

Zunifikowane zarządzanie urządzeniami końcowymi (ang. Unified Endpoint Management – UEM) to zagadnienie, z którym mierzymy się dość regularnie, testując zróżnicowane oprogramowanie wspierające zarządzanie infrastrukturą IT. Standardowo o tej porze roku sprawdzamy najnowszą wersję produktu od baramundi.

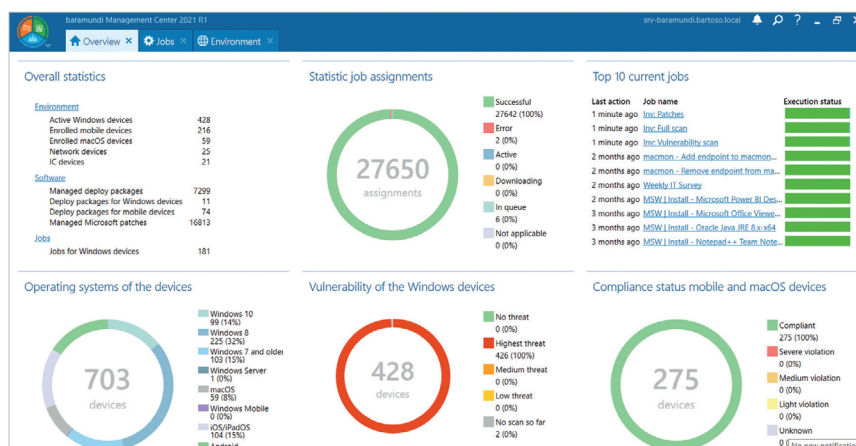


Zarządzanie końcówkami

baramundi Management Suite 2021

Marcin Jurczyk

Sposób zarządzania infrastrukturą informatyczną przedsiębiorstwa zależy w dużej mierze od skali zagadnienia. Zupełnie inne potrzeby będzie miała niewielka firma zatrudniająca od kilku do kilkunastu pracowników w porównaniu z dużym przedsiębiorstwem, gdzie liczbę użytkowników, a tym samym urządzeń, z których korzystają w codziennej pracy, można liczyć w dziesiątkach, setkach lub tysiącach. Narzędzi do kompleksowej kontroli zarówno sprzętu, jak i oprogramowania na nim zainstalowanego jest całkiem sporo. Co więcej – istnieje szereg świetnych rozwiązań powstających na rodzimym rynku, które niejednokrotnie testowaliśmy i nagradzaliśmy naszym wyróżnieniem. baramundi Management Suite (bMS) to akurat produkt pochodzący wprost zza naszej zachodniej granicy, a z którym mamy do czynienia regularnie już od 2014 r., obserwując konsekwentnie wprowadzane zmiany, nowe funkcje i usprawnienia, a także stale rosnące grono klientów. Tym razem na warsztat trafiła najnowsza na tę chwilę wersja 2021 R1, czyli pierwsze z dwóch wydań zaplanowanych na każdy rok kalendarzowy w cyklu wydawniczym producenta. Jak zwykle w przypadku bMS pierwsze



Za pośrednictwem panelu zarządzania można łatwo uzyskać wgląd w statusy najważniejszych komponentów.

wydanie w danym roku wprowadza najistotniejsze zmiany, zatem i tym razem oczekiwania są dość spore. Sprawdźmy zatem, co nowego pojawiło się od zeszłorocznego testu.

> ULEPSZENIA 2020 R2

Analizę zestawu ulepszeń, nowych funkcji i poprawek, które pojawiły się od ostatniego testu wersji 2020 R1, należy rozpocząć od wskazania zmian wprowadzonych tuż po naszej ostatniej publikacji, w ramach edycji 2020 R2. Wygląda na to, że ich lista w tej właśnie wersji jest znacznie dłuższa niż w przypadku testowanej edycji 2021 R1.

