Bezpečnost hybridního datového centra

Daniel Hejda
ATOM Team Members
by KPCS

- Proč řešit ochranu hybridního cloudu
- Jak vypadá ochrana hybridního cloudu
- Azure Monitor
- Azure Security Center
- Windows Defender ATP
- Azure Sentinel

Daniel Hejda

13 years of experience in IT Operations and Security

- Role at KPCS CZ, s.r.o.
  - Chief Information Security Officer
  - External Data Protection Officer
  - ATOM Security Engineer
    - Microsoft Award Security Solution 2018 Winner
    - IDG Security Solution 2017 Winner
- Security
  - CEHv10: Certified Ethical Hacker v10
  - PECB ISO/IEC 27001 Lead Auditor
- Microsoft
  - MVP: Cloud and Datacenter Management
  - Azure Security and Solution Architect
  - MCC: Microsoft Community Contributor
  - MCSD: Azure Solution Architect
  - MCSE: Cloud Platform and Infrastructure, Productivity, Messaging, Server Infrastructure
  - MCSA: Office365, Windows Server
- Skills
  - Microsoft Azure Cloud Architect
  - Risk Assessment (CyberSec, InfoSec)
  - Security Auditor and Advisor (ISO2700x, ISO9001)
  - GDPR and Process Auditor
  - Penetration tester and Ethical Hacker
  - Red/Blue tester (Ethical Hacker)
  - Security Analytics and Threat Investigation
  - Speaker and Trainer

Proč zrovna bezpečnost hybridního cloudu?

Základní problémy bezpečnosti hybridního cloudu

- Cloudová řešení jsou budována stejně jako lokální
  - Koncept lokálních datových center není efektivně aplikovatelný na cloudová datová centra, nebo hybridní cloudy
- Ochrana by Design / by Default
  - Komponenty v Azure a Office365/M365 jsou využívány tak, jak je připravil provozovatel a otevřeny celému světu
  - Není dbáno na hardening služeb ze strany společností, tedy na ochranu přístupu a ochranu dat (ochrana na perimetru cloudu je maximální)
  - Nejsou aktivovány sondy pro detekci potencionálních problémů
- Špatné, staré nebo žádné standardy a postupy, tedy Governance
  - Neznalost prostředí, služeb a dalších komponent vede ke zbytečně nadměrným nákladům za provoz datového centra (zbytečně vysoké TCO)
- Díky komplexnosti prostředí se ztrácí zaměření na detail
  - Často jsou využívány služby, tak jak leží a běží, je vynucen jakýsi „standard“, který však není vynucen, kontrolován, udržován a zlepšován

Jaká úskalí nám přináší hybridní cloud?

- Zvýšení komplexity prostředí (Lokální prostředí, Azure, Office365, Intune, Cloud App Security, Windows Defender ATP, Azure ATA, atd..
- Agilní rozvoj řešení (služby svévolně vznikají a zanikají (občas))
- Delegace prostředků a oprávnění k jednotlivým zdrojům a blokům cloudu
- Nerovnováha v bezpečnosti
  - lokální prostředí stále zlepšováno v oblasti bezpečnost a cloud zůstává netknutý
- Nefunkční procesy využívání služeb cloudu
- Správci celků cloudu, dodavatelé a jiní si dělají co chtějí, kdy chtějí a jak chtějí
- Velice časté změny v cloudovém prostředí („co bylo dnes, zítra být nemusí “)

