

IT professional

Nr 10 (107) październik 2020

FUNKCJE BEZPIECZEŃSTWA W OFFICE 365 s. 12

- Azure Information Protection – klasyfikowanie oraz zabezpieczenie dokumentów poprzez zastosowanie mechanizmu przypisywania etykiet
Rozszerzenie funkcjonalności działania poczty przy użyciu Message Encryption

Systemy Linux s. 61

Automatyczna instalacja systemu
Debian. Użycie pliku odpowiedzi

Sodinokibi, Maze, RagnarLocker w natarciu s. 45

Ewolucja ataków hakerskich a działania
zwiększające odporność na ransomware

KSIAŻKA GRATIS

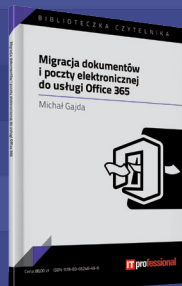
Migracja dokumentów i poczty
elektronicznej do usługi Office 365



Cena 36,00 zł (w tym 8% VAT)

ISSN 2083-9588

9 772083 958004



DOSTĘPNE
E-WYDANIE

UEM – Unified Endpoint Management to klasa rozwiązań do kompleksowego zarządzania urządzeniami klienckimi działającymi w sieci. Podobnie jak w poprzednich latach przetestowaliśmy aktualną wersję baramundi Management Suite na rok 2020.



Oprogramowanie UEM

baramundi Management Suite 2020

Marcin Jurczyk

Jedno z podstawowych zadań każdego administratora to ciągła kontrola urządzeń podłączonych do sieci firmowej. Mowa tu nie tylko o stacjach roboczych czy laptopach wykorzystywanych jako podstawowe narzędzia pracy w każdym biurze. Coraz większe znaczenie ma również efektywne zarządzanie urządzeniami mobilnymi, które w niektórych przypadkach skutecznie zastępują tradycyjne komputery. Mnogość i różnorodność urządzeń końcowych wykorzystywanych przez pracowników nie ułatwia tego zadania. Model BYOD, coraz większa popularność systemu macOS w środowisku firmowym i wyzwanie w postaci obsługi urządzeń kadry pracującej zdalnie to czynniki utrudniające zadanie produktom klasy UEM.

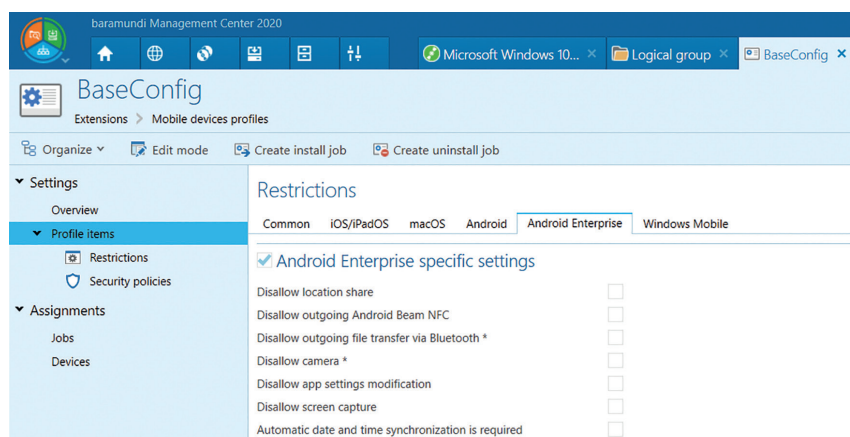
Oprogramowanie niemieckiej firmy baramundi software AG to jedno z tych rozwiązań do zarządzania urządzeniami końcowymi, które testujemy w zasadzie co roku, sprawdzając co nowego wnoszą najnowsza wersja. Od czasu pierwszego testu minęło już 6 lat – w tym czasie liczba klientów baramundi zdążyła się potroić, a każda kolejna wersja wprowadzała nowe funkcje, będące odpowiedzią na ciągle pojawiające się wyzwania: moduły Compliance Management oraz

Mobile Devices, rozpoznawanie maszyn wirtualnych VMware vSphere, wsparcie dla systemu macOS, obsługa Google Android Enterprise czy monitoring urządzeń sieciowych z wykorzystaniem protokołu SNMP. Również w tegorocznej odsłonie pojawiły się ważne nowości.

