Remote System Management

CBS-RM-DIPx

pl Opis usługi

Spis treści

1 Główne funkcje

Usługa Remote System Management firmy Bosch pozwala wykorzystać internet rzeczy (Internet of Things — IoT) do bezpiecznego, transparentnego i ekonomicznego zarządzania zasobami w całym okresie eksploatacji systemu wizyjnego. Usługa ta umożliwia użytkownikom końcowym, integratorom systemów i instalatorom wykonywanie zadań związanych z inwentaryzacją i zarządzaniem aktualizacjami oraz monitorowaniem stanu całego systemu wizyjnego firmy Bosch (DIVAR IP + BVMS + kamery) za pomocą ujednoliconej, centralnej platformy Remote Portal.

Usługa zapewnia spokój ducha klientom końcowym, umożliwiając bezpieczne, całodobowe monitorowanie systemu. Dzięki temu użytkownik może działać proaktywnie w przypadku pojawienia się problemów i rozwiązać je, zanim na przykład nagrania wideo zostaną utracone z powodu awarii dysku twardego. Bezpieczne połączenie MQTTS pozwala również zachować prywatność danych — uniemożliwia ono zyskanie dostępu do materiału wideo za pośrednictwem tego połączenia, ze względu protokół ten nie obsługuje przesyłania danych wideo i obrazów. Ponadto usługa pozwala na zdalne aktualizowanie oprogramowania i firmware'u, co pozwala na utrzymanie systemu w aktualnej wersji i pełnym bezpieczeństwie. Łączność w chmurze opiera się na pojedynczym połączeniu wychodzącym z DIVAR IP do Remote Portal. DIVAR IP konsoliduje całą komunikację przychodzącą i wychodzącą dla całego systemu wizyjnego.

Usługa została zaprojektowana z myślą o większych organizacjach i klientach prowadzących konserwację systemu w wielu rozproszonych lokalizacjach lub o instalatorach oferujących takie usługi różnym klientom. Korzyści płynące z użytkowania Remote System Management koncentrują się na sprawniejszym wykonywaniu zadań związanych z utrzymaniem systemu i unikaniu niepotrzebnych wizyt na miejscu dzięki funkcjom zdalnej obsługi — takim jak wprowadzanie aktualizacji w przypadku alertu bezpieczeństwa lub pozyskiwanie bieżących informacji o systemie pozwalającym na lepsze przygotowanie się do wizyty. Pozytywny efekt uboczny: Pełna obsługa przy minimalnej emisji CO_2. Ponadto możliwe jest zwiększenie jakości świadczonych usług poprzez działania proaktywne rozwiązywanie problemów zanim (wewnętrzni) klienci uświadomią sobie, że zachodzi jakiś problem.
Szczegóły dotyczące funkcji podano w odpowiednich kartach katalogowych serwisu.

Uwaga!

Karty katalogowe są dostępne w katalogu produktów właściwym dla danego regionu lub kraju.

2 Wymagania systemowe

Wymagania programowe

Interfejs internetowy Remote Portal może być używany w nowoczesnych przeglądarkach internetowych obsługujących standard HTML5. Aby uzyskać najlepsze wrażenia, Bosch zaleca korzystanie z przeglądarki Google Chrome.

Wymagania dotyczące urządzenia

Dla zyskania dostępu do pełnej funkcjonalności rozwiązania Remote System Management, kamery sieciowe Bosch muszą być wyposażone w oprogramowanie sprzętowe w wersji 6.50 lub nowszej.

Zgodnie z informacją w karcie katalogowej obsługiwane są tylko określone modele urządzeń DIVAR IP. W przypadku tych modeli minimalnym wymogiem jest obsługa DIVAR IP System Manager w wersji 2.0 lub nowszej. Szczegóły podano w odpowiednich kartach katalogowych.

