

Bezpieczeństwo robotów i danych w iRobot

W iRobot bardzo poważnie traktujemy bezpieczeństwo naszych produktów. Jeśli jesteście Państwo klientem iRobot i korzystają Państwo z naszych produktów połączonych z siecią, poniżej znajdują Państwo ważne informacje na temat zasad związanych z bezpieczeństwem produktów iRobot.

Najczęściej zadawane pytania dotyczące bezpieczeństwa danych iRobot

Robimy wszystko co w naszej mocy, aby zagwarantować wykorzystanie znajdujących się w naszych systemach danych w jednym celu: ułatwienia Państwu życia dzięki produktom iRobot. Poniżej znajdują Państwo odpowiedzi na najczęściej zadawane pytania dotyczące bezpieczeństwa danych w iRobot:

W jaki sposób zabezpieczamy nasze produkty połączone z siecią?

W iRobot stosujemy podejście wielopoziomowej ochrony zapewniając wiele warstw zabezpieczeń naszym robotom, chmurom i aplikacjom. Gwarantujemy, że nasze produkty spełniają wszelkie standardy branżowe dotyczące najlepszych praktyk z zakresu bezpieczeństwa, jak również korzystamy z zaawansowanych technologicznie narzędzi w celu wspierania naszych zespołów ds. projektowania i bezpieczeństwa podczas tego procesu. Po wprowadzeniu produktu na rynek, współpracujemy z naszymi dostawcami i partnerami w celu zagwarantowania, że nasze produkty oraz infrastruktura pomocnicza naszych dostawców i partnerów (w tym infrastruktura techniczna, chmury i aplikacje mobilne) są odpowiednio skonfigurowane, monitorowane oraz że wdrażane są procesy ciągłej poprawy bezpieczeństwa.

W jaki sposób przetwarzamy Państwa dane?

Wszystkie dane zbierane z produktów iRobot zgodnie z polityką prywatności są przetwarzane z dbałością i z zachowaniem wysokiego poziomu bezpieczeństwa. Dane są szyfrowane zarówno podczas transferu jak i w trakcie ich przechowywania. Dostęp do danych jest ściśle kontrolowany i ograniczony tylko do upoważnionego personelu, stale ulepszającego Państwa doświadczenia związane z korzystaniem z naszych produktów.

W jaki sposób chronione są dane podczas transferu?

Wszystkie połączone z siecią produkty iRobot komunikują się z usługą w chmurze iRobot przy pomocy niezawodnego szyfrowania. Obecnie korzystamy z 256-bitowego szyfrowania AES oraz Transport Layer Security (TLS v1.2). Szyfrowanie danych jest wzmocnione skutecznym zarządzaniem tożsamością. Wszystkie połączone z siecią produkty iRobot po opuszczeniu fabryki posiadają swoją tożsamość, która jest potwierdzana przy każdym nowym łączeniu z chmurą.

W jaki sposób przechowywane są Państwa dane?

W chmurze iRobot (powstałej na bazie AWS) dane klientów są przechowywane w formie zaszyfrowanej. Dane klientów posiadają wiele kluczy szyfrowania, które są regularnie zmieniane w celu zmniejszenia ryzyka naruszenia ochrony danych, nawet w przypadku ujawnienia klucza szyfrowania.

W ramach aplikacji mobilnej przechowywanie danych spełnia standardy platformy dotyczące danych bezpiecznych dla aplikacji. Wszelkie wrażliwe dane wykorzystywane przez aplikację nie

są przechowywane na urządzeniach mobilnych, a zamiast tego są bezpiecznie przenoszone do chmury iRobot i tam są przechowywane.

W jaki sposób uaktualniamy i zabezpieczamy nasze produkty?

W połączeniu z naszymi procesami opracowywania produktów skoncentrowanymi na bezpieczeństwie, iRobot gwarantuje, że monitorujemy i stosujemy się do wszystkich powiadomień dostawców i branży dotyczących łatek bezpieczeństwa do systemów i komponentów wykorzystywanych w naszych produktach. Co więcej, aktywnie promujemy i sponsorujemy prywatne programy „bug bounty” i eventy hackingowe w celu podejmowania współpracy ze środowiskiem zajmującym się badaniami nad bezpieczeństwem, która pomoże iRobot w odpowiedzialny sposób zająć się wszelkimi słabymi punktami, które mogą pojawić się w naszych produktach.

W jaki sposób roboty są bezpiecznie aktualizowane w domu?

