



Szybkość i bezpieczeństwo dzięki automatyzacji

Jedno oprogramowanie do zarządzania wszystkimi urządzeniami końcowymi

SPIS TREŚCI

1	Coraz większe wymagania wobec działów IT	2
2	Automatyzacja rutynowych prac.....	4
2.1	Przydzielanie systemów operacyjnych i aplikacji	4
2.2	Identyfikacja słabych punktów, podatności i automatyzacja aktualizacji	6
2.3	Inwentaryzacja sprzętu i oprogramowania, zarządzanie licencjami	7
2.4	Inteligentna automatyzacja: sterowanie czasowe i samoobsługa.....	9
2.5	Integracja z dotychczasową infrastrukturą	9
3	Zarządzanie urządzeniami mobilnymi.....	10
4	Bezpieczeństwo i ochrona danych	14

© 2025 baramundi software GmbH

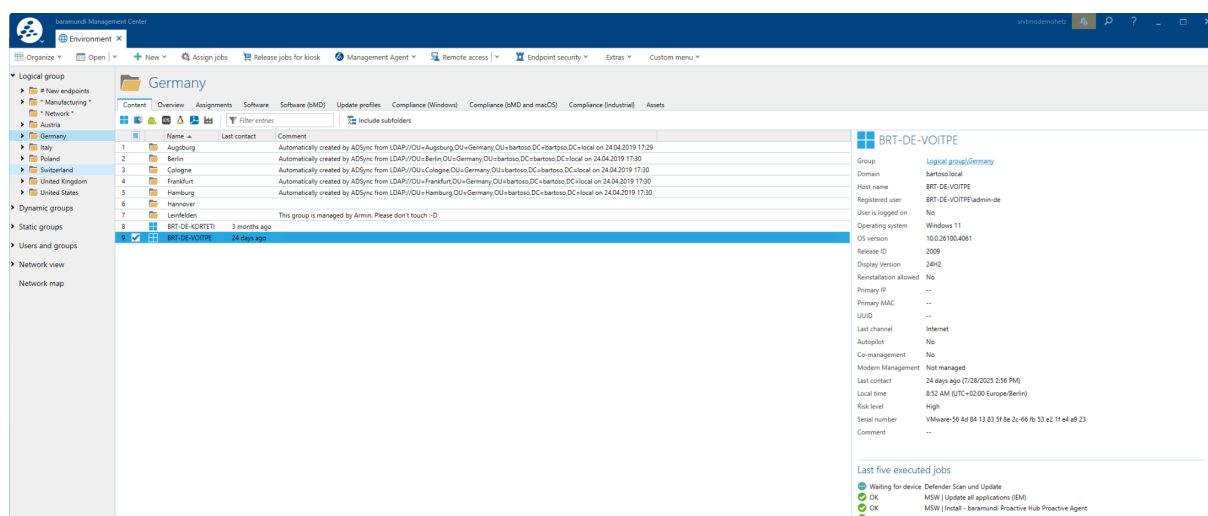
Informacje na temat wyposażenia i funkcji technicznych są niewiążące i mają wyłącznie charakter informacyjny.
Zastrzega się prawo do zmian. DocID WP-201019

1 Coraz większe wymagania wobec działów IT

Rozwój technologii informacyjnej (IT) postępuje coraz szybciej. Chociaż od powstania maszyny Z1 Konrada Zusego do pojawienia się pierwszych komputerów osobistych upłynęły dekady, obecnie branża ewoluuje niemal z miesiąca na miesiąc. Wraz ze wzrostem wydajności i różnorodności urządzeń rosną także wymagania stawiane metodom administrowania nimi.

Wielu użytkowników nie pracuje już tylko na komputerach stacjonarnych czy laptopach, lecz korzysta jednocześnie lub kolejno także ze smartfonów i tabletów. Na e-maile odpowiada się teraz w drodze, wyszukiwanie rozpoczęte na komputerze stacjonarnym kontynuuje się na smartfonie, a do sterowania prezentacjami wykorzystuje się tablet. Urządzenia mobilne używają innych systemów operacyjnych i aplikacji niż typowe urządzenia końcowe, jednak i one potrzebują dostępu do danych firmowych i e-maili – a w związku z tym wymagają również niezawodnej ochrony.

Jednocześnie zacierają się granice pomiędzy urządzeniami mobilnymi a światem komputerów stacjonarnych: obecnie dostępne są na przykład tablety z systemami operacyjnymi znanymi z komputerów osobistych, natomiast aplikacje mobilne działają na urządzeniach końcowych z systemem Windows. W związku z tym zarządzanie wszystkimi urządzeniami końcowymi wykorzystywanymi przez użytkowników w przedsiębiorstwie należałoby połączyć w jedno rozwiązanie. Pozwoli to na wdrożenie jednolitych standardów, oraz umożliwi uzyskanie pełnego obrazu stanu sieci i wszystkich urządzeń końcowych. Jednocześnie z takim całościowym rozwiązaniem będzie można łatwo zintegrować przyszłe, nowe urządzenia.



Ujednolicony obraz wszystkich rodzajów urządzeń / platform

Dzięki rozwiązaniu do ujednoliconego zarządzania urządzeniami końcowymi możliwa jest automatyzacja rutynowych zadań, a tym samym ich skuteczniejsza, szybsza i łatwiejsza realizacja. Zapewnia to konieczną orientację, a jednocześnie zwiększa poziom bezpieczeństwa sieci firmowej. Niniejsze opracowanie zawiera przegląd zadań administracyjnych, które należy koniecznie poddać automatyzacji.