Wymagana szerokość pasma zależy od specyfikacji systemu wizyjnego oraz struktury obiektu, tj. liczby kamer i urządzeń DIVAR IP w obiekcie. Bosch zaleca minimalną szerokość pasma 11 Mb/s lub 1,31 Mb/s na każde urządzenie DIVAR IP — system DIVAR IP konsoliduje komunikację przychodzącą i wychodzącą realizowaną przez siebie oraz przez podłączone kamery. Zalecenie to wynika z sytuacji najbardziej wymagającej względem przepustowości, a mianowicie pobierania większych plików aktualizacji przez system Remote Portal. Większość pozostałych zadań wymaga przepustowości około 10 Kb/s do monitorowania parametrów stanu i wymiany innych danych telemetrycznych.

Uwaga!

Zapotrzebowanie na pasmo może być zmienne. Użytkownik powinien sprawdzić, czy dostępne pasmo spełnia wymagania aplikacji. Firma Bosch udostępnia kilka narzędzi do obliczania wymaganej szerokości pasma i nie ponosi odpowiedzialności za rzeczywistą dostępność pasma i prawidłową konfigurację.

3 Aplikacja internetowa

System Remote System Management jest zintegrowany z rozwiązaniem Remote Portal, centralną platformą internetowa do aktywacji usług oraz oferującej opisane niżej dodatkowe funkcje.

Zarządzanie systemem i urządzeniem z pulpitu nawigacyjnego
Systemy i urządzenia można porządkować w układzie hierarchicznym dopasowanym do klienta lub instalacji, ograniczyć dostęp do wybranych urządzeń lub zagregować stan wielu urządzeń.

Przegląd usługi
Sekcja Usługi zawiera przegląd wszystkich usług oferowanych przez rozwiązanie Remote Portal dla różnych urządzeń. Każda usługa oferuje skonsolidowaną informację o wszystkich urządzeniach i systemach, w których jest używana.

Zarządzanie licencjami na usługi
Po pierwszym uruchomieniu urządzenia DIVAR IP w ramach rozwiązania Remote Portal usługi można aktywować, przechodząc do Remote Portal.
Do aktywacji usługi Remote System Management potrzebna jest licencja. Rodzaj licencji zależy od modelu urządzenia DIVAR IP oraz trybu pracy. Szczegóły podano w kartach katalogowych.
Zarządzanie licencjami oraz ich aktywacja jest wykonywana w rozwiązaniu Remote Portal, w sekcji Service licensing (Licencjonowanie usług).

Zarządzanie użytkownikami
Aplikacja Remote Portal pozwala na precyzyjną kontrolę dostępu do urządzeń i usług. Poprzez zarządzanie rolami *administratorzy*, *technicy* i *użytkownicy końcowi* mogą być indywidualnie powiązywani z systemami, grupami i usługami.

Uwaga!

Więcej informacji na temat rozwiązania Remote Portal jest dostępnych na stronie produktu: https://commerce.boschsecurity.com/gb/en/Remote-Portal/p/86180387339/

4 Dokumentacja

Dokumentacja użytkownika i karty katalogowe wszystkich poszczególnych systemów opartych na urządzeniach DIVAR IP są dostępne w tym miejscu:

Szkolenia techniczne: https://academy.boschsecurity.com/

UWAGA: udostępnione zostanie także oddzielne szkolenie wprowadzające Remote System Management. Zostanie ono później włączone do szkolenia certyfikacyjnego DIVAR IP all-in-one.

Jak to zrobić / Konfiguracja: https://community.boschsecurity.com/t5/Security-Video/tkb-p/bt_community-tkb-video/label-name/remote_system_mgmt?labels=remote_system_mgmt

Karty katalogowe / Zastosowania: https://commerce.boschsecurity.com/gb/en/bt/search/?text=cbs-rm-dip

5 Składniki oprogramowania o otwartym źródle

Wchodzące w skład platformy Remote Portal składniki oprogramowania o otwartym źródle są dostępne tutaj: https://remote.boschsecurity.com/open_source/open_source_licenses.txt

6 Hosting usług

Usługi wymienione tutaj są hostowane w ramach platformy AWS typu infrastruktura-jako-usługa.
Aplikacja Remote Portal jest globalną platformą typu multi-tenant. Platforma, jej baza danych, backend i frontend są hostowane w regionie AWS we Frankfurcie, w Niemczech.