W przypadku pojawienia się nowej aktualizacji, robot wchodzi w interakcję z chmurą i łączy się z bezpieczną lokalizacją w celu pobrania aktualizacji oprogramowania. Połączenie jest uwierzytelniane w celu upewnienia się, że jest to oficjalna lokalizacja iRobot. Każde pobranie aktualizacji jest kryptograficznie podpisane, aby mieć pewność, że jest to oficjalna aktualizacja iRobot.

W jaki sposób zabezpieczamy aplikację „HOME”?

Mobilna aplikacja „HOME” została stworzona zgodnie ze standardami dotyczącymi bezpieczeństwa określonymi przez producentów systemów operacyjnych i urządzeń (Apple iOS, Android, Samsung, itd.) i obejmuje zaawansowane narzędzia zaciemniania kodu w celu ograniczenia wykorzystania techniki inżynierii odwrotnej przez złośliwych użytkowników. Aplikacje mobilne są sprzedawane tylko przez certyfikowane sklepy od tych samych producentów, a użytkownicy powinni instalować aplikacje z tych stron.

W jaki sposób zabezpieczamy mapy i związane z nimi dane?

iRobot uznaje mapy domów za informacje wrażliwe i poufne. Mapy są chronione zgodnie z wytycznymi dotyczącymi standardów w branży w celu zapewnienia bezpieczeństwa tych danych, tak jak innych danych osobowych. Poza standardami wymienionymi powyżej dotyczącymi szyfrowania danych podczas transferu i przechowywania, dostęp do danych jest ściśle kontrolowany, monitorowany i regularnie sprawdzany. Urządzenia iRobot mające dostęp do tych danych posiadają oprogramowanie zapobiegające wyciekom danych oraz gwarantujące ich śledzenie w trakcie ich wykorzystania w celu wsparcia klienta i podczas procesów ulepszania robotów.

Jak bezpieczne jest korzystanie z aplikacji innej niż ta dostarczana przez iRobot?

iRobot wprowadza innowacje i pozwala na to, żeby oprogramowanie stron trzecich wchodziło w interakcje z naszymi produktami, jeśli dane oprogramowanie posiada odpowiednie poświadczenia. W rezultacie niezależni programiści mogą tworzyć narzędzia i akcesoria, które mogą poprawić doświadczenie użytkownika. Bezpieczeństwo Twoich danych generowanych przez robota i przechowywanych w chmurze iRobot pozostaje nienaruszone, jednak iRobot rekomenduje weryfikację usług stron trzecich pod względem tego, w jaki sposób przetwarzane są Twoje dane.

Przyszłe produkty i bezpieczeństwo

Zagrożenia dla bezpieczeństwa cały czas ewoluują, tak samo jak bezpieczeństwo w iRobot. iRobot cały czas rozwija się, prowadzi badania oraz wdraża procesy w celu ulepszania ogólnych możliwości firmy w zakresie bezzwłocznego identyfikowania, reagowania, izolowania i rozwiązywania problemów dotyczących naszej firmy i naszych produktów.

W celu uzyskania szczegółowych informacji dotyczących zasad i naszego podejścia do prywatności lub danych klientów, prosimy o zapoznanie się z naszą polityką prywatności.

Jeśli mają Państwo dodatkowe pytania, prosimy o [kontakt mailowy](#).

Polityka prywatności

iRobot Corporation zobowiązuje się chronić Państwa prywatność. Prosimy o zapoznanie się z [polityką prywatności iRobot](#).

Jeśli prowadzą Państwo badania w zakresie bezpieczeństwa i znaleźli Państwo błąd w którymś z naszych połączonych z siecią produktów, prosimy o kontakt! Prosimy o zapoznanie się z naszym programem „Bug Bounty” i jego zasadami jak również o przedłożenie wyników swoich badań do rozpatrzenia.

W przypadku dodatkowych pytań, prosimy o [kontakt mailowy](#).

Robot & Data Security at iRobot

At iRobot, we take the security of our products very seriously. If you're an iRobot customer, and you use our connected products, here is all the information you need to know about iRobot's product security principles.

Frequently asked questions about iRobot data security

We do everything in our control to make sure the data we have in our system is used for one purpose: making your life easier with iRobot products. Below are some answers to commonly asked questions regarding the security of the data we have at iRobot:

How do we secure our connected products?

