



Zarządzaj i chroń Twoje urządzenia, aplikacje i użytkowników

Warsztat „Endpoint Management”

Podczas warsztatu pokażemy, jak



Poprawić wynik Microsoft Secure Score przy wykorzystaniu Microsoft Endpoint Manager



Tworzyć zasady zarządzania chroniące użytkowników, dane firmowe i urządzenia



Uzyskać wgląd w urządzenia końcowe użytkowników i ich zgodność z politykami firmy



W najlepszy sposób zapewnić dostęp do aplikacji wykorzystywanych na urządzeniach końcowych

„Nowoczesne zarządzanie urządzeniami obejmuje szeroki zakres obszarów, w tym ochronę użytkowników, dodawanie/usuwanie urządzeń, zarządzanie aplikacjami, obsługę użytkowników końcowych i wdrażanie nowych funkcji. „

Forrester 2020 Badanie całkowitego wpływu ekonomicznego platformy Microsoft 365 Enterprise firmy

W jaki sposób zarządzać urządzeniami mobilnymi, laptopami i innymi punktami końcowymi użytkowników? W jaki sposób upewnić się, czy urządzenia użytkownika są zgodne z politykami IT?

Zapewnienie produktywności na dowolnym urządzeniu bez uszczerbku dla bezpieczeństwa IT

Obecnie użytkownicy poszukują nowych sposobów na utrzymanie produktywności podczas pracy na dowolnym urządzeniu. 95% organizacji zezwala na wykorzystanie urządzeń osobistych w pracy. Wszystkie te urządzenia powodują dodatkowe ryzyko, jeśli weźmiemy pod uwagę, że 70 milionów smartfonów ginie każdego roku.

Podczas warsztatu pokażemy jak zarządzać zarówno urządzeniami należącymi do firmy, jak i prywatnymi w chmurze, aby zaspokoić oczekiwania użytkowników co do nowych sposobów wykonywania pracy.



Dlaczego warto wziąć udział?

- Aby sprawdzić możliwości nowoczesnego zarządzania urządzeniami we własnym środowisku.
- Aby zobaczyć jak wykorzystać inteligentne zabezpieczenia, kontrolki oparte na ryzyku, w jaki sposób zapewnić automatyczną autoryzację nowych urządzeń, zaawansowaną analitykę i integrację z wykorzystywanymi produktami firmy Microsoft. W szczególności:

Dowiedz się, jak poprawić możliwości zarządzania za pomocą Microsoft Endpoint Manager.

Odkrywaj i chroń urządzenia końcowe, wymuszając zasady i wdrażając narzędzia zabezpieczeń.

Zabezpiecz tożsamość użytkowników za pomocą uwierzytelniania wieloskładnikowego i dostępu warunkowego z dowolnego urządzenia.

Zapewnij użytkownikom produktywność udostępniając aplikacje i urządzenia

Czego należy się spodziewać?

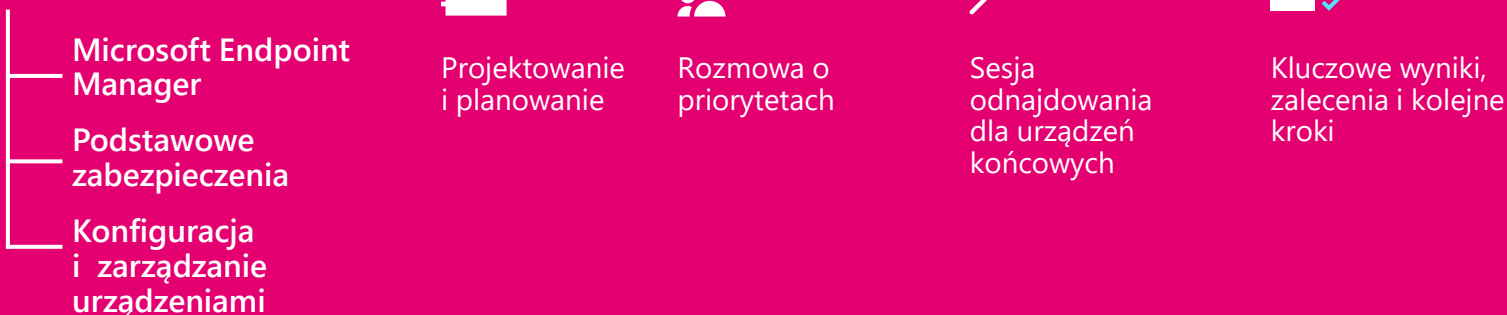
Szczegółowych informacji związanych ze zdalnym wdrażaniem, zarządzaniem i bezpieczeństwem urządzeń firmowych i osobistych w organizacji. Naszym celem jest pokazanie najlepszych sposobów zarządzania urządzeniami końcowymi na poziomie przedsiębiorstwa zapewniając możliwość ochrony tożsamości autoryzowanych użytkowników. Dzięki temu uwierzytelniając poświadczenia i zarządzając dostępem, użytkownicy otrzymają swobodę współpracy z innymi.

Podczas warsztatu pokażemy jak:

- Ulepszyć możliwości zarządzania za pomocą Microsoft Endpoint Manager
- Wyszukiwać i chronić urządzenia końcowe, egzekwując zasady i wdrażając narzędzia zabezpieczeń
- Zabezpieczać tożsamość za pomocą uwierzytelniania wieloskładnikowego i dostępu warunkowego z dowolnego urządzenia
- Zapewnić użytkownikom produktywność dzięki aplikacjom i urządzeniom, których potrzebują.

Dostosujemy warsztat do potrzeb organizacji

Przebieg warsztatu



Kto powinien wziąć udział?

Warsztaty przeznaczone są dla decydentów ds. bezpieczeństwa, takich jak::

- Dyrektor ds. Bezpieczeństwa Informatyki (CISO)
- Dyrektor ds. Informatyki (CIO)
- Dyrektor ds. Bezpieczeństwa (CSO)
- Właściciele/decydenci ds. zarządzania urządzeniami
- Właściciele aplikacji
- Bezpieczeństwo IT
- Operacje IT
- Architekt bezpieczeństwa
- Inżynierowie bezpieczeństwa

Dlaczego T-Systems Polska?

Jeśli chodzi o ujednolicone zarządzanie urządzeniami końcowymi, potrzebujesz doświadczonego partnera.

T-Systems Polska zrealizował wiele projektów związanych z zabezpieczeniami tożsamości, aplikacji i środowiska IT zwiększając bezpieczeństwo organizacji zarówno tych niewielkich po firmy z sektora Enterprise.

Skontaktuj się z nami, aby rozpocząć!