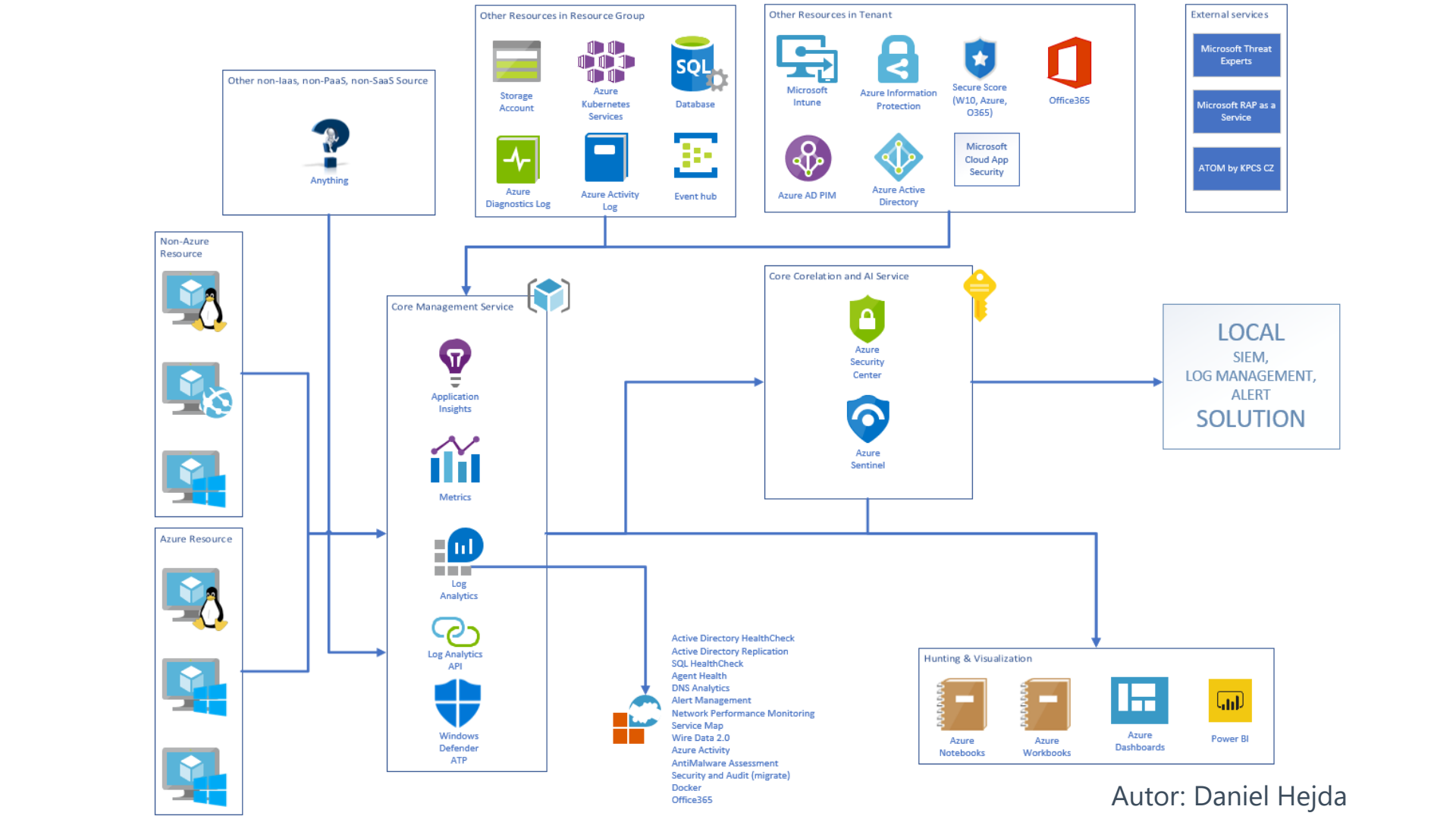
Jak z toho ven?

Ochranné prvky cloudu Microsoft Azure

- Proaktivní
  - Azure Blueprint
  - Azure Policy
  - Azure Key Vault
  - PIM/PAM/PAW/JIT
  - Azure MFA
  - Azure Information Protection
  - Azure Sentinel Playbooks
  - …
- Reaktivní
  - ASC Playbooks
  - ASC Adaptive network hardening
  - Windows Defender ATP
  - Azure Sentinel
  - Automation
  - …
- Detekční
  - Azure Security Center
  - ASC Regulatory compliance
  - ASC Security policy
  - Azure Monitor
  - …

Ochranné prvky cloudu Microsoft Azure

- Proaktivní
  - Azure Blueprint
  - Azure Policy
  - Azure Key Vault
  - PIM/PAM/PAW/JIT
  - Azure MFA
  - Azure Information Protection
  - Azure Sentinel Playbooks
  - …
- Reaktivní
  - ASC Playbooks
  - ASC Adaptive network hardening
  - Windows Defender ATP
  - Azure Sentinel
  - Automation
  - …
- Detekční
  - Azure Security Center
  - ASC Regulatory compliance
  - ASC Security policy
  - Azure Monitor
  - …



Autor: Daniel Hejda

Co se v Microsoft Azure (Security) změnilo?