> NOWOŚCI W WERSJI 2019 R2

Zanim przejdziemy do omawiania nowości w wydaniu 2020 R1, warto poświęcić chwilę na zmiany, jakie przyniosła ze sobą wersja 2019 R2. Dodano między innymi wsparcie profilu firmowego dla Android Enterprise

oraz obsługę windowsowego BitLockera. W pierwszym przypadku mamy do czynienia z logicznym odseparowaniem aplikacji oraz danych związanych z obowiązkami służbowymi od prywatnych aplikacji użytkownika. Kontekst służbowy jest centralnie zarządzany, a separacja dostępu działa w obie strony – administrator bMS nie ma kontroli nad prywatnymi aplikacjami i danymi pracownika, a te z kolei nie mają dostępu do przestrzeni firmowej. W ten sposób możliwe jest używanie prywatnych smartfonów również do obsługi aplikacji biznesowych lub umożliwianie



Rys. 1. Moduł zarządzania urządzeniami mobilnymi zyskuje nowe funkcje z każdą kolejną generacją bMS.

+ pracownikom pewnej swobody przy używaniu służbowego telefonu. Oczywiście administrator Management Suite w dalszym ciągu ma możliwość wyboru trybu pełnej kontroli nad firmowymi urządzeniami mobilnymi, wprowadzonego już w wersji 2018 R2. Profil firmowy to nieco mniej restrykcyjne podejście, dające więcej swobody użytkownikom i pozwalające uniknąć posiadania dwóch słuchawek, co w dobie sześciocalowych ekranów wydaje się znacznym ułatwieniem. Aby skorzystać z funkcji profilu firmowego, użytkownik musi jedynie zainstalować aplikację agenta EMM dostępną w Google Play i dodać urządzenie do systemu zarządzania bMS choćby poprzez zeskanowanie kodu QR. Procedura może zatem zostać przeprowadzona w sposób zdalny. Sposób wyświetlania i separacji aplikacji służbowych zależy od wersji systemu Android i nakładki producenta smartfona. Ograniczenia narzucone z poziomu konsoli bMS będą dotyczyły jedynie pracy z aplikacjami służbowymi i tak na przykład możliwe jest zablokowanie korzystania z kamery, ale tylko w trakcie pracy w kontekście firmowym. W trakcie korzystania z aplikacji prywatnych żadne restrykcje nie będą działały. Co ważne, funkcja profilu firmowego dla systemu Android dostępna jest w module Mobile Devices Premium, podobnie jak separacja danych prywatnych i służbowych dla systemu iOS.

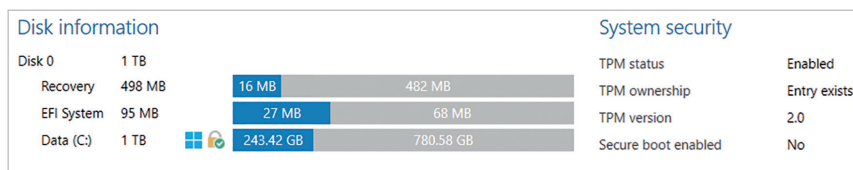
Druga z ważnych funkcji, które pojawiły się wraz z wersją 2019 R2, to wsparcie dla centralnego zarządzania szyfrowaniem dysków z użyciem wbudowanego w system Windows mechanizmu BitLocker. Administrator może w ten sposób zweryfikować wszystkie zarządzane urządzenia pod kątem szyfrowania pamięci. Istnieje również opcja zdefiniowania własnych profili konfiguracyjnych dla BitLockera, z uwzględnieniem metody szyfrowania (XTS-AES-128 lub -256), typu (pełne szyfrowanie lub szyfrowanie zajętej przestrzeni dyskowej) oraz wyboru wolumenów do zaszyfrowania (systemowy lub wszystkie dostępne). Możliwe jest

**Najnowsza
odłona baramundi
Management Suite to
kolejny duży krok w rozwoju
tego oprogramowania. Wiele
przydatnych nowości pojawiło
się zwłaszcza w zakresie
zarządzania urządzeniami
mobilnymi.**

też wymuszenie podania kodu PIN podczas procedury startowej systemu wraz z ustaleniem jego złożoności. Klucze odzyskiwania na wypadek utraty PIN-u przechowywane są w bMS w formie zaszyfrowanej, a dostęp do tego typu danych ograniczony jest na poziomie systemu uprawnień bMS.

