

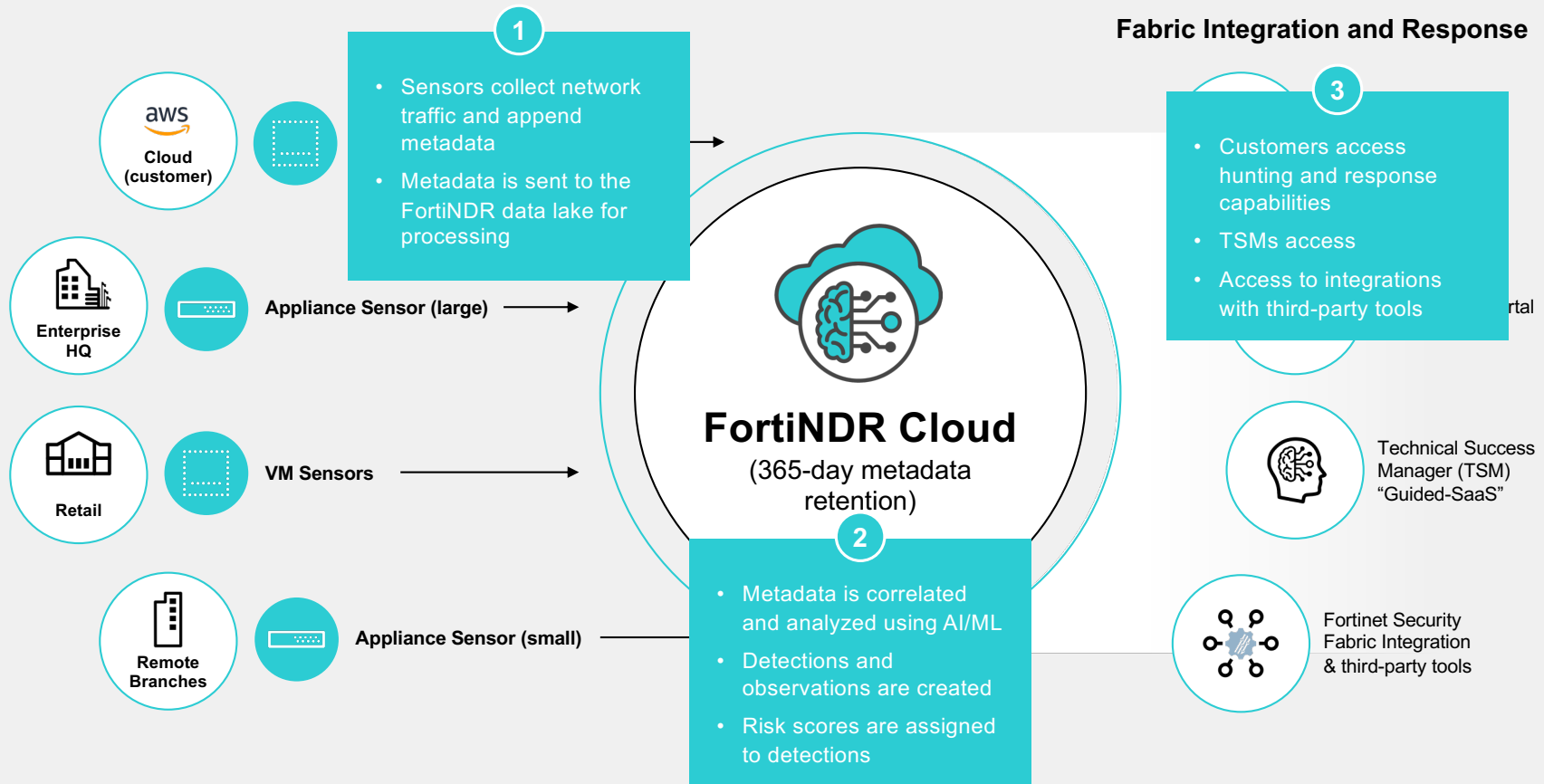


FortiNDR Network Detection and Response