2 Automatyzacja rutynowych prac

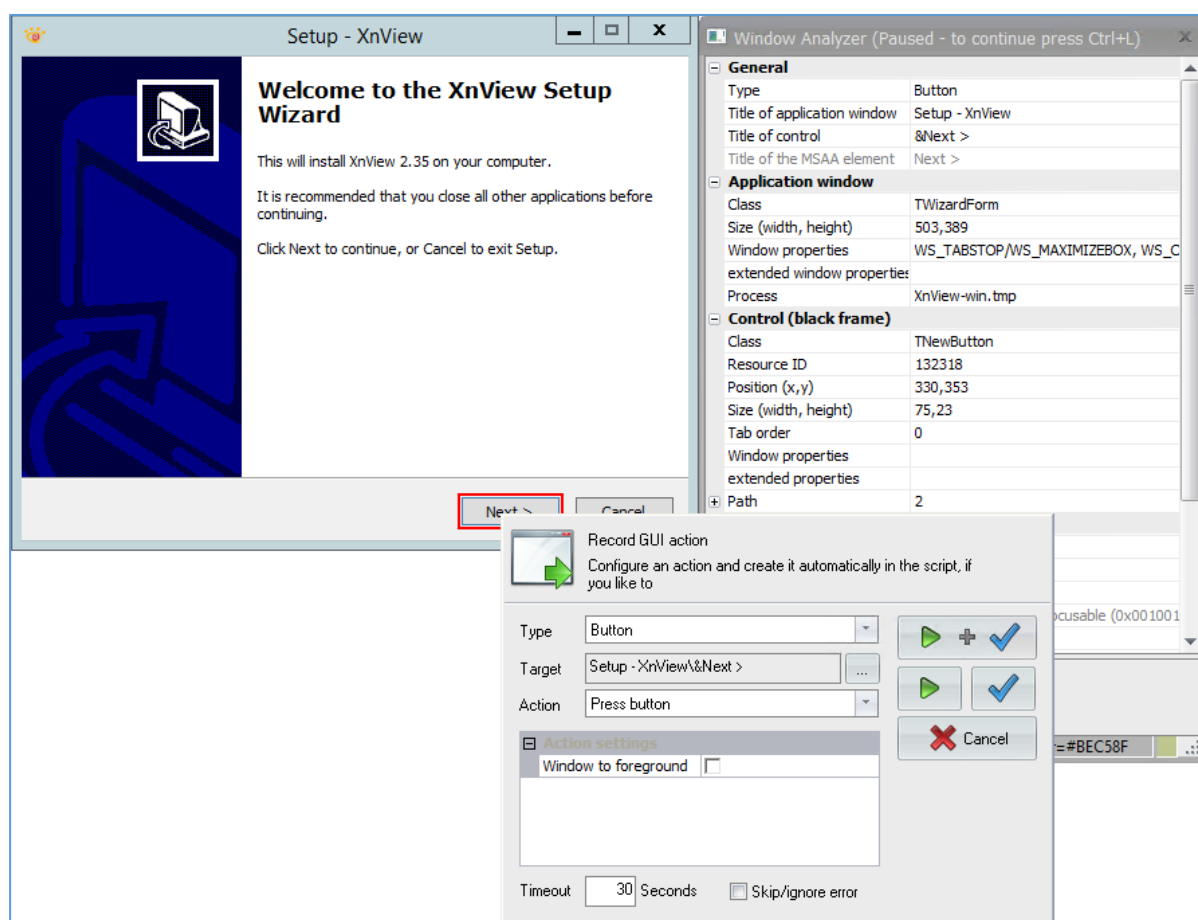
2.1 Przydzielanie systemów operacyjnych i aplikacji

Zatrudniono nowego pracownika. Dla działu IT oznacza to: Konieczność udostępnienia komputerowego stanowiska pracy lub w miarę możliwości notebooka. Zainstalowanie na komputerze systemu operacyjnego i wszystkich potrzebnych aplikacji – wliczając w to niezbędne ponowne uruchomienia, dobór właściwych sterowników itd. – zajmuje kilka godzin. Dzięki rozwiązaniu do zarządzania ten nakład czasu kurczy się do zaledwie kilku kliknięć myszą:

Zamiast konfiguracji przeprowadzanej ręcznie lub za pośrednictwem skryptu nowe urządzenie jest automatycznie rozpoznawane w sieci. W jednym etapie odbywa się przygotowanie dysku twardego oraz przyporządkowanie potrzebnych sterowników. Inteligentne rozwiązania używają natywnej metody instalacji producenta systemu operacyjnego, co pozwala na zachowanie pełni praw do roszczeń gwarancyjnych. Dzięki funkcji Wake on LAN instalację komputera można przeprowadzać nawet nocą.

Automatyczne przydzielanie jest możliwe również w przypadku oprogramowania. W większości przypadków dla profilu zastosowania definiuje się wyposażenie standardowe. W razie potrzeby administrator jednym kliknięciem myszy rozszerza ten pakiet oprogramowania na cały system docelowy – również na wiele urządzeń jednocześnie, włącznie z niezbędnymi operacjami ponownego uruchomienia przy zapewnieniu najwyższego poziomu instalacji z wykorzystaniem oryginalnych metod konfiguracji. Rozwiązanie do automatyzacji generuje przy tym komunikat zwrotny o statusie instalacji oraz ewentualnie o pojawiających się błędach. Raz zdefiniowane zadania można wykorzystać ponownie w dowolnym momencie, gdy po upływie kilku miesięcy zostanie zatrudniona kolejna osoba, czy też w przypadku wymiany urządzenia. Jednocześnie automatyczna instalacja gwarantuje standardową konfigurację komputerów oraz niewielką liczbę błędów.

