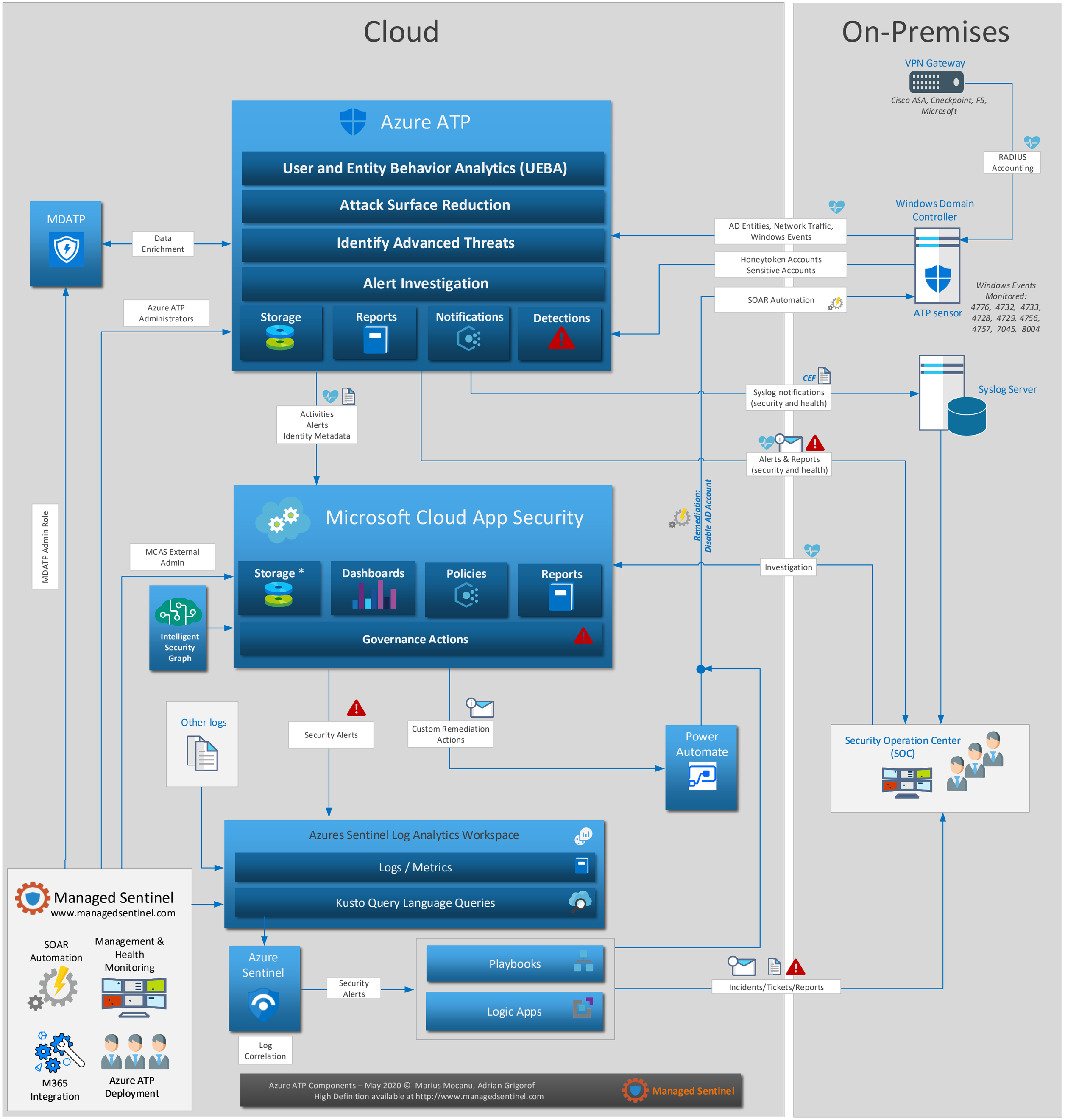
Cloud
On-Premises
Azure ATP
User and Entity Behavior Analytics (UEBA)
Attack Surface Reduction
Identify Advanced Threats
Alert Investigation
Storage
Reports
Notifications
Detections
MDATP
Data Enrichment
Azure ATP Administrators
MDATP Admin Role
VPN Gateway
Cisco ASA, Checkpoint, F5, Microsoft
RADIUS Accounting
Windows Domain Controller
AD Entities, Network Traffic, Windows Events
Honeytoken Accounts Sensitive Accounts
SOAR Automation
ATP sensor
Windows Events Monitored: 4776, 4732, 4733, 4728, 4729, 4756, 4757, 7045, 8004
CEF
Syslog notifications (security and health)
Syslog Server
Activities Alerts Identity Metadata
Alerts & Reports (security and health)
Remediation: Disable AD Account
Microsoft Cloud App Security
MCAS External Admin
Storage *
Dashboards
Policies
Reports
Intelligent Security Graph
Governance Actions
Investigation
Other logs
Security Alerts
Custom Remediation Actions
Power Automate
Security Operation Center (SOC)
Azures Sentinel Log Analytics Workspace
Logs / Metrics
Kusto Query Language Queries
Managed Sentinel
www.managedsentinel.com
SOAR Automation
Management & Health Monitoring
M365 Integration
Azure ATP Deployment
Azure Sentinel
Log Correlation
Security Alerts
Playbooks
Logic Apps
Incidents/Tickets/Reports
Azure ATP Components – May 2020 © Marius Mocanu, Adrian Grigorof
High Definition available at http://www.managedsentinel.com
Managed Sentinel