SEPARACJA DANYCH

Pierwsza z nich to pojawienie się wsparcia dla relatywnie nowego sposobu zarządzania urządzeniami mobilnymi, nazywanego przez Apple'a User Enrollment. Metoda ta pozwala użytkownikom na powiązanie własnego smartfona czy tabletu pracującego na iOS-ie z centralnym systemem zarządzania MDM w taki sposób, aby możliwa była pełna separacja danych prywatnych i służbowych. Również po stronie użytkownika leży decyzja o odpięciu własnego urządzenia od systemów firmowych, co skutkuje automatycznym usunięciem wszystkich danych służbowych. Jest to istotne usprawnienie

+ działające od 13. wersji iOS, mające szczególny wpływ na sposób kontroli i działanie w modelu BYOD. Dotychczas administrator MDM miał pełną kontrolę zarówno nad prywatnymi danymi i aplikacjami użytkowników, jak i częścią ściśle służbową. Restrykcje nakładane na zarządzane urządzenie miały charakter w pełni systemowy, przez co wyłączenie jakiejś funkcji dotyczyło także w pełni prywatnych aplikacji, co niekoniecznie zachęcało do wykorzystywania własnej słuchawki w celach służbowych. Nowy mechanizm ogranicza prawa administratora MDM do kontroli jedynie sfery biznesowej, a cała reszta pozostaje całkowicie prywatna, włączając w to także numer seryjny urządzenia czy IMEI.

W sferze MDM pojawiły się również inne usprawnienia. Możliwa jest chociażby kontrola wersji zainstalowanych aplikacji z wymuszeniem aktualizacji. Mechanizmy te działają nieco inaczej na platformie iOS zarządzanej za pośrednictwem natywnych mechanizmów VPP (ang. Volume Purchase Program) oraz dla Android Enterprise, gdzie funkcja automatycznych aktualizacji nie istnieje, a jej obsługa została rozwiązana na poziomie profili konfiguracyjnych.

AKTUALIZACJE I BEZPIECZEŃSTWO

Kolejne nowości w release R2 dla wersji 2020 to zmiana podejścia do zarządzania aktualizacjami Microsoftu. Jest to zapowiedź głębszych zmian w tym zakresie, które pojawiły się w najnowszej, testowanej przez nas wersji, o czym w dalszej części testu. W pierwszym etapie pojawiło się nowe zadanie, które pozwala przeprowadzić inwentaryzację brakujących i już zainstalowanych poprawek. Jako źródło aktualizacji wspierane są zarówno serwery Microsoftu, jak też instancja popularnej usługi WSUS. Co więcej, pojawiły się także nowe kategorie pozwalające wyfiltrować urządzenia niemające określonych aktualizacji za pośrednictwem uniwersalnych grup dynamicznych.

Inne zmiany pojawiły się w module Defense Control, a konkretniej

w opcjach konfiguracyjnych dla centralnego zarządzania BitLockerem. Dotychczas wymuszenie uwierzytelniania za pośrednictwem PIN-u przy starcie komputera automatycznie uniemożliwiało centralne wybudzanie zarządzanych stacji z racji konieczności manualnej interwencji użytkownika. Problem ten został rozwiązany poprzez wprowadzenie opcji odblokowania takiej stacji roboczej z poziomu sieci. Oczywiście najpierw konieczne jest zbudowanie relacji zaufania poprzez posługiwanie się odpowiednim certyfikatem. W ten sposób jedynie administrator bMS ma możliwość pominięcia kroku związanego z podaniem PIN-u. W procesie uwierzytelniania bierze także udział przełącznik baramundi PXE. Przygotowanie określonej grupy urządzeń końcowych do zdalnego odblokowania funkcji BitLockera odbywa się standardowo z wykorzystaniem odpowiedniego zadania z grupy Manage BitLocker.

