MORPHISEC
Moving Target Defense

FIRMA PRODUKCYJNA HIGH-TECH
STUDIUM PRZYPADKU

Wyprzedzić cyber napastników za pomocą Moving Target Defense

BRANŻA
Produkcja z wysoko-zaawansowaną technologią

ŚRODOWISKO
- Wysoko zautomatyzowane środowisko z mieszanym oprogramowaniem pakietowym i zamkniętym

WYZWANIA
- Złożony i połączony łańcuch dostaw
- Utrzymanie reputacji liderów w technologii produkcyjnej z rygorystycznym cyberbezpieczeństwem
- Zamiana tradycyjnego antywirusa na chroniący przed zagrożeniem Next Gen oparty na AI, jednak nie zwalczył on skutecznie ataków bezplikowych i na pamięć
- Szczupłe i wydajne podejście do bezpieczeństwa
- Zerowa tolerancja na naruszenia

ROZWIĄZANIE
- Wzmocnienie punktu końcowego poprzez Morphisec w celu zaawansowanej ochrony przed zagrożeniem
- Ochrona przedsiębiorstwa zarówno przed zagrożeniami dla towarów i zawansowanymi, ukierunkowanymi atakami bez stwarzania kosztów lub ingerowania w automatyzację IT

PROFIL KLIENTA

Średniej wielkości producent materiałów budowlanych stosujący technologię na wysokim poziomie znany ze swojego innowacyjnego wykorzystania technologii, doskonałej jakości i wiodący w łańcuchu dostaw.

WYZWANIE

Firma wykorzystuje wysoce zaawansowaną technologię – większa jej część jest wypracowywana wewnętrznie – w celu zaprojektowania i zarządzania złożonymi łańcuchami dostaw różnych produktów.
Wszystko jest zautomatyzowane i zintegrowane, od zakupów zagranicznych, przez magazynowanie, własną, lokalną produkcję do dostawy. Ta technologia informacyjna (IT) i automatyzacja tworzą główne kompetencje firmy i czynniki wyróżniające firmę. Naruszenie bezpieczeństwa w przedsiębiorstwie spowodowałoby nie tylko szkodę finansową, ale miałoby również wpływ na cały model biznesowy i pozycję rynkową.
Złożony i połączony łańcuch dostaw firmy znacznie bardziej naraża ją na niebezpieczeństwo. W celu ochrony jej własności intelektualnej i zapewnienia, że operacje nie zostaną pokrzyżowane przez cyberatak, firma jest mocno i profilaktycznie zaangażowana w cyberbezpieczeństwo.

Zgodnie z Dyrektorem IT (CIO) firmy, uznawanego za wizjonera w branży, „Strategiczne bezpieczeństwo jest integralną częścią – to nie jest coś dodatkowego". Pod jego przywództwem, zespół IT stosuje do cyberbezpieczeństwa to samo zintegrowane, uproszczone podejście, które używa w produkcji.