Poza wspomnianymi funkcjami wersja 2019 R2 wniosła także sporo poprawek i usprawnień, z których na uwagę zasługuje z pewnością portal **docs.baramundi.com**, na którym w końcu znaleźć można bieżącą dokumentację. Dostęp do forum i nowej bazy wiedzy (wersja

do wyboru jeden z dwóch sposobów kontroli – pełne zarządzanie przeznaczone dla modelu COBO (Company Owned Business Only) oraz omawiany przed momentem profil firmowy, pozwalający zarządzać urządzeniami w scenariuszach COPE (Company Owned Personally Enabled) oraz BYOD. Od wersji 2020 R1 dostępna jest trzecia opcja, wspierająca model COSU (Company Owned Single Use), a więc służąca do zarządzania bardziej wyspecjalizowanymi urządzeniami z systemem Android, jak chociażby skanerami kodów kreskowych. W tym przypadku sprzęt może być wykorzystywany przez wielu użytkowników, a przy tym funkcjonalność ogranicza się do jednej lub co najwyżej kilku aplikacji, a więc istotne jest również odpowiednie rozróżnienie tego typu zastosowań na poziomie oprogramowania MDM. W określonym przypadku urządzenie tego typu może od razu po włączeniu uruchamiać wybraną aplikację jako domyślny tryb pracy. Implementacja tego typu funkcji w module Mobile Devices Premium z pewnością pozytywnie wpływa na kompletność rozwiązania, które teraz pozwala efektywnie zarządzać jeszcze większą grupą urządzeń



Rys. 2. Centralna kontrola szyfrowania dysków z wykorzystaniem mechanizmu BitLocker to kolejny ułkon w kierunku użytkowników Windowsa.

2.0) w dalszym ciągu wymaga rejestracji potwierdzonej przez producenta w ciągu 3 dni roboczych. Automatyzacja tej procedury znacznie ułatwiłaby dostęp do wszystkich informacji na temat bMS.

> CO NOWEGO?

Pora na nowości, które pojawiły się w aktualnej odłonie. Na pierwszy ogień idzie nowy sposób zarządzania urządzeniami mobilnymi z Androidem. Dotychczas administrator miał

końcowych. Jest to także ułkon w kierunku przedsiębiorstw, które poza standardowym sprzętem IT posiadają również rozwiązania wspomagające biznes choćby na poziomie magazynu i logistyki, a nawet w zakresie automatyki przemysłowej. W tym ostatnim aspekcie warto zwrócić uwagę na wsparcie dla zarządzania sterownikami SIEMENS SIMATIC. bMS od wersji 2020 R1 rozpoznaje tej klasy urządzenia podpięte do sieci (SNMP), odpowiednio je

kategoryzuje, a także wyświetla istotne z punktu widzenia inwentaryzacji oraz bezpieczeństwa szczegóły, jak chociażby wersja firmware. Jest to z pewnością krok w kierunku większego wsparcia środowisk OT.

