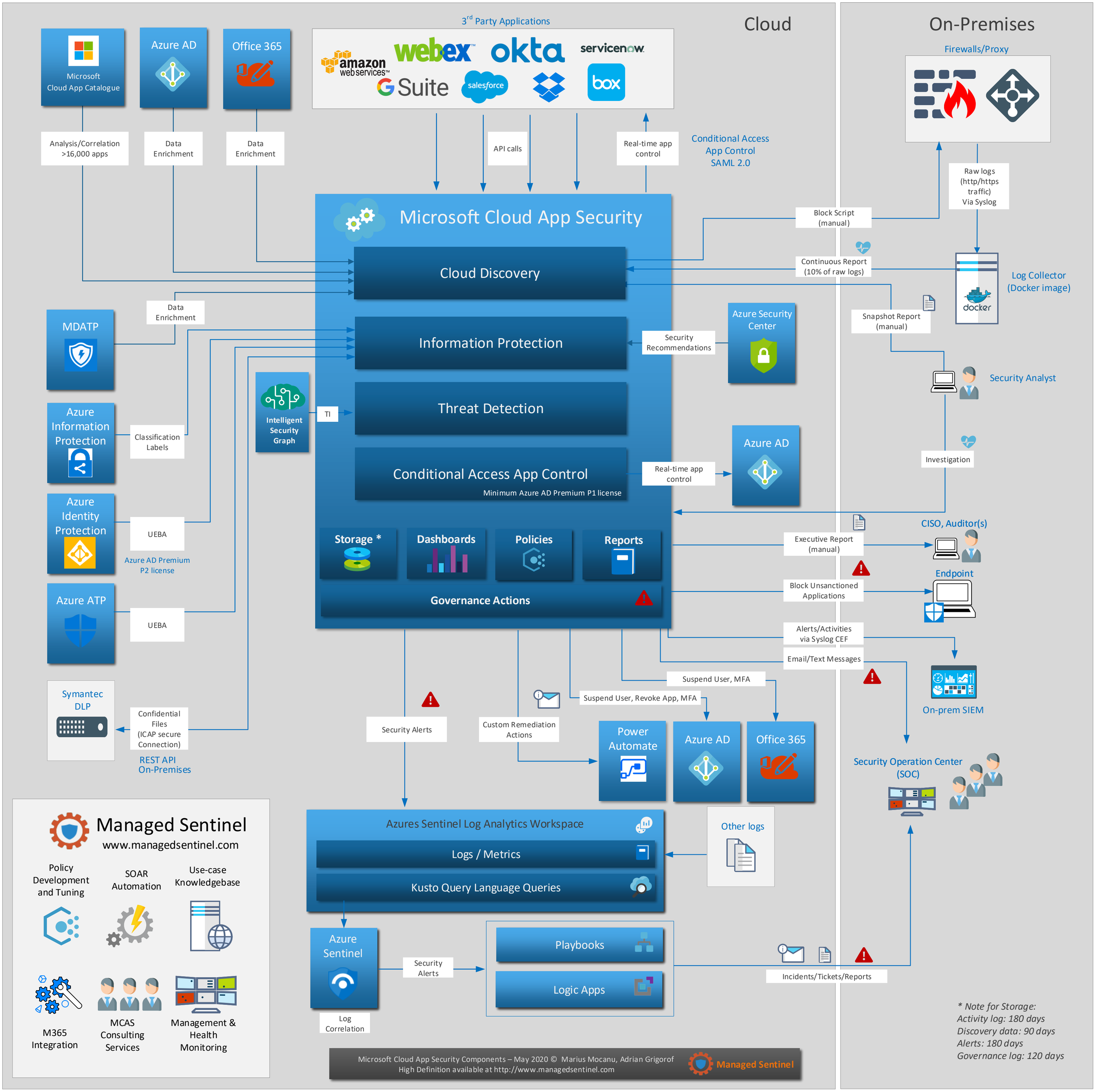
Cloud
On-Premises
3rd Party Applications
Microsoft Cloud App Security
Cloud Discovery
Information Protection
Threat Detection
Conditional Access App Control
Minimum Azure AD Premium P1 license
Storage *
Dashboards
Policies
Reports
Governance Actions
Microsoft Cloud App Security Components – May 2020 © Marius Mocanu, Adrian Grigorof
High Definition available at http://www.managedsentinel.com
Managed Sentinel
Microsoft Cloud App Security Components – May 2020 © Marius Mocanu, Adrian Grigorof
High Definition available at http://www.managedsentinel.com
Managed Sentinel
www.managedsentinel.com
Policy Development and Tuning
SOAR Automation
Use-case Knowledgebase
M365 Integration
MCAS Consulting Services
Management & Health Monitoring
Microsoft Cloud App Catalogue
Azure AD
Office 365
Analysis/Correlation >16,000 apps
Data Enrichment
Data Enrichment
API calls
Real-time app control
Conditional Access App Control SAML 2.0
Firewalls/Proxy
Raw logs (http/https traffic) Via Syslog
Block Script (manual)
Continuous Report (10% of raw logs)
Log Collector (Docker image)
Snapshot Report (manual)
Security Analyst
Data Enrichment
MDATP
Azure Security Center
Security Recommendations
Intelligent Security Graph
TI
Azure Information Protection
Classification Labels
Azure AD
Real-time app control
Investigation
Azure Identity Protection
UEBA
Azure AD Premium P2 license
CISO, Auditor(s)
Executive Report (manual)
Endpoint
Azure ATP
UEBA
Block Unsanctioned Applications
Alerts/Activities via Syslog CEF
Email/Text Messages
Suspend User, MFA
Suspend User, Revoke App, MFA
On-prem SIEM
Symantec DLP
Confidential Files (ICAP secure Connection)
REST API On-Premises
Security Alerts
Custom Remediation Actions
Power Automate
Azure AD
Office 365
Security Operation Center (SOC)
Azures Sentinel Log Analytics Workspace
Logs / Metrics
Kusto Query Language Queries
Other logs
Azure Sentinel
Log Correlation
Security Alerts
Playbooks
Logic Apps
Incidents/Tickets/Reports
* Note for Storage:
Activity log: 180 days
Discovery data: 90 days
Alerts: 180 days
Governance log: 120 days