TSplus Advanced Security

Najlepsza broń przeciwko cyberprzestępcom

Cyberprzestępcy wiedzą, że korzystasz z systemów pulpitu zdalnego

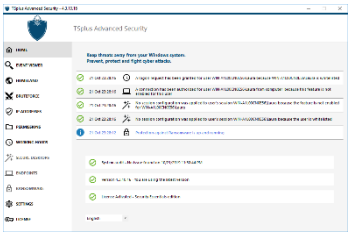
Jest rzeczą oczywistą, że cyberbezpieczeństwo - ochrona danych biznesowych, dostawców i klientów przed działaniem szkodliwych intruzów cybernetycznych - powinno być teraz priorytetem dla każdej organizacji. Starając się zapewnić jak najwyższy poziom usług i dostarczanych produktów, powinniśmy zadbać również o jak najwyższy poziom w zakresie bezpieczeństwa cybernetycznego. Nie można lekceważyć ryzyka i wynikających z niego konsekwencji, problem zagrożenia sam nie zniknie.

Jeśli chodzi o zagrożenie cyberprzestępczością, to pytanie nie brzmi już „jeśli", a zdecydowanie „kiedy". Na podstawie niedawnej ankiety, izba handlowa poinformowała, że w ciągu ostatnich dwóch lat około 55% firm w jednym zaledwie powiecie padło ofiarą ataku. **Ze względu na ryzyko biznesowe i związane z tym konsekwencje, pulpity zdalne muszą być skutecznie zabezpieczone.**

Większość organizacji zakłada, że hakerzy, którzy im zagrażają, będą motywowani wartością informacji, które firma wykorzystuje do świadczenia swoich usług. Prawda jest taka, że cyberprzestępcy niekoniecznie dbają o wartość danych korporacyjnych, osobistych lub finansowych. Wiele ataków jest przeprowadzanych na systemy, ponieważ moc obliczeniowa samych systemów jest wartością samą w sobie.

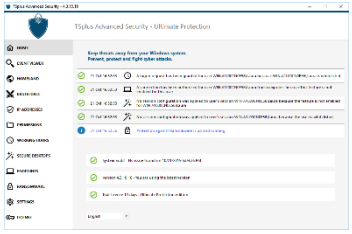
W miarę wzrostu i ewolucji infrastruktur systemu Windows, ekspertom ds. bezpieczeństwa coraz trudniej jest dostrzec wszystkie punkty końcowe w swojej architekturze. Aby dążyć do zmniejszenia ryzyka, należy również znać swoje słabe punkty bezpieczeństwa związane z Pulpitem zdalnym. **TSplus Advanced Security** składa się z solidnego i zintegrowanego zestawu funkcji zabezpieczeń, które w sposób niezwodny chronią zdalny pulpit.

To oprogramowanie łączy zaawansowaną technologię oraz efekty najnowszych wniosków i spostrzeżeń, które nasz znakomity zespół specjalistów ds. bezpieczeństwa cybernetycznego zaimplementował do rzeczywistych rozwiązań w zakresie pulpitu zdalnego. **TSplus Advanced Security jest dostępny w dwóch wersjach**:



TSplus Advanced Security *Ultimate Protection* to **narzędzie bezpieczeństwa, które jest niezbędnym wyposażeniem każdego administratora Serwerów Windows:** zapewnia wszystko, czego potrzebujesz, aby skutecznie chronić środowisko użytkowników i przeciwdziałać złośliwym działaniom.