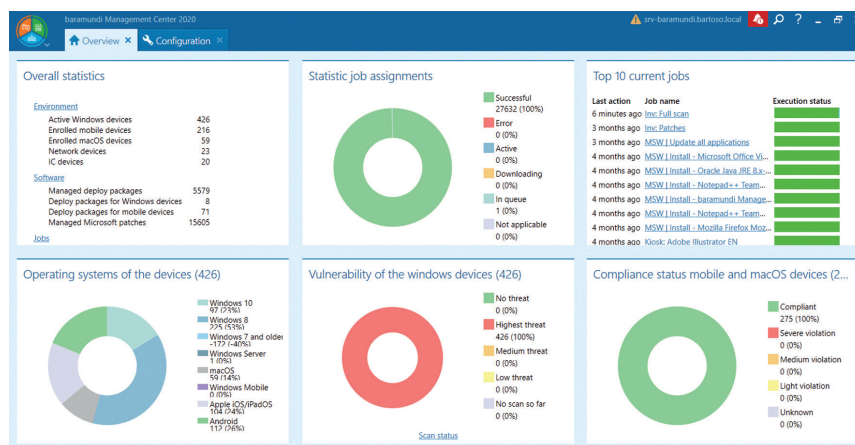
Kolejna funkcja, która pojawiła się w obecnej wersji bMS, to Argus Cockpit. W praktyce mamy do czynienia z nowym panelem kontrolnym dostępnym z poziomu chmury Microsoft Azure. Pozwala on na kontrolę serwera zarządzania baramundi dla wybranego środowiska. Argus Cockpit pozwala wyświetlać informacje na temat statusu wielu instancji bMS, co może okazać się przydatne w firmach zarządzających urządzeniami końcowymi u wielu klientów końcowych lub tam, gdzie wykorzystywanych jest wiele instancji, np. w rozproszonych geograficznie lokalizacjach. Cockpit pozwala śledzić wyniki zadań (Jobs), dzięki czemu administrator ma możliwość bieżącej kontroli i reakcji w przypadku niepowodzenia lub błędu podczas wykonywania zadania. Argus Cockpit dzięki wykorzystaniu usług chmurowych wymaga jedynie dostępu do internetu oraz przeglądarki internetowej. Nie ma potrzeby zestawiania jakichkolwiek tuneli VPN. Cała transmisja szyfrowana jest z wykorzystaniem protokołu HTTPS. Na razie Argus Cockpit dostępny jest bezpłatnie w ramach podstawowej licencji na oprogramowanie. Aby uzyskać do niego dostęp, wystarczy powiadomić partnera baramundi.

Poza wymienionymi nowościami jak zwykle usprawniono wiele funkcji dostępnych wcześniej. Wśród informacji o zarządzanych systemach Windows znaleźć można teraz także dane z MS Security Center, a więc status pracy zapory sieciowej, antywirusa czy chociażby stan UAC.

Nowa wersja to również aktualizacja wymagań oraz wspieranych systemów. W przypadku serwera zarządzania baramundi Management Server oraz baramundi PXE Relay pojawiły się ograniczenia w zakresie wsparcia dla Windows Server 2012 R2. Wersja 2020 R1 to także ostatnia edycja wspierająca SQL Server 2012 SP3 – od wersji 2020 R2, która

pojawi się niebawem, najniższa wspierana wersja SQL Servera to 2014 SP3. Zgodnie z zapowiedziami, które pojawiły się rok temu, znikło również wsparcie dla aplikacji agenta na Windows Mobile 10. Zmian dotyczących wymagań software'owych jest znacznie więcej, wszystkie dostępne są w nocie wydawniczej naj-

zarządzanie końcówkami klienckimi odbywa się za pośrednictwem aplikacji-agenta instalowanej na każdym wspieranym urządzeniu. Wśród systemów, dla których dostępna jest aplikacja agenta, znaleźć można m.in. różne wersje okienek Microsoftu, zarówno te konsumenckie, jak i serwerowe. Pełne



Rys. 3. Rzut oka na panel sterowania pozwala szybciej podjąć działania naprawcze.

nowszej wersji bMS. Nieco zaskakiwać może natomiast brak wsparcia dla nowszych wersji VMware vSphere począwszy od 6.7, nie mówiąc już o najnowszej wersji – 7.0. Wersja 6.5 to ostatnie wspierane wydanie.

> ARCHITEKTURA I WYMAGANIA

Pakiet bMS składa się z kilkunastu modułów funkcjonalnych, licencjonowanych osobno – w zależności od potrzeb danego środowiska. Licencjonowanie opiera się na dwóch czynnikach – liczbie zarządzanych urządzeń oraz modułach, z których chcemy skorzystać. Podstawowy sposób zakupu to wieczna licencja z opcją dodatkowego wsparcia ze strony producenta. Jeśli z jakiegoś względu klient wolałby zdecydować się na formę subskrypcji, to taka opcja również jest dostępna. Co więcej, niektóre moduły, jak chociażby Managed Software dostępne są tylko w takiej formie. bMS to rozwiązanie pracujące w typowym modelu klient-serwer. Co za tym idzie,

wsparcie ze strony baramundi dotyczy tych wersji, które są wciąż oficjalnie wspierane przez Microsoft. Na liście zgodności znaleźć też można starsze wersje Windowsa, jak chociażby Windows XP SP3 czy Windows Server 2008 SP2, choć w tym przypadku istnieją już dość poważne ograniczenia funkcjonalności. Aplikacja agenta dostępna jest także na macOS-a (od 10.7), Androida (od 4.0.4 lub 7.0 dla Android Enterprise) i iOS-a (od wersji 9).