WYDAJNOŚĆ I PERSONALIZACJA

Wśród innych zmian, które pojawiły się jeszcze pomiędzy wersjami 2020 R1 i 2021 R1, wymienić trzeba rozszerzenie możliwości wyświetlania danych o statusie pracy bMS w ramach Argus Cockpit. Pulpit dostępny z poziomu internetu rozbudowany został o wsparcie dla synchronizacji z widokami opartymi na uniwersalnych grupach dynamicznych. W ten sposób można niemal dowolnie dopasowywać wyświetlane informacje do własnych potrzeb.

**Z poziomu bMS
możliwy jest wgląd
w status ochrony
wszystkich urządzeń,
z uwzględnieniem informacji na
temat uruchomionych modułów
protekcji, ich wersji, a także
informacji o wykrytych
zagrożeniach.**

Poza typowymi nowościami poprzednia wersja bMS zawiera także szereg poprawek oraz usprawnień funkcjonalno-wydajnościowych dla wielu dotychczas istniejących modułów pakietu. Pełna lista jak zwykle dostępna jest w biuletynie wydawniczym danej wersji.

> NOWOŚCI 2021 R1

Przejdźmy zatem już do nowych funkcji dostępnych bezpośrednio w najnowszym aktualnie wydaniu – 2021 R1. Pierwsza i największa zmiana to pojawienie się systemu zgłoszeń – baramundi Ticketing System. Główna uwaga dotycząca tej funkcji – moduł ten dostępny jest obecnie jedynie w języku niemieckim, a więc potencjalne zalety dla rodzimego rynku są obecnie znikome. Dostępność języka angielskiego byłaby już krokiem w dobrym kierunku, choć z racji samej charakterystyki tego typu systemów brak polskiej lokalizacji dyskwalifikuje na razie ten moduł na rynkach innych niż niemieckojęzyczne. Traktujemy zatem Ticketing System jako pierwszą jaskółkę i zapowiedź rychłego wprowadzenia polskiej wersji językowej. Rozwiązanie bazuje na produkcie firmy OMNINET, a co za tym idzie – dostarczane jest z poziomu chmury, integrujące się z bMS za pośrednictwem odpowiedniego konektora. Moduł rozróżnia sześć scenariuszy zgłoszeń, nawiązując do metodologii ITIL – Incident Management, Problem Management, Task Management, Request Fulfillment, Knowledge Management oraz Change Management. Integracja z bMS polega na wykorzystaniu dobrze znanych definicji zdarzeń jako integralnej części zgłoszenia, dzięki czemu możliwe jest automatyczne wyzwalanie wybranych zadań służących do rozwiązania problemu, a następnie automatycznego dokumentowania rozwiązania. Czekamy na polską wersję językową, aby w pełni przetestować możliwości tego zintegrowanego rozwiązania.

Wśród tegorocznych nowości wymienić trzeba także zapowiadaną rozbudowę systemu zarządzania aktualizacjami Microsoftu. Tym razem pojawiło się wsparcie dla profili, za

pośrednictwem których można zbudować zoptymalizowaną politykę aktualizacji. W ramach profilu możliwe jest zdefiniowanie, jakiego typu poprawek ma dotyczyć dany profil, a także zdefiniowanie, z jakim opóźnieniem ma być zainstalowany update. Gdy mamy już zdefiniowane profile, pozostaje tylko przypisać je do odpowiednich grup (statyczne, dynamiczne i logiczne) wcześniej zdefiniowanych w bMS. W ten sposób można na przykład zaplanować przeprowadzenie aktualizacji, rozpoczynając instalacje na mniej krytycznej grupie urządzeń końcowych, opóźniając wykonanie dla reszty użytkowników o wskazany czas, tak aby uniknąć ewentualnych komplikacji.