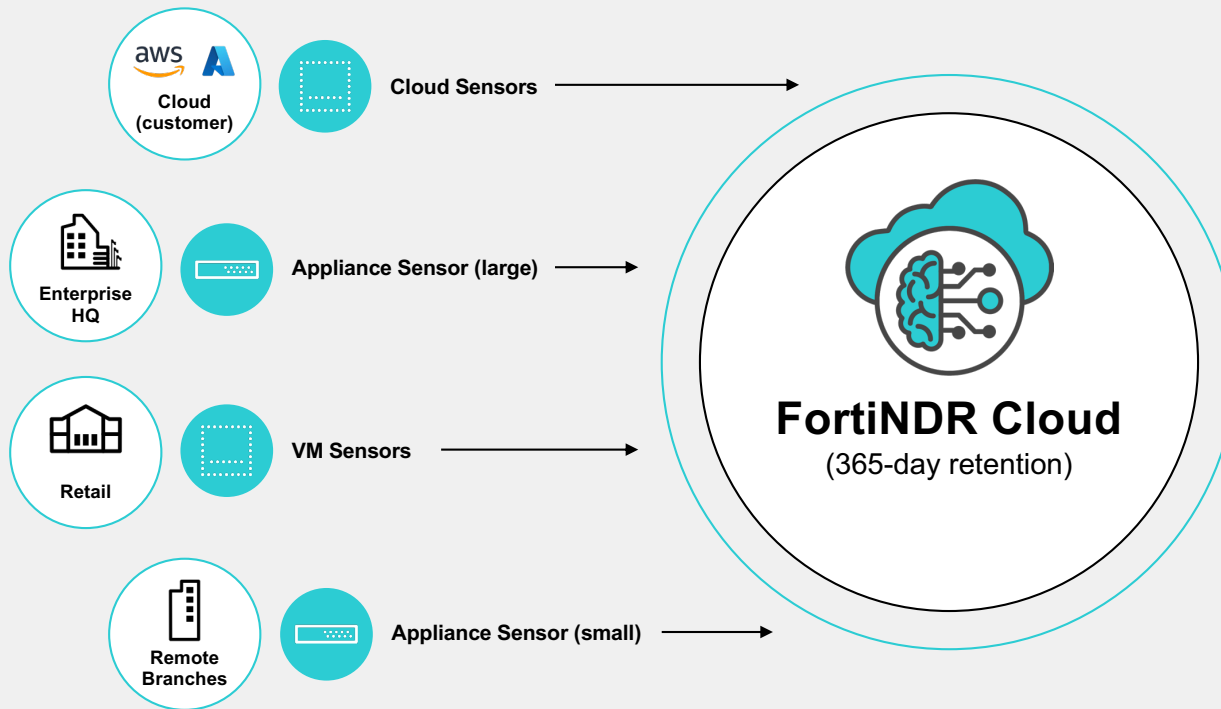
Tony Molica, Systems Engineer, Northeast USA