7 Poziom konserwacji i usługi

Bosch oferuje specjalną umowę o poziomie usług (SLA) dla certyfikowanych sprzedawców rozwiązania Remote System Management Bosch. Umowa SLA zawiera informacje o gwarantowanej dostępności, zasadach konserwacji i procesie wsparcia rozwiązania Remote System Management zapewnianych przez firmę Bosch oraz zawiera dane kontaktowe infolinii alarmowych, klauzule dotyczące kar itp.
Aby uzyskać więcej informacji, skontaktuj się z lokalnym przedstawicielem handlowym.

8 Zobowiązania klienta i użytkownika

W przypadku bezpośrednich klientów firmy Bosch do uzyskania licencji albo subskrypcji na rozwiązanie Remote System Management niezbędna jest akceptacja regulaminu oferty oprogramowanie-jako-usługa. W celu aktywacji licencji na usługi lub subskrypcji użytkownicy muszą wyrazić zgodę na regulamin aplikacji Remote Portal. Dalsze obowiązki obejmują:

- 8.1. Za połączenie internetowe między Klientem, jego centrum monitoringu/sterownią oraz miejscem instalacji kompatybilnych urządzeń (w tym kamer wideo, zwanych dalej „Urządzeniami")” do interfejsu internetowego centrum danych używanego przez firmę Bosch, jak również za połączenie między Klientem i jego partnerami umownymi odpowiadają wyłącznie Klienci.
- 8.2. Instalacja, obsługa, konserwacja i w razie potrzeby naprawa urządzeń są wyłączną odpowiedzialnością klientów.
- 8.3. Aplikacja nie jest zaprojektowana do użytku w zastosowaniach o wysokim stopniu ryzyka i nie jest udzielana żadna gwarancja dotycząca takich zastosowań, gdzie zastosowania o wysokim stopniu ryzyka oznaczają wymóg specjalnych mechanizmów chroniących przed awarią i są nimi eksploatacja obiektów jądrowych, kontrola ruchu lotniczego, podtrzymywanie życia lub inne zastosowania, urządzenia lub systemy, w których awaria urządzenia lub aplikacji może prowadzić bezpośrednio do śmierci, obrażeń ciała lub poważnych szkód fizycznych lub środowiskowych („działania o wysokim stopniu zagrożenia”). Niezależnie od wszelkich innych postanowień klienci nie powinni używać Aplikacji do działań o wysokim ryzyku ani pozwalać podmiotom zewnętrznym na takie używanie.
- 8.4. Należy uzyskać niezbędne zgody osób, których to dotyczy, zgodnie z przepisami dotyczącymi bezpieczeństwa danych i ochrony danych. Podczas używania aplikacji przez te osoby są gromadzone, przetwarzane lub wykorzystywane dane osobowe, a w danym przypadku nie obowiązują przepisy zezwalające na gromadzenie, przetwarzanie lub wykorzystywanie bez konieczności uzyskania zgody.
- 8.5. Przed wysłaniem danych i informacji do firmy Bosch należy sprawdzić, czy nie zawierają one wirusów lub innego złośliwego oprogramowania, a także upewnić się, że programy antywirusowe spełniają najnowsze wymagania.
- 8.6. Wady usług objętych umową należy zgłaszać do firmy Bosch niezwłocznie po uzyskaniu ich ujawnieniu. W przypadku opóźnienia w wysłaniu powiadomienia lub w przypadku braku zawiadomienia mimo ujawnienia wady, wyklucza się jednostronne obniżenie opłaty, zawieszenie usługi przez klienta albo nadzwyczajne rozwiązanie umowy.
- 8.7. Poniższe role i zadania są wyłączną odpowiedzialnością klienta:
  - 8.7.1. Przypisywanie ról i uprawnień odpowiednim osobom lub jednostkom dla ról użytkowników dostępnych w aplikacji Remote Portal oraz zarządzanie tymi rolami i uprawnieniami.
  - 8.7.2. Przydzielanie urządzeń partnerom umownym klienta oraz stronom partnerów umownych.
  - 8.7.3. Zamawianie, instalacja i podłączanie urządzeń do pracy zgodnie z wymaganiami systemu. Aplikacja wspiera obsługę urządzeń przez klienta przy użyciu przedstawionych funkcji.