Często konieczna jest instalacja oprogramowania, dla którego producent nie udostępnia standardowych pakietów instalacyjnych. Dzięki narzędziom zintegrowanym z typowym oprogramowaniem administracyjnym można w łatwy i intuicyjny sposób konfigurować niezbędne w takich przypadkach skrypty automatyzujące działanie interfejsów. W ten sposób nawet problematyczne konfiguracje będą przeprowadzane centralnie i automatycznie z wykorzystaniem zalecanej przez wytwórcę oprogramowania procedury konfiguracyjnej, co zapewni zachowanie gwarancji producenta.



Automatyzacja interfejsów z wykorzystaniem kreatora w programie baramundi Automation Studio

Oprogramowanie do zarządzania umożliwia nie tylko przydzielanie aplikacji, lecz również ich usuwanie z urządzenia końcowego. Wybierając rozwiązanie należy mieć na uwadze, aby było to możliwe także dla programów, których nie zainstalowano za pośrednictwem oprogramowania do zarządzania. W ten sposób można skutecznie usuwać na przykład aplikacje, które użytkownik zainstalował na swojej maszynie bez pozwolenia.

Ponadto centralna, zautomatyzowana instalacja aplikacji i systemów operacyjnych niesie ze sobą pozytywny efekt uboczny dla administratorów i użytkowników końcowych: w razie problemów z wydajnością i w przypadku poważnych błędów zamiast uciążliwie poszukiwać ich przyczyn, można po prostu przeprowadzić nocną ponowną instalację stanowiska roboczego. W ten sposób w pełni sprawne urządzenie staje się ponownie dostępne przy minimalnym nakładzie czasu pracy administratora. Umożliwia to również automatyczną migrację dużej liczby stanowisk roboczych – na przykład do nowego systemu operacyjnego jak Windows 11 czy nowej wersji pakietu Office.

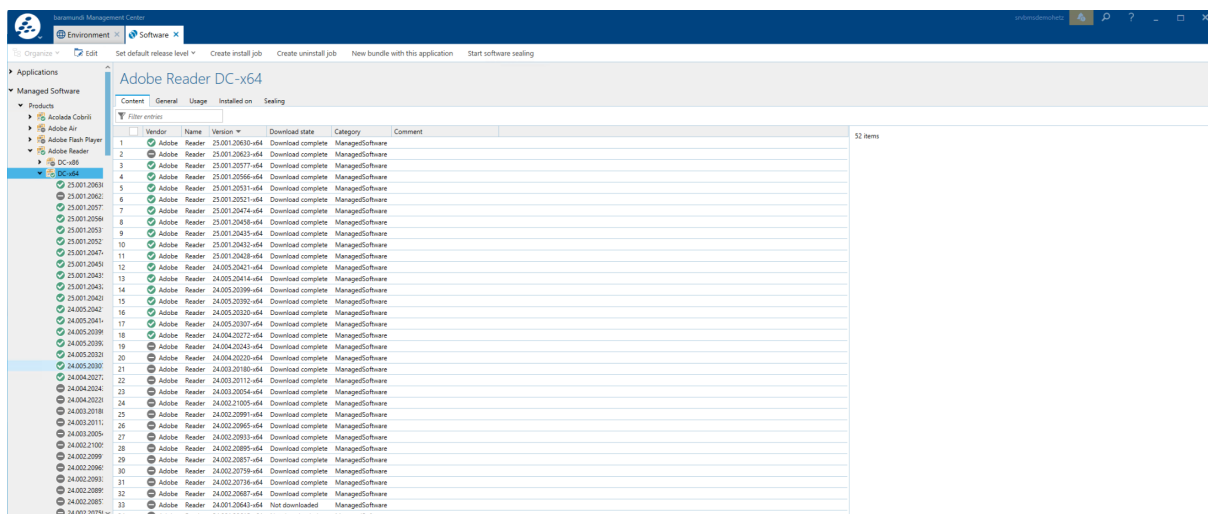
2.2 Identyfikacja słabych punktów, podatności i automatyzacja aktualizacji

Jednorazowa instalacja i po sprawie? Niestety nie. Stale pojawiają się nowe aktualizacje aplikacji i systemów operacyjnych, które należy jak najszybciej zainstalować na wszystkich komputerach. Nie chodzi przy tym tylko o nowe funkcje, lecz przede wszystkim o bezpieczeństwo: nowe wersje i łatki zamykają luki w systemie ochrony, za pośrednictwem których potencjalni intruzi mogliby wniknąć do sieci firmowej i wyrządzić poważne szkody. Skala konsekwencji sięga w takich przypadkach od szkód wizerunkowych spowodowanych publikacją wewnętrznych informacji firmowych, aż do szkód będących wynikiem kradzieży danych klientów i naruszenia przepisów o ochronie danych osobowych.

Zapory ogniowe i skanery antywirusowe stanowią wprawdzie nieodzowny element systemu bezpieczeństwa, lecz są w dużej mierze nieskuteczne w przypadku ataków przez niezabezpieczone słabe punkty. Gdy podczas tzw. ataku reverse connection zostaje wymuszone nawiązanie przez komputer pracownika – z wykorzystaniem słabego punktu – połączenie z serwerem kontrolnym intruza, zaporę ogniową z reguły nie przychodzi z pomocą, gdyż kontakt jest nawiązywany w zaszyfrowany sposób na standardowych kanałach z poziomu przedsiębiorstwa. Dlatego też kluczowe znaczenie ma zachowanie kontroli nad słabymi punktami każdego urządzenia końcowego i ich jak najszybsza eliminacja – zależnie od stopnia zagrożenia.