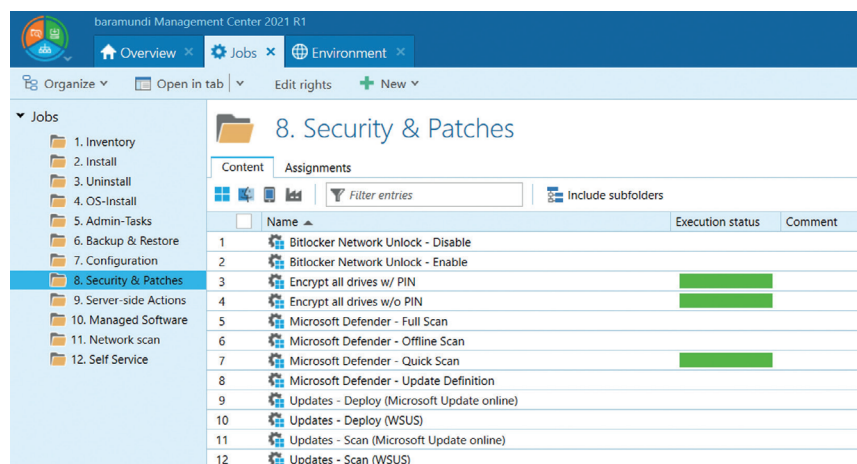
Poza wprowadzonym przed ponad rokiem centralnym zarządzaniem BitLockerem w najnowszej wersji pojawiło się także wsparcie dla centralnej kontroli mechanizmów Microsoft Defender Antivirus, czyli popularnego rozwiązania AV zintegrowanego z Windowssem. Teraz z poziomu bMS możliwy jest wgląd w status ochrony wszystkich urządzeń, z uwzględnieniem informacji na temat uruchomionych modułów protekcji, ich wersji, a także informacji o wykrytych zagrożeniach. W związku z pojawieniem się wsparcia dla Defendera na liście dostępnych zadań do wykonania pojawiły się dwa nowe – aktualizacja definicji oraz rozpoczęcie skanowania.

Nowe funkcje dotyczą także Argus Cockpit. W najnowszej wersji administrator może chociażby definiować ramy czasowe dla wyświetlanych parametrów, co wspomaga analizę trendów. Nie mogło także zabraknąć odzwierciedlenia zmian wprowadzonych na poziomie monitorowania Microsoft Defendera – w najnowszej wersji dane te są także widoczne z poziomu kokpitu Argus. Zmiany dotknęły również mobilną wersję baramundi Management Center, dostępną na iOS-a i Androida. Za pośrednictwem aplikacji mobilnej możliwe jest teraz chociażby przypisywanie zadań oraz przegląd zarządzanych urządzeń.

Lista poprawek wprowadzonych w wersji 2021 R1 jest znacznie dłuższa i zawiera m.in.: usprawnienia algorytmu wyświetlania map sieciowych, automatyczne dodawanie urządzeń pracujących pod kontrolą macOS poprzez Apple Automated Device Enrollment czy wsparcie dla in-place upgrade dla zdalnie zarządzanych urządzeń pracu-

poważne ograniczenia co do funkcjonalności, a baramundi nie może zagwarantować poprawnego działania.

Aplikacja agenta dostępna jest także na system macOS (od wersji 10.7), Android (od 4.0.4 lub 7.0 dla Android Enterprise) oraz iOS (od wersji 9). Wdrożenie bMS w zależności od skali zarządzanego środowiska może zostać



Lista zadań uzupełniana jest o nowe pozycje wraz z każdą kolejną wersją bMS.

jących pod kontrolą Windows 10. Jak zwykle odsyłamy do pełnej listy zmian dostępnej na stronach producenta.

