**Bezpieczeństwo chmury od Check Pointa**

**Firma Check Point® Software Technologies ogłosiła w Las Vegas CloudGuard, pełną rodzinę produktów bezpieczeństwa w chmurze opartych na technologiach, które zapewniają kompleksową cyberochronę Gen V dla chmury. Korzystając z rozwiązań CloudGuard, przedsiębiorstwa będą chronione przed atakami cybernetycznymi obciążającymi infrastrukturę w chmurze (IaaS) i aplikacje typu software-as-a-service (SaaS).**

Wdrażanie chmur korporacyjnych postępuje coraz szybciej, umożliwiając większą elastyczność biznesową i wydajność dzięki wdrożeniom hybrydoweych infrastruktur chmur, takich jak Amazon Web Services, Microsft Azure, VMWare NSX, jak i migracji do aplikacji opartych na chmurze, takich jak Microsoft Office365, Google G-Suite, Dropbox, Salesforce czy Box. Obserwuje się jednak wzrost wektorów ataków obciążających chmury i aplikacje chmurowe, w tym złośliwego oprogramowania, jak również wzrost liczby przypadków przejmowania kont. Według badań przeprowadzonych przez Check Point, połowa wszystkich przypadków naruszenia aplikacji SaaS w przedsiębiorstwach jest właśnie wynikiem wrogich przejęć kont online.

– *Bezpieczeństwo jest nieustannie wymieniane jako kluczowa przeszkoda w powszechnym wdrażaniu rozwiązań w chmurze przez korporacje* – powiedział **Gil Shwed**, CEO Check Point. – *Nasza nowa rodzina produktów CloudGuard zapewnia spójne i kompleksowe zapobieganie zagrożeniom w aplikacjach SaaS opartych na chmurze.*

CloudGuard SaaS jest pierwszym w branży zestawem technologii zaprojektowanych w celu zapewnienia zaawansowanego bezpieczeństwa i zapobiegania zagrożeniom w aplikacjach „typu oprogramowanie jako usługa” (SaaaS). CloudGuard SaaS zapobiega również przejęciu konta, wykorzystując czekającą na opatentowanie technologię ID-Guard.

**Kluczowe elementy bezpieczeństwa obejmują:**

l

Ochronę przed zagrożeniem typu zero-day: Zapobiega APT i nieznanemu malwareowi zeru-day przed zainfekowaniem zawartości w aplikacjach SaaS przy użyciu sandboxingu w czasie rzeczywistym, chroi przed ransomware, posiada technologię anty-botową i oraz oparty na chmórze wywiad zagrożeń w czasie rzeczywistym.

l

Ochronę tożsamości za pomocą technologii ID-Guard (w oczekiwaniu na patent): identyfikuje i blokuje oszustów starających się uzyskać dostęp do kont SaaS oraz blokuje nieautoryzowanych użytkowników i zaatakowane urządzenia.

l

Ochronę danych: automatycznie wymusza szyfrowanie wrażliwych danych oraz blokuje i kwarantannuje nieuprawnione udostępnianie poufnych plików.

**CloudGuard IaaS** – dawniej vSEC, a obecnie jeden z elementów rodziny CloudGuard, CloudGuard IaaS zapewnia zaawansowane bezpieczeństwo Gen V, zapobieganie zagrożeniom ataków na infrastrukturę publicznych i prywatnych platform chmury, w tym: Amazon Web Services, Google Cloud Platform, Microsoft Azure, Cisco ACI, OpenStack, VMware NSX, VMware Cloud na AWS, VMware ESX, Alibaba Cloud, KVM, Hyper-V i więcej.

Ataki cybernetyczne Gen V definiuje się jako zakrojone na szeroką skalę i szybko przemieszczające się ataki w sieciach komórkowych, chmurowych i lokalnych. Są wysoce wyrafinowane i z łatwością omijają konwencjonalne, statyczne systemy obrony oparte na detekcji, które są obecnie używane przez większość organizacji. Dzięki współwłasności aktywów w chmurze pomiędzy dostawcą chmury a użytkownikiem końcowym, wiedza o tym, kto jest odpowiedzialny za bezpieczeństwo, jest często niejasna i może prowadzić do dodatkowych nieporozumień. CloudGuard to jedyna w branży kompletna rodzina rozwiązań bezpieczeństwa chmury skupiona na zaawansowanym zapobieganiu zagrożeniom i utrzymywaniu aplikacji chmury korporacyjnej, ochrony informacji i danych przed atakami cyber-atakami Gen.