Nie zmieniły się za to wymagania sprzętowe dla poszczególnych komponentów bMS. Serwer zarządzania wymaga minimum 8 GB RAM (zalecane 16 GB), 5 GB przestrzeni dyskowej oraz co najmniej jednego interfejsu sieciowego 1 GbE. Wymagania dotyczące przestrzeni dyskowej są bezpośrednio zależne od liczby aplikacji, które będziemy dystrybuować za pomocą bMS, a także liczby poprawek czy obrazów systemów operacyjnych, które zamierzamy rozpowszechniać, i tak wymagania dla serwera DIP to 10 GB dla aplikacji, 90 GB

na potrzeby modułu Managed Software, 400 GB na lokalną kopię poprawek i aktualizacji, a także 6 GB na każdy system operacyjny, który będzie wdrażany za pomocą modułu OS-Install. Dodatkowo 10 GB przestrzeni trzeba także zarezerwować na potrzeby bazy danych. Wspierane są silniki SQL Server od wersji 2012 SP3 (od wersji R2 2014 SP3) oraz Oracle 12c R2 oraz 19c. Dla niewielkich wdrożeń (około 300 zarządzanych urządzeń) możliwe jest wykorzystanie darmowej wersji SQL Express, dzięki

geograficznie, z pewnością skorzystają z rekomendacji baramundi i odseparują komponenty platformy, delegując im w celu podniesienia wydajności własne zasoby obliczeniowe.

> FUNKcjONALNOŚĆ

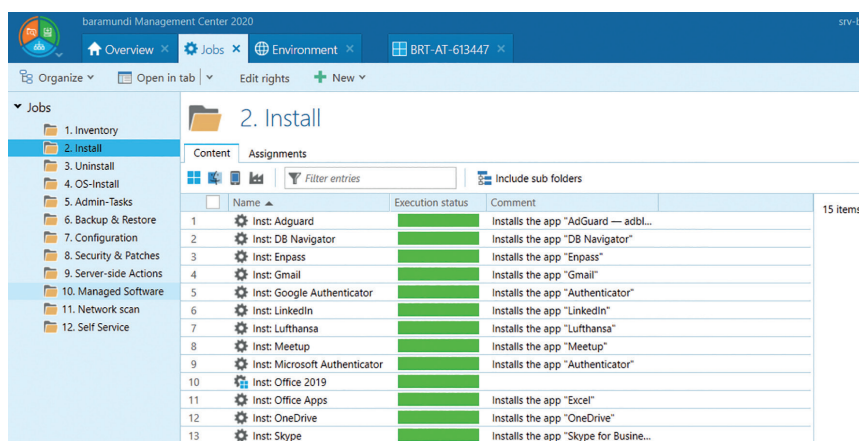
Jak już wcześniej wspomniano, Baramundi Management Suite to oprogramowanie modułowe. Producent odpowiednio klasyfikuje każdy z modułów w ramach grup funkcjonalnych. I tak 20 modułów zostało podzielonych na 8 grup:

- integracja z innymi rozwiązaniami (moduł Connect).

Pierwsza grupa obejmuje funkcje strictly inwentaryzacyjne, a więc stanowi absolutny trzon rozwiązania. Znajdziemy tam kompleksowe rozwiązanie pozwalające na szybką weryfikację dokładnego stanu posiadania – zarówno w zakresie sprzętu, jak i oprogramowania. Administrator za pomocą kilku kliknięć może wygenerować szczegółowy raport na temat środków trwałych, w tym urządzeń sieciowych, a także szybko zidentyfikować użytkowników korzystających z niestandardowego oprogramowania. Wspieranie dla protokołu SNMP oraz baz MIB pozwala na bardziej kompletną inwentaryzację sprzętu, dla którego nie ma możliwości wykorzystania aplikacji agenta. Ostatni moduł w grupie – AUT – umożliwia optymalizację kosztów związanych z licencjami na oprogramowanie poprzez monitorowanie użycia danej aplikacji, i ewentualne przesuwanie licencji na użytkowników, którzy rzeczywiście będą w stanie je wykorzystać.