9 Informacje związane z RODO

Cel przetwarzania danych

Bosch przetwarza dane osobowe tylko w takim zakresie i w taki sposób, w jaki jest to konieczne:

1. w celu wypełnienia zobowiązań firmy Bosch wynikających z umowy/regulaminu korzystania z oferty usług Remote System Management; oraz
2. w celu okazjonalnego dostosowania się do instrukcji klienta (mogą to być instrukcje szczegółowe lub instrukcje o charakterze ogólnym określone w niniejszej umowie lub w inny sposób przekazane firmie Bosch przez klienta),
3. i nie będzie przetwarzać danych osobowych w żadnym innym celu.

Kategorie danych

- Dane urządzenia: dane wprowadzone przez administratora danych lub przekazane przez urządzenie administratora danych — dane główne urządzenia, dane telemetryczne dotyczące stanu urządzenia oraz metadane dotyczące wersji oprogramowania. Lokalizacja urządzenia i osoba do kontaktu w jego sprawie. Używane dla umożliwienia realizacji rozwiązania Remote System Management na rzecz administratora danych.
- Dzienniki urządzenia: w celu umożliwienia rozwiązywania problemów z systemem działania urządzenia są rejestrowane.
- Dane konfiguracyjne użytkownika: dane wprowadzone przez administratora danych podczas używania rozwiązania, takie jak informacje o dostępie użytkownika — w tym adres IP — nazwa firmy, imię, nazwisko i adres e-mail niezbędne do zapewnienia dostępu do aplikacji użytkownika.
- Dzienniki użytkownika: dokumentacja użytkowania systemu przez użytkowników obejmująca wykonywane czynności i powiązane z nimi znaczniki czasu. Używane do pomocy w rozwiązywaniu spraw związanych z konserwacją oraz do poprawy jakości pracy.
- Dane nieosobowe, takie jak dane dotyczące witryny, konta klienta i konfiguracji usług, w tym typy i przepływy.

Osoby, których dane dotyczą

- Pracownicy klienta
- Użytkownicy końcowi lub partnerzy umowni klienta („klienci klientów”)

Podwykonawcy

Wszyscy podwykonawcy zostali wymienieni w **tab. 1**.

	Nazwa i adres podwykonawcy oraz imię i nazwisko inspektora ochrony danych osobowych albo osoby do kontaktu w przypadku pytań dotyczących ochrony prywatności	**Zakres usługi (zakres zamówienia złożony przez wykonawcę)**	**Miejsce przetwarzania danych**	**Przekazanie/ udostępnienie danych osobowych klienta (rodzaj danych i grupa osób, których dane dotyczą)**
1	Amazon Web Services (AWS)	Dostawca infrastruktury/ hostingu (zgodnie z koncepcją bezpieczeństwa), a także dostawca usług zarządzanych w zakresie przechowywania, manipulowania i wyszukiwania danych oraz łączności w chmurze	Regiony infrastruktury AWS (patrz sekcja 6)	Wszystkie kategorie i osoby, których dane dotyczą, wymienione w sekcji 9
2	Robert Bosch India Inspektor ochrony danych dla Bosch India (RBEI/DSO) DPO.India@in.bosch.com	Ograniczona grupa wsparcia operacji technicznych	No.123, Industrial Layout, Hosur Road, Koraman-galaBengaluru-560 095 Karnataka, India	Wszystkie kategorie i osoby, których dane dotyczą, wymienione w sekcji 9 Zespół operacyjny ma dostęp na poziomie systemu jedynie do aplikacji i pamięci masowej, a nie konta lub witryny
3	Bosch.IO GmbH https://www.bosch-digital.com/imprint/	Obsługa i konserwacja bazy danych cyfrowych kopii urządzeń (https://eclipse.dev/ditto/) do przechowywania, manipulowania i wyszukiwania danych urządzeń	Regiony infrastruktury AWS (patrz sekcja 6)	Kategorie danych urządzenia

Tabela 1

Środki techniczne i organizacyjne

Następujące środki techniczne i organizacyjne zostały uzgodnione między administratorem danych i podmiotem przetwarzającym dane stosownie do danego indywidualnego przypadku. Patrz: wykaz wzorów.