Zgodnie ze statystykami National Vulnerability Database opracowanymi przez US-CERT każdego tygodnia identyfikowanych i dokumentowanych jest ok. 100 nowych luk w zabezpieczeniach. W tym przypadku oprogramowanie do zarządzania może ułatwić pracę administratorów dzięki automatycznemu i regularnemu skanowaniu wszystkich urządzeń końcowych i serwerów. W rezultacie administratorzy otrzymują przejrzyste listy zawierające zestawienia np. najbardziej niebezpiecznych słabych punktów w sieci firmowej lub w urządzeniach końcowych z najczęstszymi lukami bezpieczeństwa. Pozwala to na określenie priorytetów i precyzyjne likwidowanie luk.

Jeżeli oprócz skanera słabych punktów rozwiązanie dysponuje również funkcją do zarządzania łatami, zamykanie takich zidentyfikowanych luk może odbywać się centralnie, w sposób zautomatyzowany. Oprócz patch'y Microsoftu rozwiązanie do zarządzania powinno również centralnie i automatycznie przydzielać aktualizacje przynajmniej dla często używanych aplikacji, takich jak Adobe Reader, Java czy Firefox, które z uwagi na dużą popularność są szczególnie narażone na ataki. Aktualne pakiety oprogramowania dla licznych aplikacji są również dostępne jako Managed Software od producentów UEM. Mogą one być udostępniane do produktywnego wykorzystania lub do testów na własnych zasadach.



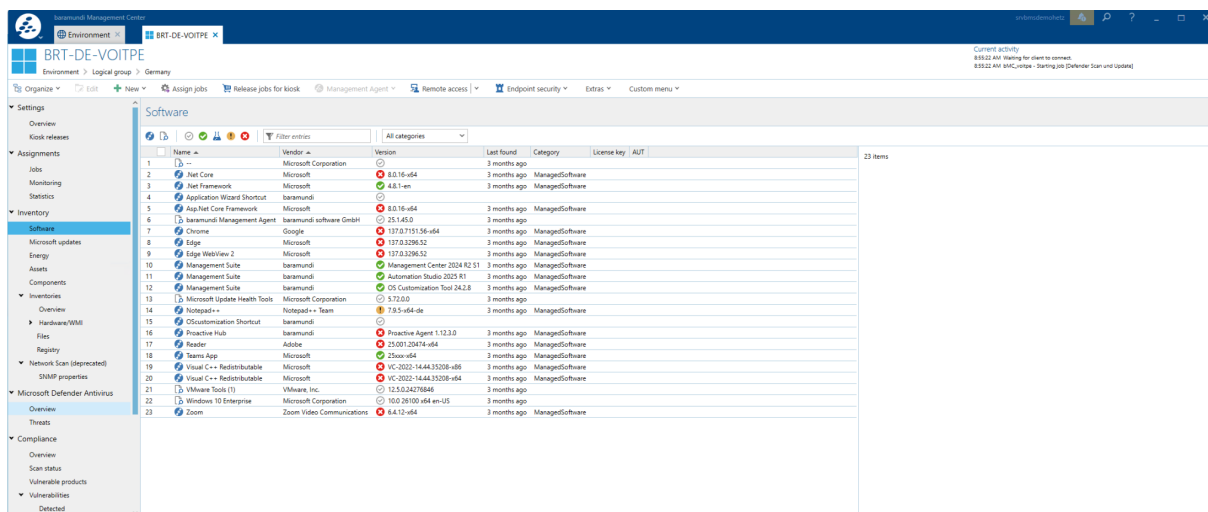
Vendor	Name	Version	Download state	Category	Comment
1	Adobe Reader	25.001.20630-64	Download complete	ManagedSoftware	
2	Adobe Reader	25.001.20623-64	Download complete	ManagedSoftware	
3	Adobe Reader	25.001.20771-64	Download complete	ManagedSoftware	
4	Adobe Reader	25.001.20566-64	Download complete	ManagedSoftware	
5	Adobe Reader	25.001.20531-64	Download complete	ManagedSoftware	
6	Adobe Reader	25.001.20521-64	Download complete	ManagedSoftware	
7	Adobe Reader	25.001.20474-64	Download complete	ManagedSoftware	
8	Adobe Reader	25.001.20438-64	Download complete	ManagedSoftware	
9	Adobe Reader	25.001.20423-64	Download complete	ManagedSoftware	
10	Adobe Reader	25.001.20412-64	Download complete	ManagedSoftware	
11	Adobe Reader	25.001.20428-64	Download complete	ManagedSoftware	
12	Adobe Reader	24.005.20421-64	Download complete	ManagedSoftware	
13	Adobe Reader	24.005.20411-64	Download complete	ManagedSoftware	
14	Adobe Reader	24.005.20399-64	Download complete	ManagedSoftware	
15	Adobe Reader	24.005.20392-64	Download complete	ManagedSoftware	
16	Adobe Reader	24.005.20330-64	Download complete	ManagedSoftware	
17	Adobe Reader	24.005.20307-64	Download complete	ManagedSoftware	
18	Adobe Reader	24.004.20272-64	Download complete	ManagedSoftware	
19	Adobe Reader	24.004.20242-64	Download complete	ManagedSoftware	
20	Adobe Reader	24.004.20220-64	Download complete	ManagedSoftware	
21	Adobe Reader	24.003.20180-64	Download complete	ManagedSoftware	
22	Adobe Reader	24.003.20112-64	Download complete	ManagedSoftware	
23	Adobe Reader	24.003.20054-64	Download complete	ManagedSoftware	
24	Adobe Reader	24.002.21005-64	Download complete	ManagedSoftware	
25	Adobe Reader	24.002.20991-64	Download complete	ManagedSoftware	
26	Adobe Reader	24.002.20965-64	Download complete	ManagedSoftware	
27	Adobe Reader	24.002.20933-64	Download complete	ManagedSoftware	
28	Adobe Reader	24.002.20895-64	Download complete	ManagedSoftware	
29	Adobe Reader	24.002.20857-64	Download complete	ManagedSoftware	
30	Adobe Reader	24.002.20758-64	Download complete	ManagedSoftware	
31	Adobe Reader	24.002.20736-64	Download complete	ManagedSoftware	
32	Adobe Reader	24.002.20687-64	Download complete	ManagedSoftware	
33	Adobe Reader	24.001.20649-64	Not downloaded	ManagedSoftware	
34	Adobe Reader	24.001.20611-64	Not downloaded	ManagedSoftware	