Druga grupa modułów odpowiada za realizację zadań związanych z początkiem cyklu życia każdego urządzenia klienckiego, a więc jego aktywację i instalację. OS-Install, co sugeruje sama nazwa, pozwala przygotować automatyczną instalację systemu operacyjnego. OS-Cloning z kolei to narzędzie, które pozwoli na automatyczne kopiowanie wcześniej przygotowanego systemu na wskazane urządzenia końcowe. Tego typu funkcje docenią z pewnością ośrodki szkoleniowe lub szeroko rozumiana branża edukacyjna wykorzystująca komputery w celach dydaktycznych.

Po zakończeniu procesu instalacji i aktywacji urządzeń końcowych kolejnym krokiem jest dystrybucja oprogramowania. Za czynności z tym związane odpowiadają moduły należące do kolejnej grupy, a więc Deploy oraz Automate. Pierwszy z nich umożliwia zdalną dystrybucję oprogramowania z wykorzystaniem wiersza poleceń, skryptów czy plików odpowiedzi. Intuicyjny kreator umożliwia przygotowanie paczek instalacyjnych. Opcjonalnie można zdefiniować operacje do wykonania



Rys. 4. Większość czynności administracyjnych bazuje na zdefiniowanych wcześniej zadaniach.

czemu można zaoszczędzić na kosztach licencji. W praktyce darmowa wersja SQL może się sprawdzić również w nieco większych środowiskach, w zależności od tego, z jakich modułów funkcjonalnych zamierzamy skorzystać. Wciąż nie ma natomiast wsparcia dla darmowych silników bazodanowych, jak chociażby PostgreSQL, który z powodzeniem sprawdza się w produktach konkurencyjnych.

W stosunku do poprzednich wersji nie nastąpiły żadne zmiany w kwestii scenariuszy wdrożeniowych. Implementacja bMS w zależności od skali zarządzanego środowiska może zostać zrealizowana na pojedynczej maszynie fizycznej lub wirtualnej, na której zainstalowane zostaną wszystkie komponenty, takie jak chociażby serwer zarządzania, serwer bazodanowy czy interfejs zarządzania. Większe przedsiębiorstwa, często rozproszone

- inwentaryzacja sprzętu i oprogramowania (moduły Inventory, Network Devices oraz AUT (Application Usage Tracking),
- instalacja systemów operacyjnych (OS-Install oraz OS-Cloning),
- dystrybucja oprogramowania (Deploy oraz Automate),
- zarządzanie urządzeniami mobilnymi (Mobile Devices oraz Mobile Devices Premium),
- inteligentne zarządzanie infrastrukturą IT (Remote Control, Energy Management, License Management oraz nowy Argus Cockpit),
- gwarancja bezpieczeństwa (Vulnerability Scanner, Defense Control, Managed Software oraz Patch Management),
- tworzenie kopii zapasowych oraz odzyskiwanie danych (Disaster Recovery oraz Personal Backup),

przed instalacją oraz po jej zakończeniu. Instalacja może być zrealizowana w trybie cichym, bez ingerencji użytkownika lub w trybie interakcyjnym. Moduł Automate to z kolei rozbudowane narzędzie ułatwiające automatyzację instalacji oprogramowania oraz najczęstszych czynności administracyjnych na urządzeniach klienckich wyposażonych w aplikacje agenta. Automatyzacja ograniczona jest jedynie do systemów klienckich Microsoftu.

Grupą, na której rozwój położono największy nacisk w ostatnich latach, są moduły zarządzania urządzeniami mobilnymi. Wersja premium stanowi rozszerzenie funkcji podstawowych o omawiane już wcześniej opcje związane z obsługą BYOD czy szeroko pojętej separacji aplikacji biznesowych i prywatnych.