- Log Analytics → Azure Monitor
  - Intelligence Packs → ….???….
- Application Insights → Azure Monitor
- Azure Security Center → Azure Sentinel (částečný přechod)
- Azure Dashboards v Sentinel → Azure Workbooks
- Azure Workbooks → Export Excel
- Azure Monitor → latency, recuring, smart groups, atd…
- Windows Admin Center >integrace< Azure Security Center

Koncepce?

- Governance cloudových služeb
  - Postupy
  - Politiky
  - Standardy
  - Konvence
  - Metodiky
  - Referenční architektury
- Quality Assurance / Quality Control
  - Nastavení procesu kontroly
  - Nastavení procesu zlepšování
  - Budování znalostní báze

5 důvodů proč využívat vše dohromady?

- Jednotné úložiště logů a auditních stop
- Snadnější dotazování do auditního logů a prováděné threat hunting
- Jednoduchost nasazení
- Centrální pohledy napříč informacemi (semafor pro detekce)
- Automatizace nasazení (deploy, re-deploy)

Automatizace nasazení

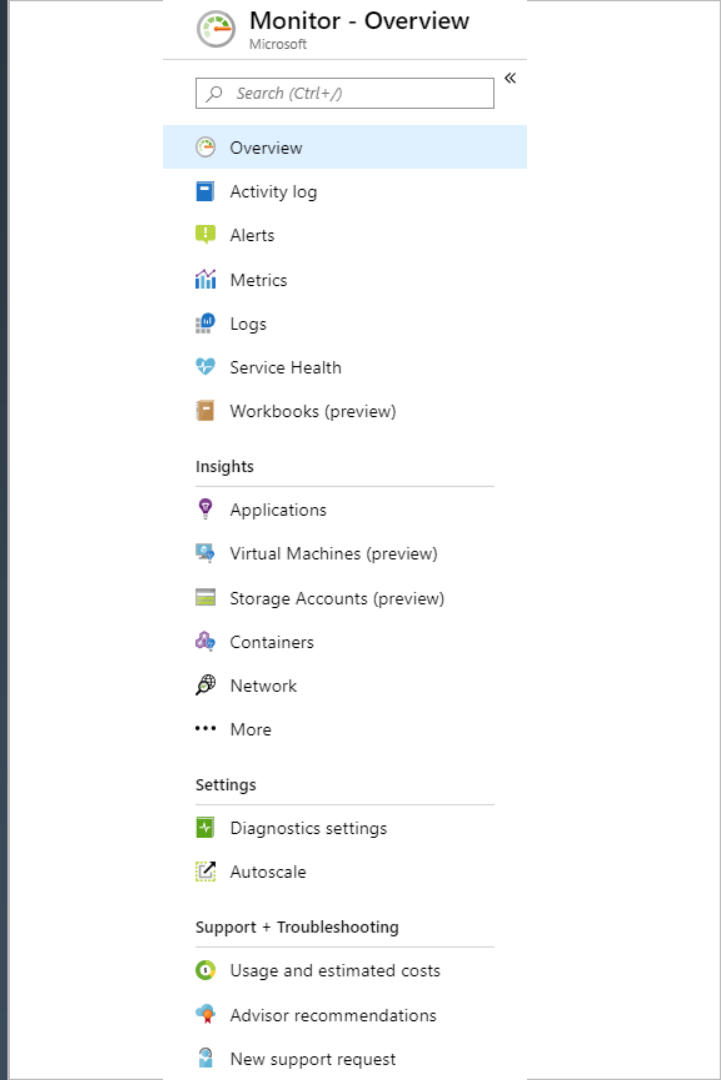
- Klientská část
  - pomocí Automation Hybrid Worker na koncovém zařízení
- Managementové prostředí
  - Nasazení pomocí ARM šablon
  - Včetně konfigurace