> ARCHITEKTURA

Oprogramowanie bMS niezmienianie opiera swoje działanie na modelu klient-serwer, więc do poprawnej pracy wymagana jest instalacja aplikacji agenta na wszystkich zarządzanych stacjach. Wśród systemów, dla których dostępna jest aplikacja agenta, znaleźć można zróżnicowane wersje okienek Microsoftu, zarówno te konsumencie, jak i serwerowe. Pełne wsparcie ze strony baramundi dotyczy tych wersji, które są wciąż oficjalnie wspierane przez Microsoft, czyli począwszy od wersji Microsoft Windows 10 Enterprise 2015 LTSB dla urządzeń klienckich oraz Windows Server 2016 dla serwerów. Starsze generacje, jak chociażby Windows XP SP3 czy Windows Server 2008 SP2, znajdują się również na krótkiej liście wspieranych systemów, choć w tym przypadku istnieją już dość

zrealizowane w ramach pojedynczej maszyny fizycznej lub wirtualnej, na której zainstalowane zostaną wszystkie komponenty funkcjonalne, takie jak chociażby serwer zarządzania, silnik bazy danych czy interfejs zarządzania. Większe przedsiębiorstwa, często rozproszone geograficznie, z pewnością skorzystają z rekomendacji producenta i odseparują komponenty pakietu, dedykując im własne zasoby obliczeniowe w celu podniesienia wydajności i dostępności.

W dalszym ciągu nie ma wsparcia dla integracji z VMware vSphere powyżej wersji 6.5 Update 1. W praktyce stawia to pod dużym znakiem zapytania sens istnienia modułu baramundi Virtual – inicjalna data EoGS (ang. end of general support) dla vSphere 6.5 została przedłużona wiosną tego roku o 11 miesięcy, do 15 października 2022 roku. Niewiele zmieniło się także pod kątem wspieranych silników bazodanowych. W dalszym ciągu do wyboru mamy MS SQL (2014 SP3 lub nowszy) oraz Oracle 19c

+ (12x R2 dostępny tylko do wersji 2022 R1 włącznie). W małych środowiskach do 250 klientów istnieje możliwość skorzystania z darmowej wersji SQL Express Edition, choć w dalszym ciągu stoimy na stanowisku, że przydałoby się wsparcie dla darmowego silnika, jak chociażby PostgreSQL.

Nasze środowisko testowe ograniczało się do jednej maszyny wirtualnej, na której zainstalowano niezbędne komponenty do sukcesywnego zarządzania wszystkimi najpopularniejszymi elementami pakietu. W dużych, rozproszonych geograficznie środowiskach konieczne może się okazać odseparowanie modułów funkcjonalnych, począwszy od serwera zarządzania, poprzez usługi bazodanowe, po baramundi Gateway (komunikacja ze światem) czy baramundi Automation Studio.

> WYMAGANIA

Nic nie zmieniło się za to, jeśli chodzi o wymagania sprzętowe dla poszczególnych komponentów wchodzących w skład baramundi Management Suite. Dla serwera zarządzania wystarczy 8 GB RAM-u (zalecane 16 GB), 5 GB przestrzeni dyskowej oraz co najmniej jeden interfejs sieciowy 1 GbE. Wymagania dotyczące magazynowania są bezpośrednio zależne od liczby aplikacji, które będziemy dystrybuować za pomocą bMS, a także poprawek i obrotów systemów operacyjnych, które zamierzamy rozpowszechniać. 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. Wartości te mogą się różnić w zależności od tego, jak bardzo zróżnicowane jest zarządzane środowisko pod kątem oprogramowania. Konieczne będzie również zarezerwowanie około 10 GB przestrzeni dyskowej na potrzeby bazodanowe, bez względu na to, czy zdecydujemy się zainstalować wybrany silnik razem z serwerem zarządzania, czy też na osobnej maszynie.

> FUNKCJONALNOŚĆ

Baramundi Management Suite to oprogramowanie zbudowane na modułach funkcjonalnych, z których można utworzyć narzędzie dopasowane do aktualnych potrzeb przedsiębiorstwa w zakresie zarządzania urządzeniami końcowymi. Producent sklasyfikował każdy z modułów w ramach następujących grup funkcjonalnych:

- 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 MDM (Mobile Devices oraz Mobile Devices Premium);
- inteligentne zarządzanie infrastrukturą IT (Remote Control, Energy Management, License Management oraz Argus Cockpit);
- gwarancja bezpieczeństwa (Vulnerability Scanner, Defense Control, Managed Software oraz Patch Management);
- tworzenie kopii zapasowych oraz odzyskiwanie danych (Disaster Recovery oraz Personal Backup);
- integracja z innymi rozwiązaniami (moduł Connect).