Trzy kolejne moduły realizujące funkcje inteligentnego zarządzania zostały rozszerzone o dostępność wspomnianego już Argus Cockpit. Remote Control, Energy Management oraz License Management to narzędzia usprawniające zarządzanie urządzeniami klienckimi. Pierwszy pozwala na zdalny dostęp do wszystkich urządzeń w domenie zarządzania Management Suite, chociażby w celu przeprowadzania diagnostyki czy zdalnej pomocy. Dwa kolejne pozwalają na wgląd w szczegółowe raporty o zużyciu energii elektrycznej przez urządzenia klienckie,

a także na kontrolę legalności oprogramowania zgodnie z posiadaną licencją.

Kolejna grupa zawiera moduły odpowiadające za bezpieczeństwo. Zmieniła się tu nieco konwencja nazewnictwa. Vulnerability Scanner to oczywiście skaner podatności uwzględniający polityki bezpieczeństwa. Moduł Patch Management z kolei pozwala na automatyzację łatania luk wykrytych w systemach Microsoftu. Do kontroli aktualizacji oprogramowania firm trzecich dostępny jest moduł Managed Software, bazujący na predefiniowanej liście oprogramowania zarządzanej przez baramundi. Defense Control to z kolei scentralizowany panel konfiguracyjny dla szyfrowania danych z wykorzystaniem BitLockera.

Przedostatnia grupa zawiera dwa moduły, które w dalszym ciągu dotyczą zabezpieczania danych, ale w nieco innym aspekcie. Personal Backup umożliwia kopiowanie wybranych danych użytkownika, które można przechowywać lokalnie lub na serwerze kopii zapasowych ze wsparciem dla mechanizmów kompresji, harmonogramów i kopii inkrementalnych. W przypadku Disaster Recovery mowa już o kopiach zapasowych całych obrazów systemu operacyjnego i dysków twardych, dzięki czemu w łatwy sposób można przywrócić kompletne środowisko po utracie laptopa czy awarii komputera.

Ostatni na liście moduł Connect pozwala integrować oprogramowanie baramundi z innymi aplikacjami za pośrednictwem usług bazujących na REST API. Dzięki temu i tak już spore możliwości Management Suite można relatywnie łatwo rozszerzyć o funkcje oprogramowania firm trzecich. **IT**

Autor jest architektem w międzynarodowej firmie z branży IT. Zajmuje się infrastrukturą sieciowo-serwerową, virtualizacją infrastruktury i pamięcią masową.

Werdykt

baramundi Management Suite 2020

Zalety

- + wsparcie dla najpopularniejszych platform stacjonarnych i mobilnych
- + ciągły rozwój funkcji MDM (profil firmowy i nowe urządzenia)
- + nieograniczona skalowalność
- + licencjonowanie
- + modularność
- + dokumentacja w formie webowej
- + możliwość kontroli stanu pracy z poziomu chmury (Argus Cockpit)

Wady

- uzależnienie od komercyjnych rozwiązań bazodanowych
- rozpoznawanie maszyn wirtualnych tylko do wersji vSphere 6.5

Ocena

9/10

PODSUMOWANIE

Najnowsza odsłona baramundi Management Suite to kolejny duży krok w rozwoju tego oprogramowania. Wiele przydatnych nowości pojawiło się zwłaszcza w zakresie zarządzania urządzeniami mobilnymi. O ile pierwsze próby baramundi dostarczania funkcji MDM pozostawiały sporo do życzenia, to każda kolejna edycja pakietu pokazuje, że producent postawił sobie za punkt

honoru, aby zarządzanie urządzeniami mobilnymi nie stanowiło jedynie dodatku, a jeden z głównych filarów rozwiązania. Ciekawie zapowiada się także otwarcie na świat OT, który mimo wszystko nieco odbiega od standardów IT. Na razie otrzymaliśmy podstawowe wsparcie dla sterowników Siemens, a więc dość oczywistego partnera, biorąc pod uwagę kraj pochodzenia

bMS. Ciekawy jest dalszy rozwój na tym polu szczególnie w aspekcie modułów odpowiedzialnych za kontrolę funkcji security. Nieustannie czepiamy się braku wsparcia dla darmowego silnika bazodanowego, jak chociażby PostgreSQL. Testy podobnego oprogramowania z rodzimego rynku pokazują, że da się i można przy tym zaoszczędzić na kosztach wdrożenia.