kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Embedded Systems Security

Kompleksowa ochrona przeznaczona dla systemów wbudowanych

Rynek systemów wbudowanych stale rośnie, co zauważają cyberprzestępcy – w 2019 roku odnotowano o 28% więcej prób infekcji w systemach stosowanych w bankomatach i terminalach płatniczych niż w roku 2018.

Systemy wbudowane są wszędzie wokół nas i wpływają na każdą część naszego codziennego życia. Na nich polegamy we wszystkim, od systemów PoS i bankomatów po urządzenia medyczne i telekomunikację. Oznacza to więcej wektorów ataku niż kiedykolwiek wcześniej.

Ponieważ Windows 7 niedawno osiągnął koniec wsparcia technicznego, firmy nie powinny zwlekać z aktualizacją systemu operacyjnego w swoich systemach wbudowanych i muszą podjąć wszelkie niezbędne dodatkowe środki ochrony. Warto zauważyć, że chociaż Windows XP stał się przestarzały wiele lat temu, nadal jest najczęściej używanym systemem operacyjnym w systemach wbudowanych. Jest to otwarte zaproszenie dla hakerów.

Cyberprzestępcy coraz częściej zwracają uwagę na te urządzenia wbudowane jako cel ataków. Może to skutkować znacznymi szkodami finansowymi. Biorąc to pod uwagę, firmy muszą być mądrzejsze niż kiedykolwiek, aby chronić swoje systemy i dane. Dzięki zaawansowanej analizie zagrożeń, wykrywaniu złośliwego oprogramowania w czasie rzeczywistym, wszechstronnej kontroli aplikacji i urządzeń oraz elastycznemu zarządzaniu, Kaspersky Embedded Systems Security jest kompleksowym zabezpieczeniem zaprojektowanym specjalnie dla systemów wbudowanych.

Najważniejsze informacje

Wydajna konstrukcja nawet dla sprzętu z niższej półki

Kaspersky Embedded Systems Security został stworzony z myślą o skutecznym działaniu nawet na słabszym sprzęcie (z 256 MB pamięci RAM i procesorem Pentium III) oraz na starym oprogramowaniu (z systemu Windows XP), bez ryzyka przeciążenia systemu. Słabe kanały komunikacyjne (już od 56 kb/s) również nie stanowią problemu, nawet gdy modem mobilny jest jedyną opcją komunikacji i działa na 2G z powodu słabego sygnału.

Niezawodna ochrona pamięci

Zaawansowana technologia zapobiegania exploitom czuwa nad krytycznymi procesami, aby uniemożliwić exploitom atakowanie przez niezałatane luki, a nawet luki typu zero-day w aplikacjach i komponentach systemu. Jest to szczególnie ważne dla ochrony przed powszechnymi atakami ransomware, takimi jak WannaCry i ExPetr.

Optymalizacja pod kątem Windows XP

Większość systemów wbudowanych nadal działa na niewspieranym systemie Windows® XP. Kaspersky Embedded Systems Security został zoptymalizowany do działania z pełną funkcjonalnością na platformie Windows XP, a także Windows 7, Windows 8 oraz Windows 10.

Kaspersky Embedded Systems Security dokłada wszelkich starań, aby w najbliższej przyszłości zapewnić 100% wsparcie dla systemu Windows XP, dając firmom czas na stopniową aktualizację.

Zgodność

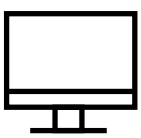
Unikalny, kompleksowy zestaw składników ochrony w Kaspersky Embedded Systems Security — ochrona przed złośliwym oprogramowaniem, kontrola aplikacji i urządzeń, zarządzanie zaporą, monitorowanie integralności plików i audyt dzienników — identyfikuje i blokuje złośliwe działania przeciwko Twoim systemom oraz wykrywa różne wskaźniki naruszenia bezpieczeństwa. Pomaga to firmom spełnić wymagania dotyczące zgodności z przepisami, takimi jak PCI/DSS, WIFT itp.

Bankomaty

Terminale płatnicze

Automaty biletowe

Systemy kasowe



Stare komputery

Sprzęt medyczny

Ochrona przed złośliwym oprogramowaniem
- Opcjonalnie
- W czasie rzeczywistym/na żądanie
- Zapobieganie wykorzystaniu luk w zabezpieczeniach przez oprogramowanie ransomware i inne zagrożenia

Ochrona sieci
- Zarządzanie zaporą sieciową
- Ochrona przed zagrożeniami sieciowymi

Zoptymalizowane wymagania systemowe
- 256 MB pamięci RAM lub więcej
- System operacyjny: Windows XP i nowsze
- Przepustowość sieci: od 56 kb/s

Kaspersky Embedded System Security

Monitorowanie integralności systemu
- Monitorowanie integralności plików
- Kontrola dzienników zdarzeń

Wzmacnianie systemu
- Kontrola uruchamiania aplikacji
- Kontrola dystrybucji oprogramowania
- Kontrola urządzeń

Funkcje

Potężna ochrona przed szkodliwym oprogramowaniem

Proaktywne, wspomagane chmurą wykrywanie i analiza zagrożeń współpracuje z tradycyjnymi technologiami w celu zapewnienia ochrony przed znanymi, nieznanymi i zaawansowanymi zagrożeniami. Opcjonalny (ale zdecydowanie zalecany) składnik chroniący przed złośliwym oprogramowaniem można wyłączyć w scenariuszach ze słabszym sprzętem lub wolnymi kanałami komunikacji.