Azure Monitor

Monitoring & Log Management

Azure Monitor

- Nástroj pro monitoring hybridního prostředí
  - Windows
  - Linux
  - Cokoliv
- Komponenty
  - Zpracování a řízení alertů
  - Globální metriky
  - Globální aletry
  - Application Insights
  - Virtual Machine Insights
  - Container Insights
  - Log Analytics
  - Workbooks
- Dokumentace zde: https://github.com/MicrosoftDocs/azure-docs/tree/master/articles/azure-monitor



Nasazení agentů pro monitoring

- Rozšíření v rámci prostředí Microsoft Azure
- Lokální instalace
  - Log Analytics Agent (MMA Agent SCOM)
  - Dependency Agent (sběr informací o síťovém provozu)
  - Windows Defender Script PS1
  - Network Peformance Monitor Script
    - TCP Monitor - povoluje port 8084 skrze PS1 - TCP SYN-SYNACK-ACK
    - ICM Monitor – povoluje ICMPv4, ICMPv6 - ICMP ECHO ICMP ECHO REPLY
- Aplikační monitoring
  - Nasazení do Windows IIS – Web Platform Installer – Application Insights
  - Nasazení do dalších systémů – část kódu např. do header/footer.php

Prostupy vyžadované ke správnému fungování

- Monitorované zařízení musí mít přístup do internetu na portu 443 (HTTPS)
  - IaaS v Azure
  - Lokální server
- Lze provést úpravu a využít OMS Gateway
- Proxy je podporováno, ale je vždy doporučeno provést bypass na stanovené URL adresy

Agent Resource	Ports
*.oms.opinsights.azure.com	443
*.blob.core.windows.net	443
*.azure-automation.net	443
*.ods.opinsights.azure.com	443

Azure Security Center

User and entity behavior analytics (UEBA)