Gotowe do przydzielenia pakiety oprogramowania o różnych poziomach dostępu

Skuteczne zarządzanie słabymi punktami systemu wymaga jednak czegoś więcej, niż tylko ich identyfikacji i instalacji patch'y. Niezbędna jest również wiedza o tym, czy aktualizacja istotna dla bezpieczeństwa rzeczywiście dotarła do wszystkich urządzeń końcowych. Instalacje mogą się nie powieść, użytkownik może zablokować ich przeprowadzanie, a notebooki używane poza firmą mogą być niedostępne. Aby zapewnić, że wszystkie luki zostaną rzeczywiście wyeliminowane, zastosowane rozwiązanie musi zatem generować komunikat zwrotny o statusie instalacji oraz ewentualnie występujących błędach.

2.3 Inwentaryzacja sprzętu i oprogramowania, zarządzanie licencjami

Pełen obraz sytuacji jest istotny nie tylko dla identyfikacji słabych punktów i zapewnienia bezpieczeństwa. Administratorzy IT muszą również przygotowywać raporty o wykorzystaniu sprzętu i oprogramowania lub też – w przypadku audytu licencji przeprowadzanego przez producenta oprogramowania – być w stanie wykazać prawidłowe przydzielanie licencji. Z punktu widzenia kosztów ważna jest identyfikacja nieużywanego oprogramowania na urządzeniach końcowych, które korzysta z drogich licencji.



	Name	Vendor	Version	Last found	Category	License key / AUT
1	...	Microsoft Corporation	...	3 months ago	ManagedSoftware	...
2	.Net Core	Microsoft	6.0.16-x64	3 months ago	ManagedSoftware	...
3	.Net Framework	Microsoft	4.8.1-en	3 months ago	ManagedSoftware	...
4	Application Wizard Shortcut	baramundi	...	3 months ago	ManagedSoftware	...
5	Asp.Net Core Framework	Microsoft	6.0.16-x64	3 months ago	ManagedSoftware	...
6	baramundi Management Agent	baramundi software GmbH	...	3 months ago	ManagedSoftware	...
7	Chrome	Google	117.0.1915.16-x64	3 months ago	ManagedSoftware	...
8	Edge	Microsoft	117.0.2296.52	3 months ago	ManagedSoftware	...
9	Edge WebView 2	Microsoft	117.0.2296.52	3 months ago	ManagedSoftware	...
10	Management Suite	baramundi	Management Center 2024 R2 S1	3 months ago	ManagedSoftware	...
11	Management Suite	baramundi	Automation Studio 2025 R1	3 months ago	ManagedSoftware	...
12	Management Suite	baramundi	OS Customization Tool 24.2.8	3 months ago	ManagedSoftware	...
13	Microsoft Update Health Tools	Microsoft Corporation	5.72.0.0	3 months ago	ManagedSoftware	...
14	Notepad++	Notepad++ Team	7.9.5-x64-de	3 months ago	ManagedSoftware	...
15	OSCustomization Shortcut	baramundi	...	3 months ago	ManagedSoftware	...
16	Proactive Hub	baramundi	Proactive Agent 1.12.3.0	3 months ago	ManagedSoftware	...
17	Reactor	Adaptive	15.001.22478-x64	3 months ago	ManagedSoftware	...
18	Teams App	Microsoft	250xx-x64	3 months ago	ManagedSoftware	...
19	Visual C++ Redistributable	Microsoft	VC-2022-14.44.35208-x66	3 months ago	ManagedSoftware	...
20	Visual C++ Redistributable	Microsoft	VC-2022-14.44.35208-x64	3 months ago	ManagedSoftware	...
21	VMware Tools (I)	VMware, Inc.	12.5.5.24278646	3 months ago	ManagedSoftware	...
22	Windows 10 Enterprise	Microsoft Corporation	10.0.20100-x64-en-US	3 months ago	ManagedSoftware	...
23	Zoom	Zoom Video Communications	6.4.12-x64	3 months ago	ManagedSoftware	...

Lista zainstalowanego oprogramowania

Automatyczna ewidencja za pośrednictwem oprogramowania do zarządzania umożliwia precyzyjne i szybkie ustalenie, jaki sprzęt i oprogramowanie są używane w sieci firmowej. Dzięki temu aktualna baza danych jest przez cały czas dostępna na potrzeby analiz zarządczych. Zachowanie pełnego obrazu sytuacji jest trudne, w szczególności w związku z licencjami zbiorczymi i aktualizacyjnymi. W tym przypadku przejrzystość i zgodność zapewnia rozwiązanie do zarządzania licencjami, które można za pośrednictwem interfejsu połączyć z aplikacją administrującą.

Dodatkowo można też określić stopień faktycznego wykorzystania programu, co pozwala na eliminację zbędnych kosztów. W tym celu protokołuje się uruchomienie aplikacji na poszczególnych urządzeniach końcowych. Pokazuje to, na których komputerach program jest nieużywany w określonym czasie – i na których licencjach można zatem zaoszczędzić. Ważne: zastosowane rozwiązanie musi przy tym być zgodne z europejskimi przepisami o ochronie danych i nie może dopuszczać monitorowania indywidualnych zachowań pracowników.