October 2024

FortiNDR In Action



Technical Success Managers In-Depth



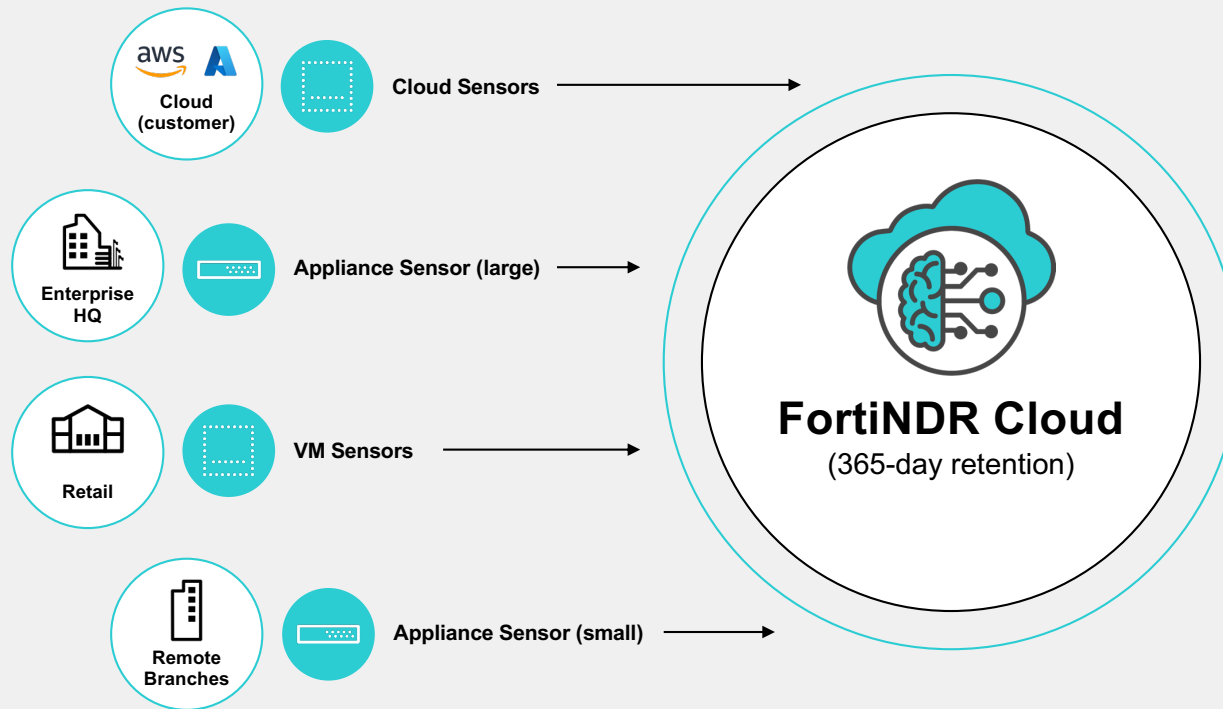
**Technical Success Manager
(TSM) “Guided-SaaS”**