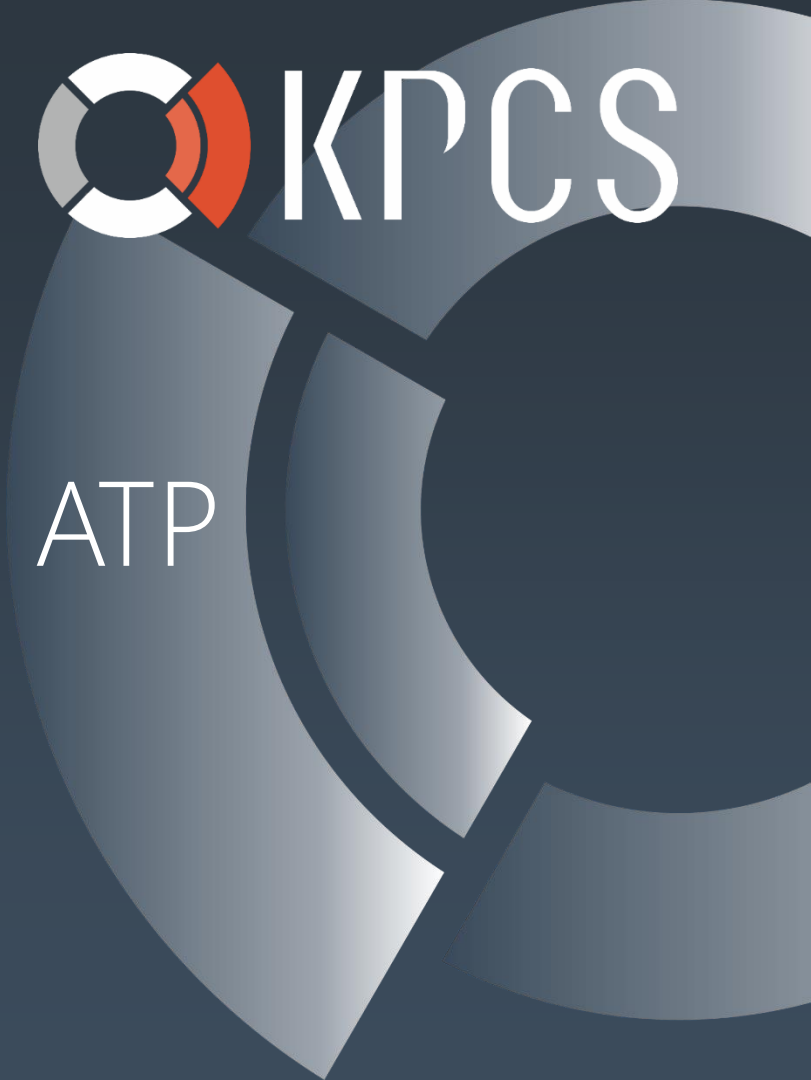
Azure Security Center

- UEBA pro sledování chování systémů a ochrana před hrozbami (cca 140 hrozeb)
  - Mapa security alertů
  - Vlastní alerty
  - Alerty detekované Microsoftem
- Kontrola compliance
  - Secure Score
  - Compliance
  - Security Policy
- Hygiena prostředí
  - Kontrola služeb a jejich nastavení
- Rozšířená ochrana služeb
  - Just-In-Time (pouze Azure resources)
  - Adaptive application controls
  - Adaptive network hardening (pouze Azure resources)
  - File Integrity Monitoring
- Orchestrace a auto-remediace (Playbook)

Další možnosti nastavení

- Cílení na zdroje (pmocí Solution Targeting)
- Připojeno pomocí Log Analytics Agenta, tedy není vyžadována další konfigurace
- Rozšiřuje datovou základu Log Analytics