Automatyczna ewidencja niesie ze sobą korzyści również dla działu wsparcia IT: rozwiązania stosowane przez helpdesk można połączyć z oprogramowaniem do zarządzania za pośrednictwem interfejsów. W ten sposób pracownicy działu wsparcia mogą w razie zapytań szybko zarejestrować sprzęt i oprogramowanie używane na danym stanowisku pracy. Prawidłowe informacje o danym urządzeniu końcowym są kluczowe dla szybkiego i kompetentnego opracowania sprawy użytkownika.

2.4 Inteligentna automatyzacja: sterowanie czasowe i samoobsługa

W wielu firmach wprowadzono fazy obsługi technicznej, dla których zakłada się, że zadania administracyjne mogą być przeprowadzane na określonych komputerach wyłącznie w ustalonym czasie. Wydajne oprogramowanie do zarządzania udostępnia zatem zadania sterowane czasowo. Dzięki temu możliwe jest precyzyjne zlecenie instalacji łąt na urządzeniu końcowym w określonym czasie.

Z kolei zadania sterowane zdarzeniami odciążają administratora IT w działaniach związanych z reagowaniem na występujące zdarzenia. Na przykład: gdy w ramach inwentaryzacji przeprowadzanej na urządzeniu końcowym zostanie znaleziona gra XY, powinna zostać automatycznie usunięta. Zamiast podejmować działanie w każdym przypadku znalezienia gry, administrator otrzymuje teraz tylko raport dotyczący jej odinstalowania.

Dla administratorów i użytkowników wygodna jest również możliwość udostępniania przygotowanych procesów instalacyjnych w punkcie samoobsługowym (tzw. Kiosku). Pozwala to na szybkie i nieskomplikowane opracowywanie standardowych kwestii, takich jak instalacja Firefoksa – i to dokładnie wtedy, gdy użytkownik potrzebuje tego do niezakłóconej pracy. Jednocześnie zmniejsza to zapotrzebowanie na wsparcie, gdyż zadanie to jest realizowane w pełni automatycznie. Administrator zachowuje jednak pełną kontrolę również nad tego rodzaju samodzielnymi instalacjami.

Ponadto wydajne oprogramowanie do zarządzania umożliwia włączenie użytkowników do procesów instalacyjnych, pozostawiając jednocześnie kontrolę w rękach administratora. Przykładowo użytkownik może otrzymać prawo do przekładania w określonym przedziale czasowym instalacji łąty, która wymaga ponownego uruchomienia urządzenia. Dzięki temu współpracownicy mogą wykonywać swoje zadania bez zakłóceń, a instalacja przebiega podczas przerwy na kawę. Jednocześnie ma się pewność, że przydzielanie istotnych patch'y nie będzie przeciągać się w nieskończoność.

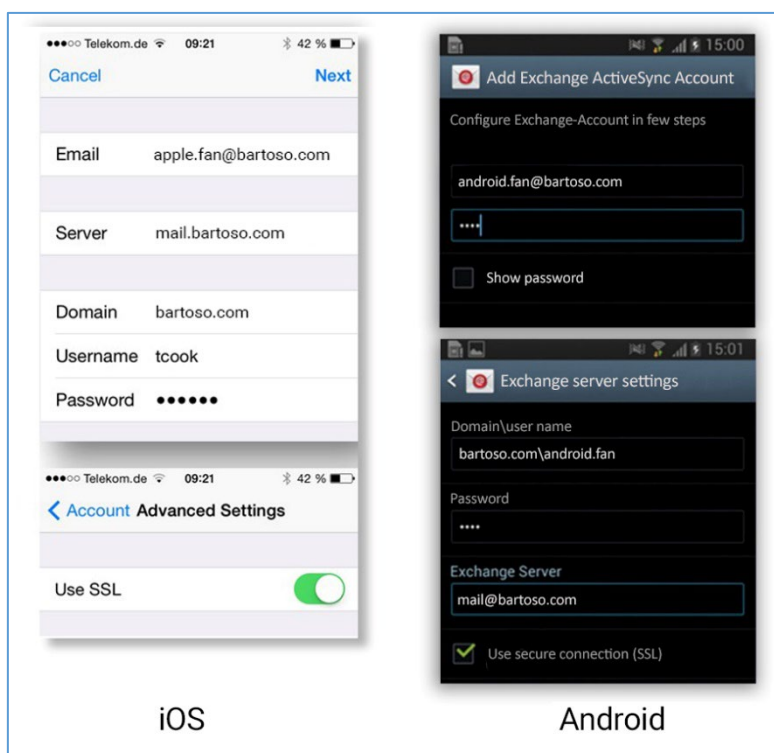
2.5 Integracja z dotychczasową infrastrukturą

Oprogramowania do zarządzania nie należy traktować jako nowej wyspy na morzu istniejącej infrastruktury. Aby umożliwić niezakłóconą integrację, oprogramowanie to musi mieć do dyspozycji nowoczesne interfejsy. Tylko w ten sposób można zautomatyzować także pozostałe procesy organizacyjne. Przykładowo po wprowadzeniu nowego komputera osobistego do systemu ERP w rozwiązaniu do zarządzania możliwe jest automatyczne utworzenie urządzenia końcowego ze wszystkimi istotnymi danymi, takimi jak numer inwentaryzacyjny, centrum kosztów itd., oraz natychmiastowe zapewnienie mu oprogramowania i konfiguracji.