**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)

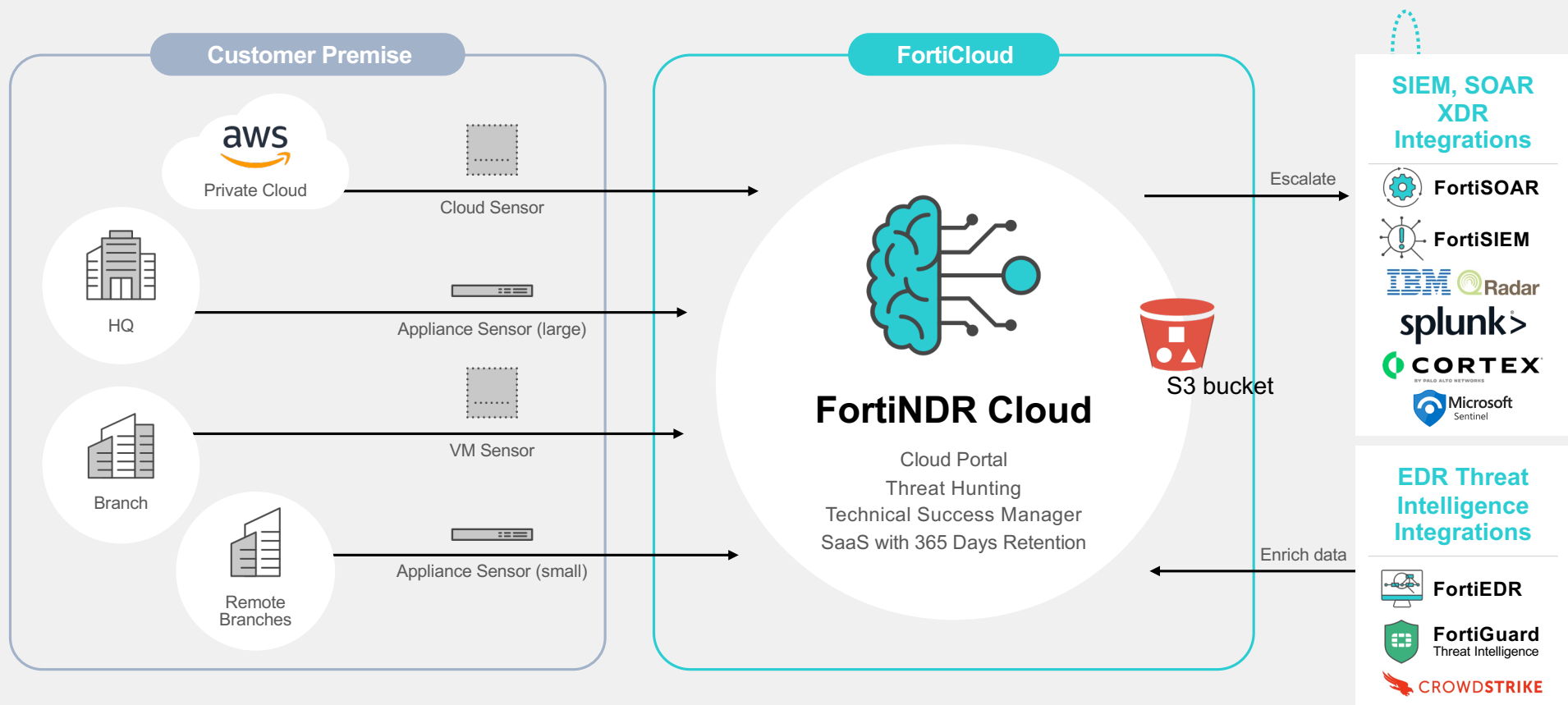
Complements FortiNDR Cloud threat intel and detection engines:

- 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control ("C2")	Exfiltration	Impact
Exploit Public-Facing Application	Command & Scripting Interpreter	BITS Jobs	Boot or Logon Autostart Execution	BITS Jobs	Adversary-in-the-middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
External remote services	Exploitation for Client Execution	Boot or Logon Autostart Execution	Create or Modify System Process	De-obfuscate / Decode Files or Information	Brute Force	Domain Trust Discovery	Lateral Tool Transfer	Data from Local System	Data Encoding	Exfiltration Over Alternative Protocol	Resource Hijacking
Hardware Additions	Scheduled Task/Job	Browser Extensions	Event Triggered Execution	Execution Guardrails	Credentials from Password Stores	File and Directory Discovery	Remote Services		Data Obfuscation	Exfiltration Over C2 Channel	
Phishing	Scripting	Create or Modify System Process	Process Injection	Indicator Removal	Forced Authentication	Network Service Discovery	Use Alternate Authentication Material		Dynamic Resolution	Exfiltration Over Web Service	
Trusted Relationship	System Services	Event Triggered Execution	Scheduled Task / Job	Masquerading	OS Credential Dumping	Network Share Discovery			Encrypted Channel		
Valid Accounts	User Execution	External Remote Services	Valid Accounts	Obfuscated Files or Information	Steal or Forge Kerberos Tickets	Permission Groups Discovery			Fallback Channels		
	Windows Management Instrumentation	Scheduled Task / Job		Process Injection		Remote System Discovery			Ingress Tool Transfer		
		Server Software Component		Rootkit		System Information Discovery			Multi-State Channels		
		Valid Accounts		Scripting		System Network Configuration Discovery			Non-Application Layer Protocol		
				Subvert Trust Controls		System Network Connections Discovery			Non-Standard Port		
				System Binary Proxy Execution		System Owner/User Discovery			Proxy		
				Template Injection					Remote Access Software		
				Use Alternate Authentication Material					We Service		
				Valid Accounts							

- 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®