- Pozor: Již není dostupná Investigation Map

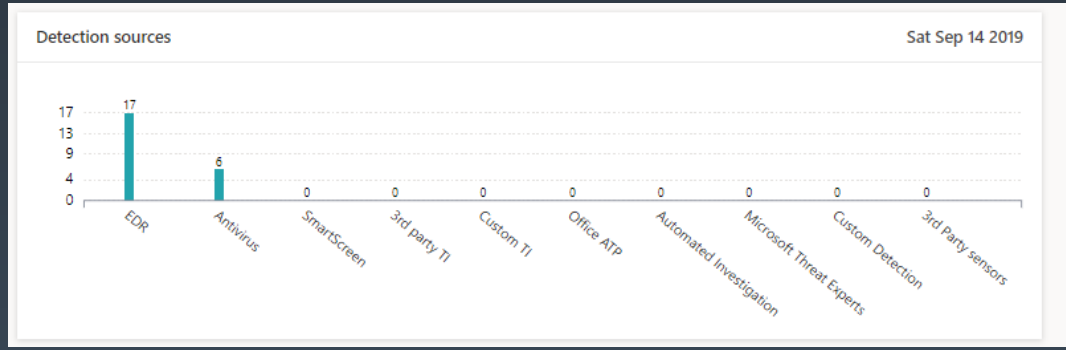


Windows Defender ATP

Threat Management & End-point Protection

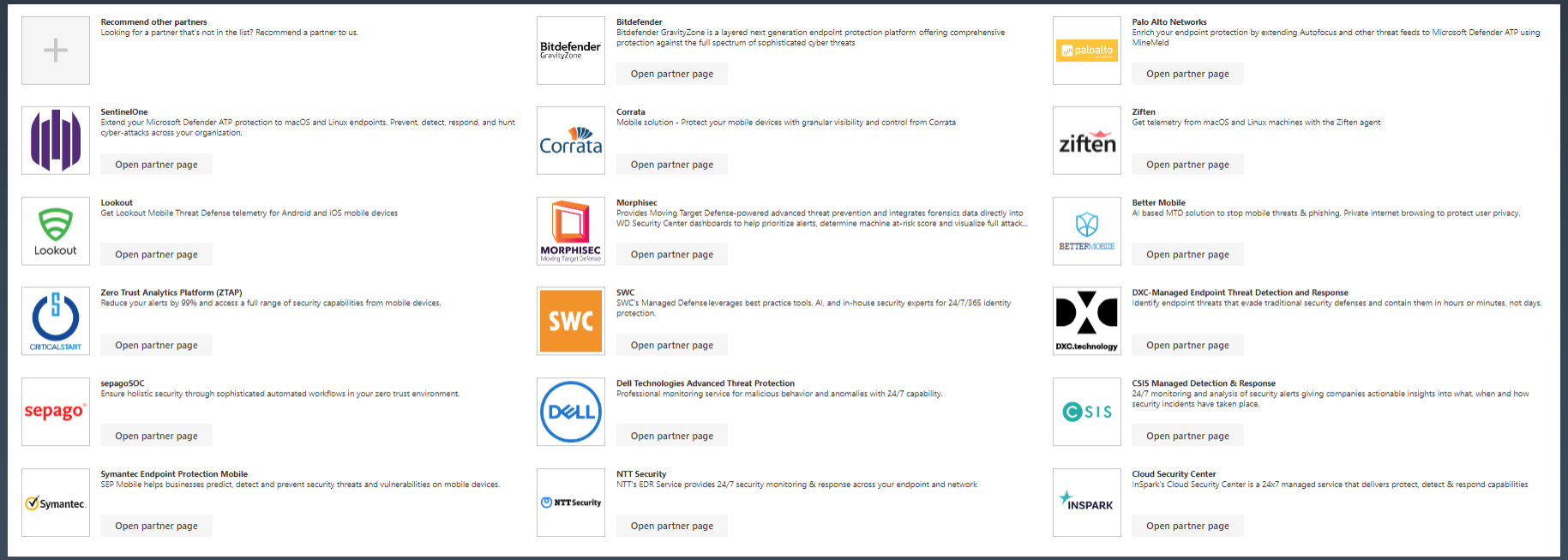
Windows Defender ATP

- Ochrana koncového bodu (detekční zdroje EDR, Anitivirus, Smart Screen, …)



- Secure score – výběr možností nastavení, které se budou počítat do Secure Score
  - Windows Defender Antivirus
  - Windows Defender Exploit Guard
  - Windows Defender Application Guard
  - Windows Defender SmartScreen
  - Windows Defender Firewall
  - Windows Defender Credential Guard
  - BitLocker
  - OS Platform
- Integrace se SIEM (HP ArcSight, Splunk, Generic API)
- Azure Sentinel Integrace - ????
- Mnoho možností, mnoho kontrol, mnoho různých integrací ochrany
- Threat & Vulnerability Management

Integrace s třetí stranou



Připojení klientů

- Je vyžadováno povolení portu 443 z koncového zařízení

- Způsoby nasazení na server
  - WS2008R2 SP1, 2012 R2 a 2016 – přidat Workspace ID
  - WS 1803 a 2019 – nasazeno pomocí scriptu
  - Linux – jedině s využitím řešení třetích stran

Agent Resource	Ports
winatp-gw-cus.microsoft.com	443
winatp-gw-eus.microsoft.com	443
winatp-gw-neu.microsoft.com	443
winatp-gw-weu.microsoft.com	443
winatp-gw-uks.microsoft.com	443
winatp-gw-ukw.microsoft.com	443
winatp-gw-aus.microsoft.com	443
winatp-gw-aue.microsoft.com	443

Azure Sentinel

nextGen SIEM

Azure Sentinel

- Nová generace SIEM řešení (využití ML a AI)
- Možnost využití expertů pro investigace problémů
  - Microsoftu (služba Microsoft Threat Experts)
    - https://www.microsoft.com/security/blog/2019/02/28/announcing-microsoft-threat-experts/
  - ATOM (služba KPCS CZ, s.r.o.)
    - https://www.atom.ms/atom
- Nadstavba nad Log Analytics Workspace (rozšíření datové základy a schématu)
- Threat Management
  - Incidenty
  - Workbooky
  - Dashboards
  - Huning
  - Notebooks
- Rozšíření a konfigurace
  - Konektory (AAD, AIP, AWS, ASC, AATP (ATA v Cloudu), Check Point, Cisco ASA, …)
  - Custom Alerty
  - Playbooky

Azure Monitor
Azure Security Center
Windows Defender ATP
Azure Sentinel

Office 365

Microsoft Azure

Power BI

Exchange

Skype for Business

Windows

SharePoint

Enterprise
Mobility & Security

Microsoft®
System Center