Poza biblioteką modułów administrator bMS może także integrować rozwiązanie z innym oprogramowaniem za pośrednictwem interfejsu REST API opartego na protokole HTTPS. Obsługiwane formaty danych to XML oraz JSON.

Pierwsza grupa funkcjonalna obejmuje moduły mające za zadanie pomoc przy inwentaryzacji środowiska, które stanowią absolutny trzon rozwiązania. Pierwszy z modułów to kompleksowe rozwiązanie umożliwiające szybką weryfikację dokładnego stanu posiadania w zakresie sprzętu, jak i oprogramowania. Administrator ma możliwość wygenerowania szczegółowego raportu na temat środków trwałych. Może także szybko powiązać użytkowników

z wykorzystywanym przez nich oprogramowaniem. Wsparcie dla protokołu SNMP oraz baz MIB pozwala na dokładniejszą inwentaryzację sprzętu, dla którego nie istnieje program agenta. Ostatni moduł w grupie – AUT – pozwala na optymalizację kosztów licencyjnych związanych z oprogramowaniem. Odbyna się to dzięki aktywnemu monitorowaniu użycia aplikacji przez użytkowników, po czym możliwe jest wygenerowanie zestawienia, na podstawie którego licencje mogą zostać rozdysponowane w inny sposób.

Druga grupa modułów funkcjonalnych realizuje zadania związane z inicjacją cyklu życia każdego urządzenia klienckiego, czyli jego aktywacją i instalacją oprogramowania. OS-Install, jak z nazwy wynika, pozwala na przygotowanie automatycznej instalacji systemu operacyjnego. OS-Cloning z kolei to narzędzie ułatwiające automatyczne kopiowanie wcześniej przygotowanego systemu na wskazane urządzenia końcowe. Tego typu funkcja może okazać się szczególnie przydatna w szeroko rozumianej branży edukacyjnej, gdzie konieczne jest szybkie przywrócenie do ustawień początkowych po każdorazowym zakończeniu zajęć.

Od razu po ukończeniu procesu instalacji i aktywacji urządzeń końcowych konieczna jest dystrybucja oprogramowania. Za czynności z tym związane odpowiadają moduły należące do kolejnej grupy, czyli Deploy oraz Automate. W pierwszym przypadku mamy do czynienia z narzędziem umożliwiającym zdalną dystrybucję oprogramowania z wykorzystaniem różnych mechanizmów, jak chociażby linia poleceń, skrypty czy pliki odpowiedzi. Za pośrednictwem kreatora możliwe jest przygotowanie paczek instalacyjnych. Opcjonalnie można także zdefiniować szereg operacji do wykonania przed instalacją oraz po jej zakończeniu. Sama instalacja może być przeprowadzona w trybie cichym (bez ingerencji użytkownika) lub w trybie interaktywnym. Moduł Automate z kolei to rozbudowane narzędzie ułatwiające automatyzację instalacji oprogramowania oraz

najczęstszych czynności administracyjnych na urządzeniach klienckich. Automatyzacja ograniczona jest jednak tylko do wspieranych systemów klienckich Microsoftu.

Patrząc na akcenty kładzione na poszczególne bloki funkcjonalne bMS, łatwo zauważyć, że grupą, na której rozwój położono największy nacisk, są moduły zarządzania urządzeniami mobilnymi. Wersja Premium zawiera rozszerzenie funkcji podstawowych o omawiane już wcześniej opcje, dotyczące chociażby obsługi BYOD czy szeroko pojętej separacji aplikacji biznesowych i prywatnych.