3 Zarządzanie urządzeniami mobilnymi

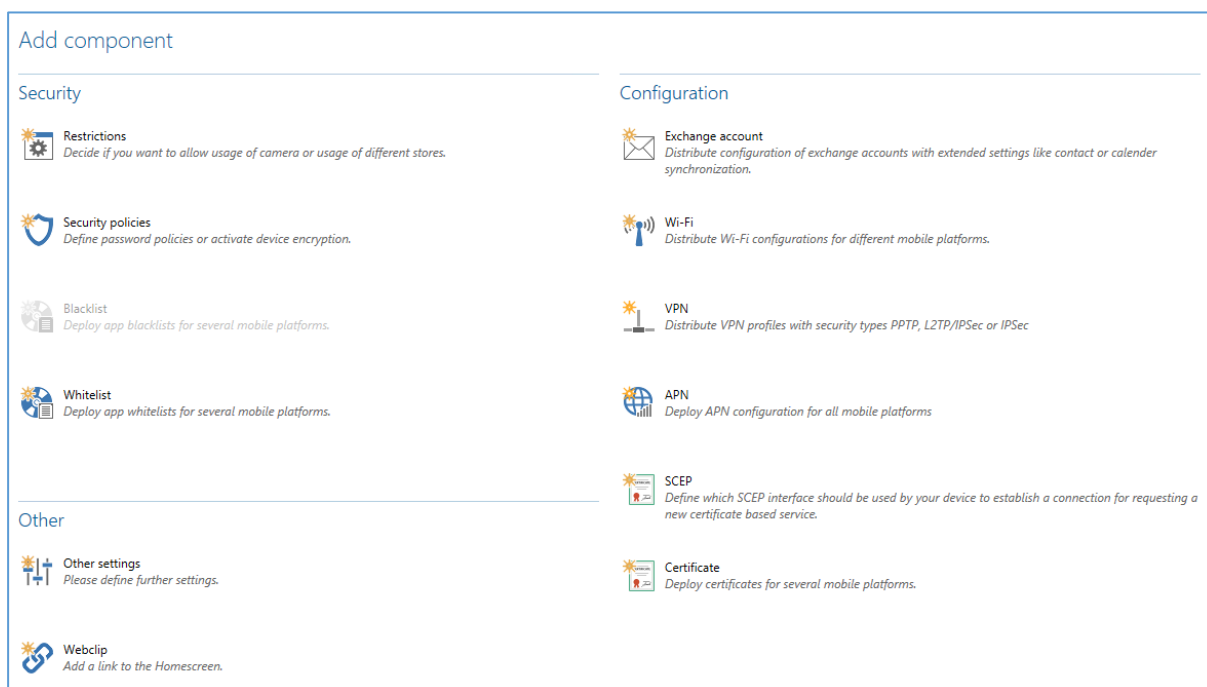
Używanie urządzeń mobilnych stało się w wielu firmach standardem; liczni pracownicy chcą mieć możliwość dostępu do danych firmowych ze swoich urządzeń mobilnych. Firmy mogą z tego czerpać pewne korzyści, jednak administratorzy IT muszą być świadomi ryzyka, jakie to rozwiązanie z sobą niesie. Aby móc bezpiecznie włączyć laptopy, tablety i smartfony w codzienne życie zawodowe pracowników, absolutnie koniecznym warunkiem jest efektywna ochrona połączona z inwentaryzacją zasobów IT. W idealnym przypadku system zarządzania urządzeniami mobilnymi jest zintegrowany z rozwiązaniem UEM, gdyż wiele zadań związanych z administrowaniem tymi urządzeniami można również zautomatyzować.

Gdy na przykład porównamy trzy najpopularniejsze platformy mobilne: iOS oraz Android, szybko okazuje się, że w celu utworzenia kont Exchange w różnych miejscach trzeba wprowadzać takie parametry jak imię i nazwisko, adres e-mail, serwer, domena czy szyfrowanie. W praktyce oznacza to ogromne obciążenie i wymaga od administratora znajomości wszystkich masek wprowadzania. Ten przepływ pracy można znacznie uprościć dzięki zastosowaniu wieloplatformowych modułów profili oraz centralnemu zarządzaniu urządzeniami.



Konfiguracja Exchange na różnych platformach mobilnych

W tym celu smartfon lub tablet należy jednorazowo zarejestrować w systemie administracyjnym („enrollment”) np. korzystając z programu Device Enrollment Program (DEP) firmy Apple, lub skanując kod QR. Zadania administracyjne – przykładowo konfiguracja Exchange – mogą być potem wykonywane centralnie za pośrednictwem rozwiązania do zarządzania. Odpowiednie ustawienia są wprowadzane na ujednoliconym, wieloplatformowym interfejsie; potem można je dystrybuować na administrowane urządzenia.



Wieloplatformowe moduły profili do konfigurowania mobilnych urządzeń końcowych

Zalety takiego rozwiązania są oczywiste: administrator nie musi już wiedzieć, kto i na jakim urządzeniu mobilnym dokonał danych ustawień – cały czas korzysta ze znanego interfejsu swojej centralnej konsoli administracyjnej. Takie rozwiązanie zmniejsza złożoność, oszczędza czas i ogranicza podatność procesów na błędy. Efektem jest również zwiększenie poziomu bezpieczeństwa.

Kolejna zaleta: dzięki oprogramowaniu do zarządzania zadania można również wykonywać zdalnie – administrator w ogóle nie musi się zbliżać do urządzenia. Jeżeli na przykład użytkownik znajdujący się w innym oddziale uruchomi nowe urządzenie z systemem iOS, zostanie to automatycznie odnotowane w systemie zarządzania za pośrednictwem Apple DEP. Następnie administrator może dokonać dalszej konfiguracji. Stosowane przy tym procesy i zadania można opracowywać i wykorzystywać wielokrotnie – również dla dużej liczby urządzeń jednocześnie.

Ponadto urządzenia mobilne mogą łatwiej „znikać” niż komputery stacjonarne. W związku z tym konieczne jest przedsięwzięcie odpowiednich środków zaradczych. Pod uwagę bierze się

m.in. automatyczną blokadę po wyłączeniu ekranu, możliwość zdalnego usunięcia wybranego profilu i wreszcie przydzielanie silniejszych haseł.