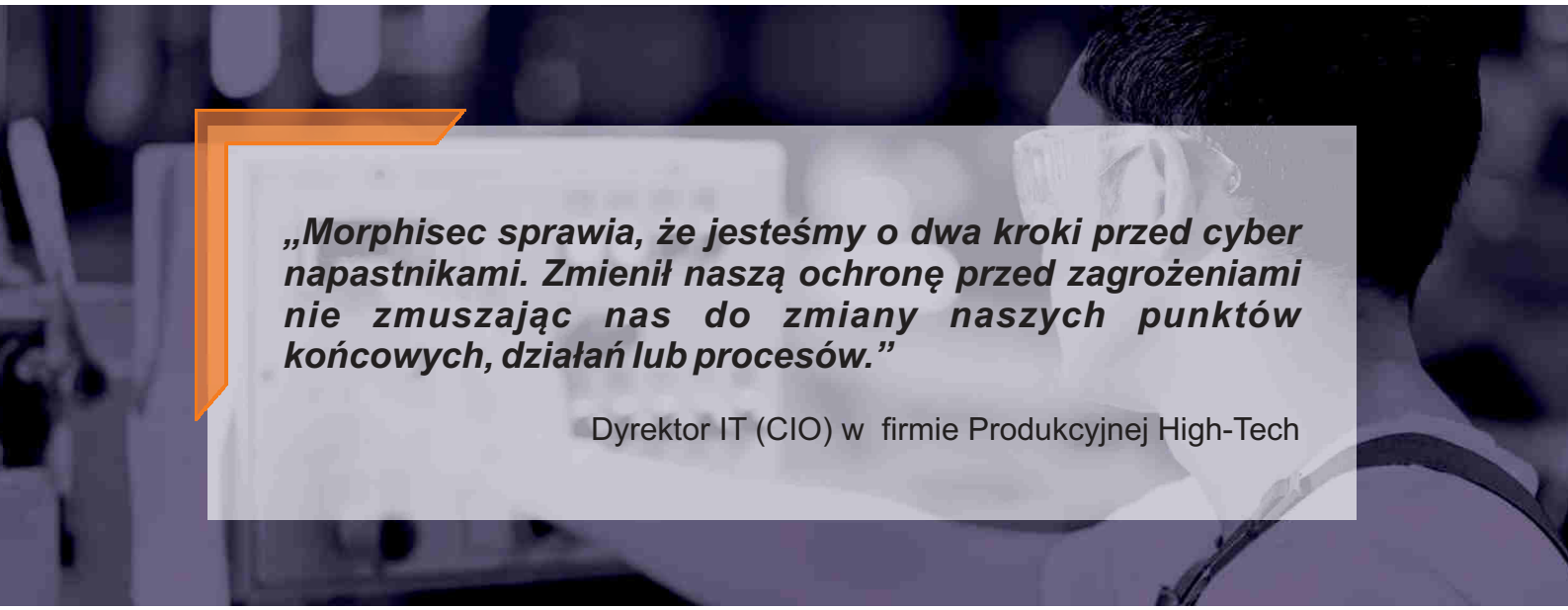
Ostatnio firma wymieniła swój tradycyjny program antywirusowy na program Next Gen oparty na AI chroniący przed zagrożeniem.
Dyrektor IT (CIO) szybko zdał sobie sprawę, że pomimo poprawy, rozwiązanie AI nie zapewniało właściwej ochrony przed zaawansowanymi atakami na pamięć (in-memory). Potrzebowali rozwiązania, które można by stosować właśnie w tych rodzajach zaawansowanych ataków, ale które nie stwarzałoby kosztów lub nie kolidowałoby z ich zaawansowanymi działaniami w produkcji i sieci dostaw.

ROZWIĄZANIE

Po uznaniu, że zaawansowane ataki na pamięć (in-memory) stanowią inną i zagrażającą egzystencji klasę zagrożeń, zdolnych do wstrzymania produkcji i działań biznesowych, Dyrektor IT (CIO) firmy doszedł do wniosku, że potrzebna była inna technologia, taka która nie polegała na wcześniejszej wiedzy o ataku. Określił trzy kluczowe wskaźniki efektywności (KPI) dla rozwiązań w zakresie bezpieczeństwa: zasięg, prędkość i łatwość użycia. Po sprawdzeniu różnych rozwiązań, zawęził zakres do zapobiegania, zamiast produktów typu wykrywanie-reagowanie, wskazując Moving Target Defense jako najbardziej obiecującą koncepcję. Wybrał rozwiązanie Morphisec Endpoint Threat Prevention z powodu optymalnych wyników wobec jego KPI i nowatorską technologię Moving Target Defense. Dyrektor IT (CIO) był w szczególności pod wrażeniem sposobu, w jaki Morphisec zmniejsza powierzchnię możliwego ataku i stosuje podstęp, żeby zmusić ataki do ujawnienia się.
Morphisec został zainstalowany bez wstępnego pilotażu. Wdrożenie nastąpiło bez żadnych zakłóceń w funkcjonowaniu lub konfliktu z innymi produktami czy aplikacjami związanymi z bezpieczeństwem.

WYNIKI

Od instalacji, Morphisec działa bezbłędnie, znacząco zmniejszając obszar możliwego ataku firmy z zerowym obciążeniem. Dla Dyrektora IT (CIO) jest to decydujące, ponieważ czas, jaki jego zespół poświęca na serwis zabezpieczeń i fałszywe ostrzeżenia, oznacza czas spędzony z dala od ich podstawowych działań. Docenia również, że punkty końcowe i działania nie są spowolnione przez ciężkie oprogramowanie lub aktualizowanie zasad bezpieczeństwa.
Przedsiębiorstwo jest teraz chronione zarówno przed zagrożeniami dla towaru i zaawansowanymi atakami, takimi jak: ataki bezplikowe i z poziomu przeglądarki, exploit i złośliwe oprogramowanie, Trojany i skrypty, które stosują techniki unikania wykrycia, backdoor oraz ataki na sieć dostawy osadzone w aplikacjach firm trzecich. Co więcej, odkąd Morphisec skutecznie zapobiega nieznanym zagrożeniom, nie ma opóźnień w działaniach przeciwko najnowszym zagrożeniom ze strony cyber napastników.



„Morphisec sprawia, że jesteśmy o dwa kroki przed cyber napastnikami. Zmienił naszą ochronę przed zagrożeniami nie zmuszając nas do zmiany naszych punktów końcowych, działań lub procesów.”

Dyrektor IT (CIO) w firmie Produkcyjnej High-Tech