Wykrywanie szkodliwego oprogramowania w czasie rzeczywistym za pomocą Kaspersky Security Network

Kaspersky Security Network (KSN) to wspierana przez chmurę, globalna sieć analizy zagrożeń firmy Kaspersky. Miliony rozproszonych na całym świecie węzłów stale dostarczają do naszych systemów informacje o zagrożeniach w świecie rzeczywistym, zapewniając szybką reakcję nawet na najnowsze, pojawiające się i ewoluujące zagrożenia, w tym ataki masowe. Ten ciągły przepływ nowych danych o próbach ataków złośliwego oprogramowania i podejrzanych zachowaniach tworzy natychmiastowe werdykty dotyczące plików, zapewniając ochronę w czasie rzeczywistym przed najnowszymi zagrożeniami.

Kontrola aplikacji

Przyjęcie scenariusza domyślnej odmowy za pomocą funkcji Kontrola uruchamiania aplikacji optymalizuje odporność systemu na naruszenia danych. Blokując uruchamianie jakichkolwiek aplikacji innych niż określone programy, usługi i zaufane składniki systemu, możesz automatycznie całkowicie zablokować większość form złośliwego oprogramowania.
Kontrola dystrybucji oprogramowania wykorzystuje podejście „zaufanego instalatora", eliminując potrzebę czasochłonnego, ręcznego umieszczania na białej liście plików utworzonych lub zmienionych podczas aktualizacji, bądź instalacji oprogramowania. Wystarczy po prostu określić instalator jako zaufany i przeprowadzić aktualizację w standardowy sposób.

Monitorowanie i kontrola urządzeń

Kontrola urządzeń firmy Kaspersky pozwala kontrolować urządzenia pamięci masowej USB podłączone lub próbujące połączyć się fizycznie ze sprzętem systemowym. Zapobieganie dostępowi nieautoryzowanych urządzeń oznacza blokowanie wspólnego punktu wejścia wykorzystywanego przez cyberprzestępców jako pierwszy krok w ataku złośliwego oprogramowania.
Wszystkie połączenia urządzeń USB są monitorowane i rejestrowane, dzięki czemu niewłaściwe użycie USB może zostać zidentyfikowane jako potencjalne źródło ataku podczas badania incydentu i procesu reagowania.

Zarządzanie zaporą systemu Windows

Zaporę systemu Windows można skonfigurować bezpośrednio z Kaspersky Security Center, co zapewnia wygodę lokalnego zarządzania zaporą sieciową za pomocą jednej ujednoliconej konsoli. Jest to niezbędne, gdy systemy wbudowane nie należą do domeny, a ustawień zapory systemu Windows nie można skonfigurować centralnie.

Ochrona przed zagrożeniami sieciowymi

Ochrona przed zagrożeniami sieciowymi pomaga zapobiegać zagrożeniom sieciowym, w tym skanowaniu portów, atakom DoS oraz przepełnieniem bufora. Stale monitoruje aktywność sieciową i w przypadku wykrycia podejrzanego zachowania uruchamia predefiniowaną odpowiedź.

Monitorowanie integralności plików*

Śledzi działania wykonywane na określonych plikach i folderach w określonym zakresie. Możliwe jest również skonfigurowanie zmian, które mają być śledzone w czasie, gdy monitorowanie jest przerwane.

Kontrola dzienników zdarzeń*

Kaspersky Embedded Systems Security monitoruje możliwe naruszenia ochrony na podstawie sprawdzania dzienników zdarzeń systemu Windows. Aplikacja powiadamia administratora o wykryciu nietypowego zachowania, które może wskazywać na próbę cyberataku.

Integracja z SIEM

Kaspersky Embedded Systems Security może konwertować zdarzenia w dziennikach aplikacji na formaty obsługiwane przez serwery Syslog, dzięki czemu mogą one być przesyłane i pomyślnie rozpoznawane przez wszystkie systemy SIEM. Zdarzenia można eksportować bezpośrednio z Kaspersky Embedded System Security do SIEM lub centralnie za pośrednictwem Kaspersky Security Center.

Elastyczne zarządzanie

Zasadami bezpieczeństwa, aktualizacjami sygnatur, skanowaniem w poszukiwaniu złośliwego oprogramowania i gromadzeniem wyników można łatwo zarządzać za pomocą jednej scentralizowanej konsoli zarządzającej – Kaspersky Security Center.
Ponadto, klientami w sieci lokalnej można zarządzać za pomocą lokalnej konsoli GUI lub wiersza poleceń – szczególnie przydatne podczas pracy w odizolowanych, segmentowanych sieciach, które są typowe dla systemów wbudowanych.

* Wymaga licencji Kaspersky Embedded Systems Security Compliance Edition

Informacje o cyberzagrożeniach: www.securelist.pl
Informacje ze świata bezpieczeństwa IT: kaspersky.pl/blog
Ochrona IT dla MŚP: kaspersky.pl/biznes
Ochrona IT dla korporacji: kaspersky.pl/korporacje

www.kaspersky.pl

2020 AO Kaspersky Lab. Wszelkie prawa zastrzeżone. Zarejestrowane znaki handlowe i nazwy usług należą do ich właścicieli.

Jesteśmy skuteczni. Jesteśmy niezależni. Jesteśmy transparentni. Zobowiązaliśmy się do budowania bezpieczniejszego świata, w którym technologia czyni nasze życie lepszym. Dlatego go chronimy, aby każda osoba wszędzie mogła korzystać z jego nieskończonych możliwości. Aktywuj cyberbezpieczeństwo dla lepszego jutra.

Dowiedz się więcej na stronie www.kaspersky.pl/transparentnosc

Sprawdzony. Transparentny. Niezależny.