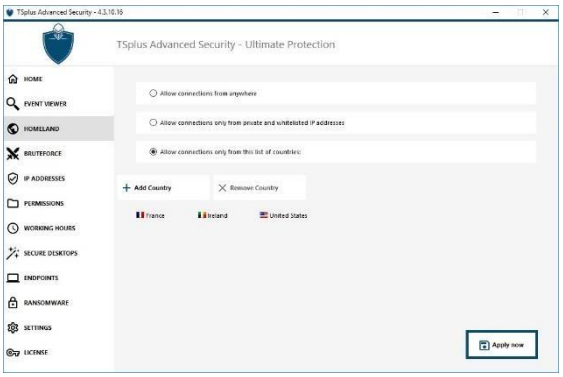
TSplus Advanced *Security Essentials* to **najlepszy pakiet zaawansowanych funkcji ochrony, zapewniający bezpieczeństwo połączeń pulpitu zdalnego**. Jest to niedrogie rozwiązanie bezpieczeństwa, które można zastosować do wszystkich RDP od W7 do W10 Pro



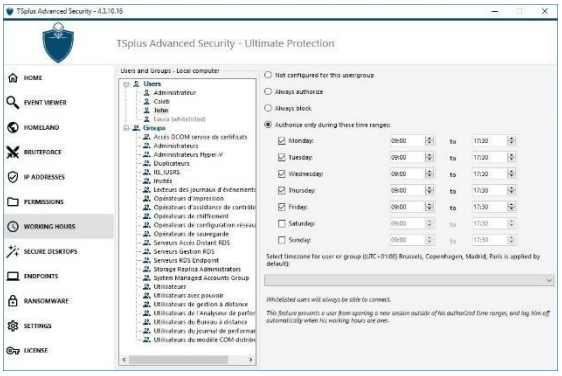
TSplus Advanced Security zapewnia 6 ważnych zabezpieczeń

➢ Zapobiegaj otwarciu sesji przez obcokrajowców.

Twoi użytkownicy znajdują się w Niemczech, Francji, we Włoszech i Stanach Zjednoczonych. Dlaczego zezwalać na łączenie się użytkowników z innych krajów?
Dzięki **TSplus Advanced Security** możesz w mgnieniu oka chronić swoje serwery TSplus przed hakerami próbującymi otworzyć sesję z zagranicy. To jest niezwykle proste, a zarazem potężne. Po prostu to zrób!



Funkcja jest dostępna w TSplus Advanced Security Essentials.



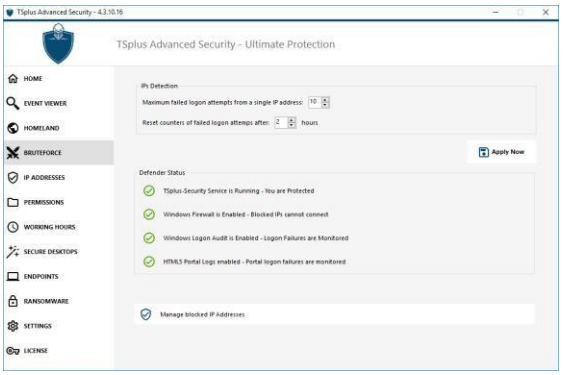
Funkcja jest dostępna w TSplus Advanced Security Essentials

➢ Uniemożliw użytkownikom łączenie się w nocy.

Użytkownicy pracują w ciągu dnia i nie mogą łączyć się poza godzinami pracy. To takie proste! Każdy użytkownik łączący się w nocy zostanie automatycznie wylogowany z systemu.

➢ Unikaj ataków brute-force.

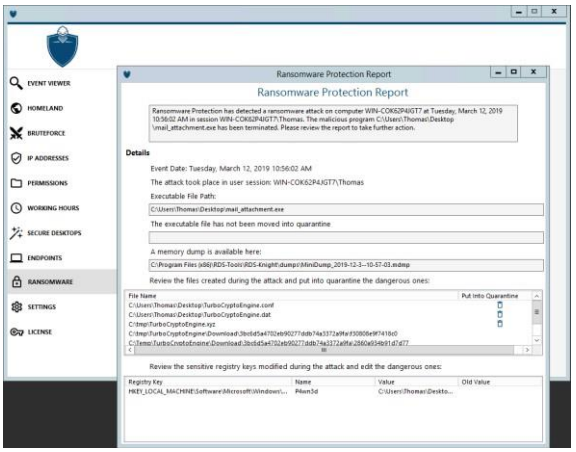
Zatrzymaj ciągłe ataki dzięki ochronie przed atakami brute-force **TSplus Advanced Security**. Funkcja ta natychmiast ochroni Twój serwer, monitorując nieudane próby zalogowania się w systemie Windows i po kilku błędach automatycznie umieszcza podejrzane adresy IP na czarnej liście. Co więcej, możesz go skonfigurować zgodnie z własnymi potrzebami.