W dalszej kolejności należy zapewnić, aby administrator miał stałą kontrolę nad urządzeniami i na przykład otrzymywał powiadomienia o wywoływanych przez użytkownika zagrożeniach dla systemu operacyjnego.

Z tego powodu rozwiązanie do zarządzania powinno oferować możliwość definiowania zasad zgodności, które będą poddawane regularnej, automatycznej weryfikacji. Administrator będzie otrzymywał informacje naruszeniach, co da mu możliwość podjęcia środków zaradczych – takich jak wysłanie wiadomości e-mail do użytkownika, a nawet zdalne usunięcie urządzenia z sieci. Równie istotne, jak zapobieganie manipulowaniu oprogramowaniem układowym, jest jego terminowe aktualizowanie tuż po udostępnieniu nowej wersji przez producenta. Z reguły zawiera ona nie tylko nowe funkcje, lecz również usuwa słabe punkty poprzedniej wersji. Na nowoczesnych platformach istnieje już możliwość zdalnego sterowania tego rodzaju aktualizacjami.

Aby zapobiec uruchamianiu niebezpiecznych aplikacji lub udostępnić szereg aplikacji uznanych przez firmę za zaufane, rozwiązanie do zarządzania powinno obsługiwać funkcję tzw. czarnej lub białej listy. Administrator może wówczas zapobiec instalacji lub uruchomieniu niepożądanych aplikacji na kompatybilnych urządzeniach mobilnych. Z kolei funkcja białej listy umożliwia określenie aplikacji wyraźnie dozwolonych, co uniemożliwia instalację lub uruchamianie pozostałych programów.

Zależnie od preferencji administratora dla danego urządzenia końcowego można zastosować funkcję czarnej lub białej listy. Po podjęciu decyzji co do rodzaju listy zostają na nią wpisane odpowiednie aplikacje; całość jest potem przesyłana na urządzenie mobilne jako profil.

Jako aktywny członek społeczności AppConfig – inicjatywy wiodących producentów rozwiązań EMM – firma baramundi obrała za cel uproszczenie przydzielania i konfigurowanie aplikacji z wykorzystaniem natywnych rozwiązań producentów systemów operacyjnych. Pakiet oferuje różnorodne funkcje do Mobile Device Management (MDM) i Mobile Application Management (MAM), a przez odpowiednie aplikacje firm zewnętrznych z obszaru zarządzania dokumentami (DMS) i danymi osobowymi (PIM) został wzbogacony o funkcje do zarządzania treścią urządzeń mobilnych (MCM). Połączenie tych obszarów odbywa się dzięki standardom konfiguracyjnym na poziomie iOS i AppConfig, tak aby rozwiązanie do zarządzania mogło również zagwarantować wygodne przydzielanie i konfigurowanie funkcji MCM, których zasadnicze funkcjonalności, takie jak synchronizacja i obróbka danych, pozostają zastrzeżone dla aplikacji firm zewnętrznych.

Integracja systemu Enterprise Mobility Management z pakietem oprogramowania do zarządzania urządzeniami końcowymi nie tylko eliminuje nakłady ponoszone na konfigurację, konserwację i obsługę – umożliwia również zarządzanie urządzeniami mobilnymi i

komputerami stacjonarnymi we wspólnych grupach i jednostkach organizacyjnych oraz wdrażanie jednolitych standardów. Takie podejście uważa się za bardziej przyszłościowe z uwagi na możliwość łatwiejszego włączania nowych klas urządzeń do jednolitego rozwiązania.

4 Bezpieczeństwo i ochrona danych

Administrowanie systemem informatycznym oznacza również odpowiedzialność za zabezpieczanie i bezpieczeństwo danych. W związku z tym kluczowe jest automatyczne tworzenie kopii zapasowych. Umożliwia to łatwe i proste odtworzenie danych i ustawień użytkownika w razie awarii – włącznie ze słownikiem i ikonami na pulpicie. Dzięki oprogramowaniu do zarządzania można zautomatyzować także te procesy, w tym wynikające z dyrektywy RODO.

Równie istotne jest postępowanie zgodnie z obowiązującymi przepisami o ochronie danych. Ponieważ w oparciu o liczne dane użytkowników, potencjalnie gromadzonych przez system administracyjny, możliwe byłoby określenie indywidualnych zachowań tych osób, konieczne jest zapewnienie przestrzegania tych regulacji – na przykład poprzez zróżnicowane zarządzanie uprawnieniami, bądź syntetyczne prezentowanie i przechowywanie danych. Dlatego ważne jest, aby producent rozwiązania do zarządzania uwzględnił obowiązujące przepisy o ochronie danych osobowych już na etapie projektowania rozwiązania i wdrożył je w odpowiedni sposób.

baramundi software GmbH

Firma baramundi software rozwija zintegrowane zarządzanie punktami końcowymi do centralnego zarządzania komputerami, urządzeniami mobilnymi i serwerami. Automatyzuje dystrybucję oprogramowania, upraszcza zarządzanie poprawkami i zapewnia przejrzystość w sieci. baramundi wnosi w ten sposób znaczący wkład w bezpieczeństwo IT i redukuje zasoby.

www.baramundi.com

Wersja testowa baramundi Management Suite

Mogą Państwo otrzymać bezpłatną 30-dniową pełną wersję baramundi Management Suite i przetestować samodzielnie rozwiązanie od początku do końca. Dowiedzą się Państwo, jak zautomatyzować czasochłonne rutynowe zadania, zaoszczędzić cenne zasoby i zyskać czas na produktywnie czynności.

[Prośba o bezpłatną wersję testową!](#)

**Cieszymy się, mogąc
Państwa poznać!**

Zachęcamy do kontaktu!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +34 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com