At iRobot, we take a defense-in-depth approach to security, adding multiple layers of protection around our robots, cloud and apps from start to finish. We ensure that the development of our products follows industry-standard security best practices, and we are using technology-leading tools to assist our development and security teams during this process. When deployed to market, we work with our suppliers and partners to ensure that our products and our suppliers' and partners' supporting infrastructure (including physical infrastructure, cloud and mobile apps) are properly configured, monitored and continuous security improvement processes are in place.

How do we handle your data?

All the data collected from your iRobot products as per the Privacy policy is handled with care and high levels of security. The data is encrypted both in transit and at rest. Data access is controlled strictly and limited only to authorized personnel to do their job and help improve your product experiences.

How is data secure while in transit?

All iRobot connected products communicate with the iRobot cloud service using robust encryption. Currently, we use AES 256-bit encryption and Transport Layer Security (TLS v1.2). Data encryption is augmented through strong identity management. All iRobot connected products have identities when they come out of the factory and those identities are validated upon each new cloud connection.

How is data stored at rest?

Within iRobot's cloud (built on top of AWS), customer data is stored encrypted. Customer data has multiple encryption keys which are rotated on a regular basis to reduce the risk of the data being compromised even in the event of a key exposure.

Within the mobile application, data storage follows the platform's standards for application-secure data; any sensitive data that is used by the application is not stored on the mobile device, but is instead securely transported to iRobot's cloud for storage.

How do we keep our products up-to-date and secure?

In conjunction with our security-minded development processes, iRobot ensures that we monitor and adhere to all supplier and industry alerts regarding security patches to systems and components used in our products. Additionally, we actively promote and sponsor private bug bounty programs and hacking events to collaborate with the broad security research community to assist iRobot to responsibly address any vulnerabilities that may be discovered in our products.

How are the robots securely updated in the home?

When a robot requires an update, the robots are notified of the available update when they interact with the cloud and connect to a secure location to download a software update. The connection is authenticated to ensure it is the official iRobot location. Each download is cryptographically signed to assure it is an official iRobot update.

How do we secure the iRobot Home App?

The mobile iRobot Home application is built to the security standards as specified by the manufacturers of the operating systems and devices (Apple iOS, Android, Samsung, etc.), and include advanced obfuscation tools to limit reverse-engineering by malicious users. The mobile apps are sold only through qualified application stores from these same manufacturers, and users should only install the app from these sites.

How do we secure maps and map data?

iRobot considers maps of the home to be your sensitive, confidential information. Maps are protected following the industry standard guidelines to ensure the security of this data just like any other personal data. In addition to the standards mentioned above for encryption at-rest and in-flight, access to this data is tightly controlled, monitored and regularly audited. iRobot machines accessing this data have data-leak prevention software installed to ensure the data is tracked as it is accessed for use in customer support and robot improvement processes.

How secure is using an app not provided by iRobot?

iRobot embraces innovation and lets third-party software interact with our products when that software presents the correct credentials. As a result, independent developers are able to create tools and accessories that may create an enhanced user experience for you. While the security of your data produced by your robot and stored in the iRobot cloud remain safe, iRobot recommends you to verify the third-party documents on how your data is handled.

How long will you continue the support of the security of your product?

We will notify customers at least 6 months before the end of software security support for a particular connected product.

Do you support running your mobile app on non-standard (jailbroken or rooted or otherwise compromised) mobile devices?

The iRobot Home App utilizes security controls provided by the device manufacturer, as such we cannot safeguard the security and privacy of data stored on the iRobot Home App when it

is running on a jailbroken or rooted device that compromises the device's security controls in any way.

Future products and security

The landscape of security threats is ever evolving, as is the security at iRobot. iRobot continuously trains, researches, and exercises processes that improve the maturity of the company's overall ability to identify, react to, isolate and resolve security issues within our company and our products as quickly as possible.

For more details on our principles and approach on privacy or customer data, please take a look at our [Privacy Policy](#).

Any additional questions, please [email us](#).

Privacy Policy

iRobot Corporation is committed to protecting your privacy. [View our Privacy Policy](#).

Vulnerability Disclosure Policy

If you are a security researcher and believe you have found a bug in one of our connected products, we'd like to hear from you! Please visit our [Bug Bounty program](#) for the program's rules and to submit your research for consideration. For any additional security issues or submitting vulnerabilities directly to iRobot, please [email us](#). We'll reply within 3 business days and then keep in touch as we strive to mitigate security issues or vulnerabilities within 90 days