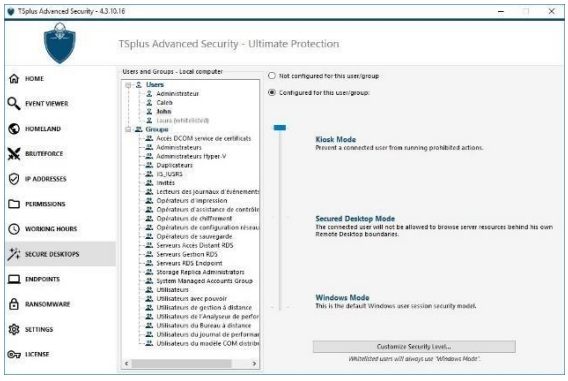
Funkcja jest dostępna w TSplus Advanced Security Essentials.

➢ Wykrywaj i zatrzymuj Ransomware.

Ransomware to najbardziej istotne ze współczesnych zagrożeń cybernetycznych. Wrogie działania w twoich systemach albo całkowicie zablokują twój dostęp, albo zaszyfrują większość twoich plików, dopóki nie zapłacisz okupu żądanego przez cyberprzestępców. **Ochrona TSplus Advanced Security Anti-Ransomware** skutecznie wykrywa, blokuje i zapobiega atakom ransomware. Zapobiegnie katastrofalnym skutkom dla Twojej firmy, usuwając oprogramowanie ransomware na wczesnym etapie.



Dowiedz się, jak przewidywać te zagrożenia, korzystając z raportów pokazujących źródło ataku



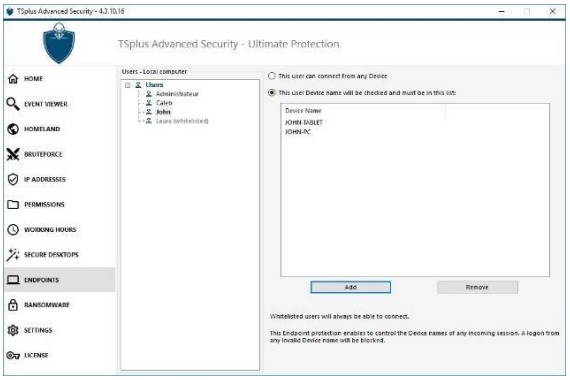
Użytkownicy natychmiast skorzystają z chronionego środowiska

➢ Chroń profile użytkowników.

Systemy Windows zapewniają zbyt wiele funkcji i tylko niewielu ekspertów może odpowiednio zarządzać tego rodzaju złożonością. Wielu z nas nie ma wystarczających umiejętności, aby konfigurować reguły bezpieczeństwa i ukrywać funkcje systemu Windows przed zdalnymi pulpitami użytkowników. **TSplus Advanced Security wymusi dla ciebie poziom bezpieczeństwa, którym chcesz** zabezpieczyć serwer RDS. A najlepsze jest to, że możesz to zrobić **„użytkownik na użytkownika" lub na grupę**.

➢ Zablokuj połączenia z nieautoryzowanych urządzeń.

Wraz z rozwojem trendu BYOD i pracy zdalnej, gdzie technologia umożliwia użytkownikom łączenie się i pracę z dowolnego miejsca za pomocą własnego urządzenia, rosną zagrożenia. Musisz mieć pewność, że każde urządzenie może być kontrolowane i jest bezpieczne. Dzięki **TSplus Advanced Security** możesz zezwolić użytkownikowi na dostęp z dowolnego urządzenia lub po prostu **z określonego urządzenia**, wprowadzając jego nazwę, która będzie sprawdzana przez ochronę punktu końcowego.