- I. Środki zapewniające poufność (art. 32, ust. 1 lit. b) RODO)
  - I. Fizyczna kontrola dostępu: brak możliwości nieuprawnionego dostępu do systemów przetwarzania danych.
  - II. Logiczna kontrola dostępu: brak możliwości nieautoryzowanego korzystania z systemu poprzez stosowanie bezpiecznych haseł, automatyczne mechanizmy blokujące, uwierzytelnianie dwuskładnikowe i szyfrowanie danych.
  - III. Kontrola dostępu do danych: brak możliwości nieautoryzowanego odczytu, kopiowania, zmiany lub usuwania w ramach systemu poprzez wprowadzenie mechanizmów autoryzacji i uprawnień dostępu oddzielnych dla danego użytkownika i rejestrowanie dostępu.
  - IV. Kontrola rozdzielności: oddzielne przetwarzanie danych gromadzonych w różnych celach.

- II. Środki zapewniające integralność (art. 32, ust. 1 lit. b) RODO)
  - I. Kontrola transferu: brak możliwości nieuprawnionego odczytywania, kopiowania, zmieniania lub usuwania danych podczas elektronicznej transmisji poprzez wykorzystanie szyfrowania, wirtualnych sieci prywatnych (VPN) oraz podpisów elektronicznych.
  - II. Kontrola wprowadzania danych: ustalanie, czy dane osobowe zostały wprowadzone, zmienione lub usunięte w systemach przetwarzania danych oraz kto wykonał te czynności poprzez rejestrowanie i zarządzanie dokumentami.

- III. Środki mające na celu zapewnienie dostępności i odporności (art. 32, ust. 1 lit. b) RODO), np:
  - I. Kontrola dostępności: ochrona przed przypadkowym uszkodzeniem lub zniszczeniem albo utratą danych poprzez strategię tworzenia kopii zapasowych.
  - II. Kontrola zamówień: brak możliwości przetwarzania danych w ramach zamówienia zgodnie z art. 28 RODO bez przekazania odpowiednich instrukcji ze strony administratora danych poprzez jednoznaczne zapisy umowy, sformalizowane zarządzanie zamówieniami, rygorystyczny wybór usługodawcy, obowiązek uprzedniego porozumienia oraz kontrole następcze.
  - III. Odporność: obowiązek takiego projektowania systemów i usług (np. magazynowanie, dostęp i przepustowość linii) tak, aby móc zapewnić odporność nawet na okresowo wysokie naprężenia lub stałe wysokie obciążenie procesów.

- IV. Środki służące do pseudonimizacji danych osobowych:
  - I. Rozdzielenie danych głównych administratora danych klienta od danych klienta
  - II. Używanie identyfikatorów pracowników, klientów i dostawców zamiast prawdziwych imion i nazwisk

- V. Środki służące do szyfrowania danych osobowych:
  - I. Szyfrowanie symetryczne
  - II. Szyfrowanie asymetryczne
  - III. Haszowanie

- VI. Środki mające na celu szybkie przywrócenie dostępności danych osobowych po zdarzeniu fizycznym lub technicznym poprzez mechanizmy tworzenia kopii zapasowych.

- VII. Procedury okresowego przeglądu, oceny i ewaluacji (art. 32, ust. 1 lit. d) RODO; art. 25 ust. 1 RODO):
  - I. Zarządzanie prywatnością
  - II. Zarządzanie reagowaniem na incydenty
  - III. Domyślna ochrona danych (art. 25 ust. 2 RODO)
  - IV. Ocena przez OSD, audyty informatyczne
  - V. Ocena zewnętrzna, audyty, certyfikaty

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202309141013