Trzy kolejne moduły realizujące funkcje inteligentnego zarządzania – Argus Cockpit, Remote Control, Energy Management oraz License Management – to narzędzia usprawniające zarządzanie urządzeniami klienckimi. Wspomniany wcześniej kokpit Argus to sukcesywnie rozwijany interfejs umożliwiający kontrolę nad stanem pracy bMS z dowolnego miejsca z dostępem do internetu, dzięki wykorzystaniu technologii chmurowej. Remote Control pozwala na zdalny dostęp do wszystkich urządzeń w domenie zarządzania Management Suite w celu przeprowadzania działań diagnostycznych i zdalnej pomocy. Dwa kolejne pozwalają na wgląd w szczegółowe raporty o zużyciu energii elektrycznej

przez urządzenia klienckie, a także na kontrole legalności oprogramowania.

Następna w kolejności grupa funkcjonalna zawiera moduły odpowiadające za zapewnienie szeroko rozumianego bezpieczeństwa. Vulnerability Scanner to skaner podatności bazujący na ustalonej wcześniej polityce bezpieczeństwa, obowiązującej w organizacji. Moduł Patch Management z kolei pozwoli zautomatyzować proces łatania wykrytych luk dla systemów Microsoft. W dalszym ciągu dostępny jest klasyczny sposób zarządzania aktualizacjami znany z wcześniejszych wersji bMS, jak również omawiany wcześniej mechanizm działający na podstawie profili. 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 microsoftowego BitLockera oraz kontroli nad wbudowanym w systemy Windows Microsoft Defenderem.

Ostatnia grupa zawiera dwa moduły, które w dalszym ciągu dotyczą bezpieczeństwa danych, jednak z nieco innej perspektywy. Personal Backup pozwala na tworzenie kopii wybranych danych użytkownika, które można przechowywać lokalnie lub na serwerze backupu.

Wspierane są tu mechanizmy typu kompresja, harmonogramy i kopie przyrostowe. W przypadku Disaster Recovery mowa już o kopiach zapasowych całych obrazów systemu operacyjnego i dysków twardych, dzięki czemu możliwe jest przywrócenie obrazu całego urządzenia w przypadku chociażby awarii sprzętowej. **IT**

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

Werdykt

baramundi
Management Suite 2021

Zalety

- + modułarna budowa i licencjonowanie
- + nowe funkcje MDM
- + rozbudowane scenariusze wdrożeniowe
- + nowy moduł aktualizacji dla Microsoftu
- + zarządzanie aktualizacją aplikacji dla platform mobilnych
- + REST API

Wady

- uzależnienie od komercyjnych rozwiązań bazodanowych
- rozpoznawanie maszyn wirtualnych tylko do wersji vSphere 6.5
- system zgłoszeń na razie tylko w języku niemieckim

Ocena

9/10

PODSUMOWANIE

Rozbudowę pakietu baramundi Management Suite obserwujemy już od wielu lat. To, co cechuje wszystkie kolejne generacje oprogramowania, to konsekwentny rozwój produktu i coraz więcej nowych funkcji. Trudno oprzeć się wrażeniu, że twórcy bMS od kilku lat kładą duży nacisk na zarządzanie urządzeniami mobilnymi, co nie jest tak oczywiste

wśród oferty konkurencji, której propozycja w tym zakresie sprowadza się do podstawowej funkcjonalności. Premiera nowego systemu zgłoszeń to bez wątpienia kolejny krok w dobrym kierunku, biorąc pod uwagę zwłaszcza integrację z rozbudowanym systemem zadań. Pozostaje jednak pewien niedosyt związany z tymczasowym brakiem wsparcia przynajmniej dla

języka angielskiego, który umożliwiłby przetestowanie tej funkcji w wystarczającym zakresie. Konsekwentny rozwój oprogramowania musi iść w parze z adekwatnie wysoką oceną, którą przyznajemy już od kilku lat z racji braku ewidentnych wpadek. Mam nadzieję, że do kolejnego testu pojawi się sensowne spolszczenie modułu baramundi Ticketing System.