Logowanie z nieznanego urządzenia zostanie zablokowane.

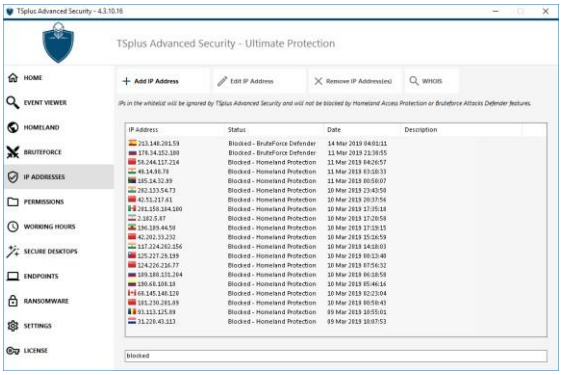
Łatwe zarządzanie

Sprawdź działania ochronne TSplus Advanced Security w czasie rzeczywistym.

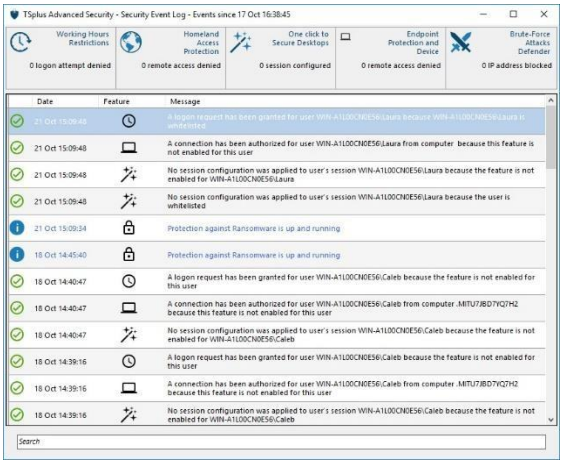
Dzięki **Dziennikowi Zdarzeń Bezpieczeństwa** możesz wyświetlić wszystkie szczegółowe informacje dotyczące ostatnich 2500 zdarzeń i śledzić wszelkie żądania logowania i konfigurację w czasie rzeczywistym:

- Zablokowane, nieudane lub przyznane połączenia.
- Zatrzymane ataki i pliki poddane kwarantannie.
- Skonfigurowane sesje użytkownika.

Jest to bardziej odpowiednia alternatywa niż pełne rozwiązanie kontrolne. Ponadto dostępne jest również pogłębione globalne wyszukiwanie w celu szybkiego znalezienia określonych zdarzeń.



Dodaj/Edytuj lub Usuń adres IP z białej listy



Zobacz i przeszukaj 2500 ostatnich zdarzeń w dzienniku zdarzeń bezpieczeństwa.

Ujednolicone i wydajne zarządzanie adresami IP.

Zarządzanie adresami IP jest łatwiejsze dzięki jednej liście umożliwiającej zarządzanie zarówno zablokowanymi, jak i zapisanymi na białej liście adresami IP. Wygodny pasek wyszukiwania zapewnia możliwości wyszukiwania na podstawie wszystkich dostarczonych informacji. Ponadto administratorzy mogą wykonywać działania na kilku wybranych adresach IP za pomocą jednego kliknięcia - takie jak odblokowanie i dodanie do białej listy wielu zablokowanych adresów IP. Możliwe jest również dostarczenie istotnych opisów do dowolnych adresów IP.

Utrzymuj zagrożenia z dala od Twojego systemu Windows.
TSplus Advanced Security ochroni Cię przed atakami na Pulpit Zdalny.

Wymagania

TSplus Advanced Security jest zgodny z następującymi wersjami 32 i 64-bit.
Systemy operacyjne:

- Windows 7 do Windows 10
- Windows Server 2008 R2 do Windows Server 2019

Pobierz 15-dniową wersję próbną