud

Documentation: https://docs.fortinet.com/product/fortindr-cloud/

Fortinet's worldwide Community: https://community.fortinet.com/

Fortiguard: https://www.fortiguard.com/.

Fortinet Developer Network: https://fndn.Fortinet.net


FORTINET