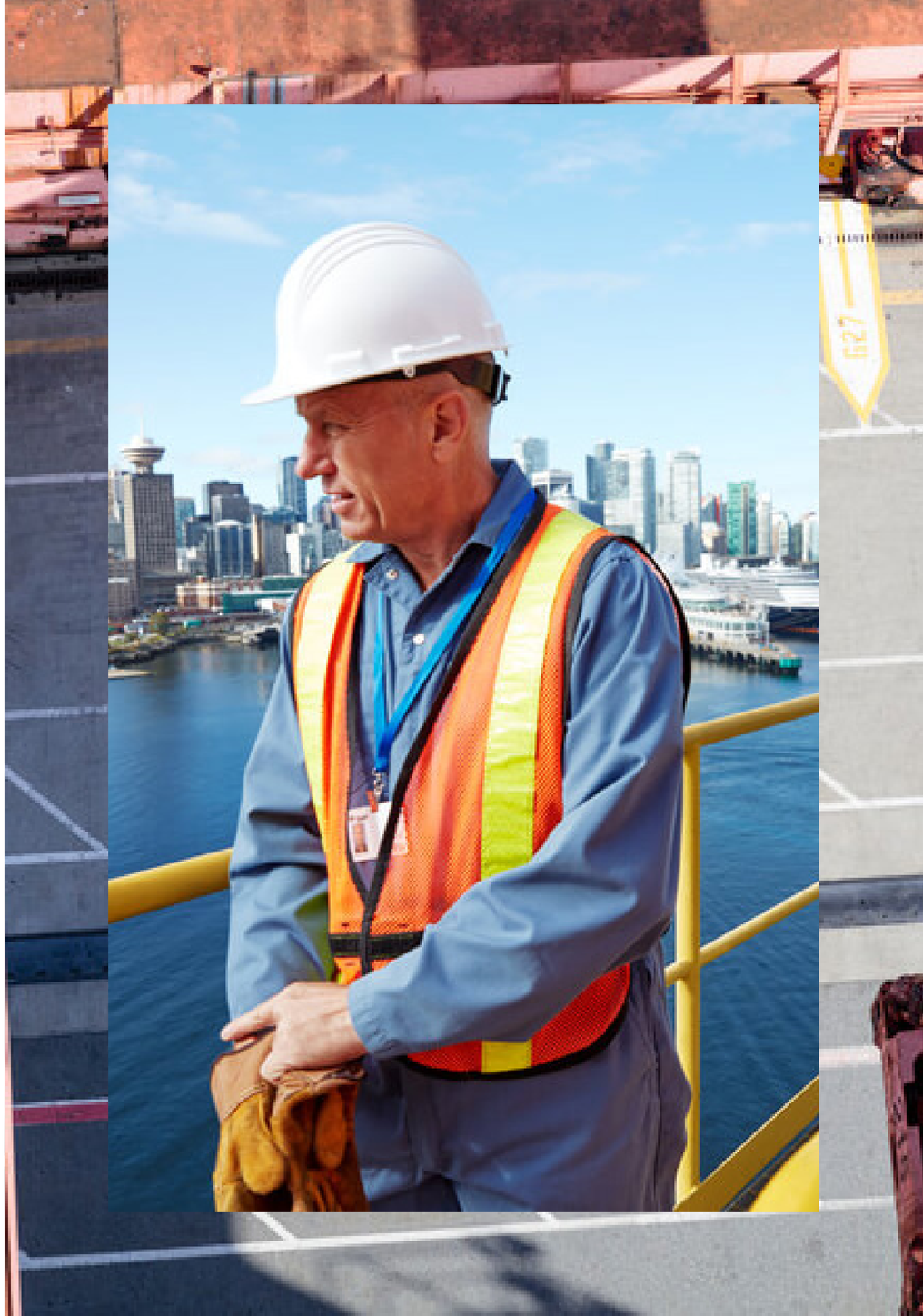
HPE GreenLake

Bezpieczeństwo 360° – wszędzie, gdzie potrzebujesz i zawsze, gdy potrzebujesz

Pierwsze kroki >



Bezpieczeństwo ze wszystkich stron

Zabezpieczenia typu silicon-to-cloud firmy HPE przyspieszają osiągnięcie wyników w rozproszonym świecie

Próbując zabezpieczyć swoje zbiory danych w coraz bardziej złożonych rozproszonych środowiskach IT, współczesne przedsiębiorstwa stoją w obliczu bezprecedensowych wyzwań. W rzeczywistości co 11 sekund[1] jakaś firma pada ofiarą ataku typu ransomware.

Nasza branża znajduje się w krytycznym momencie. Szukamy nowych sposobów na przywrócenie bezpieczeństwa i pomagamy w zabezpieczeniu rozległego i płynnego cyfrowego łańcucha dostaw, od krawędzi do chmury.

Współczesne przedsiębiorstwa zmagają się z coraz bardziej zaawansowanymi i uporczywymi zagrożeniami, takimi jak oprogramowanie ransomware i złośliwe oprogramowanie, które atakują niskie poziomy infrastruktury IT, poza zasięgiem rozwiązań oprogramowania zabezpieczającego punkty końcowe. Cyberprzestępcy zwiększają swoją agresywność, skalę i budżety, tworząc coraz bardziej wyrafinowany rynek dla nowych programów wykorzystujących luki w zabezpieczeniach.

Aby sprostać wyzwaniom związanym z bezpieczeństwem w wysoce rozproszonych środowiskach IT, firma HPE zaczyna od fundamentów – zagrożeń w zaufanym łańcuchu dostaw, krzemie oraz opartej na zasadzie „zero zaufania” ochrony 360 stopni dla infrastruktury zapewniającej organizacjom moc obliczeniową. Architektura bezpieczeństwa HPE typu „zero zaufania” i bezpieczny cykl życia produktów są inicjowane bardzo głęboko, już na początkowych etapach produkcji i kończą się zabezpieczonym wycofaniem z eksploatacji, tworząc bezpieczną ofertę serwerów zgodnych ze standardami branżowymi. Obecnie na całym świecie można znaleźć ponad dwa miliony aktywnych serwerów, w których wprowadzone zostały zabezpieczenia z zastosowaniem mechanizmu „Silicon Root of Trust from HPE” – technologii stosowanej wyłącznie przez HPE.

[1] Cybersecurity Ventures: 5 najważniejszych faktów, liczby, prognozy i statystyki dotyczące cyberbezpieczeństwa w latach 2020-2021

Kliknij na odpowiednią strzałkę w niniejszym e-Przewodniku, aby przejść do określonej sekcji, którą chcesz przeczytać.

1. Nieustannie zmieniający się krajobraz

Zagrożenia rozwijają się wraz z postępem technologicznym

Dziś specjaliści IT nie pytają już czy, ale kiedy organizacja stanie się przedmiotem cyberataku. Cyberprzestępcy będą uderzać wszędzie tam, gdzie znajdą słabe punkty lub możliwości, włamując się do oprogramowania sprzętowego we wszystkich możliwych urządzeniach, począwszy od urządzeń domowych aż po serwery centrów danych. A zagrożenia bezpieczeństwa wydają się rozwijać w tym samym tempie, co technologia, skutkując nieustannym ruchem i ewolucją celu.

Prawie 60% specjalistów IT zgadza się, że „trudno jest chronić złożone i dynamicznie zmieniające się powierzchnie ataków", a „niemożność integracji rozwiązań bezpieczeństwa jest powodem, dla którego naruszenia danych nadal mają miejsce".[2] Jest jasne, że nawet najbardziej świadome bezpieczeństwa organizacje IT mogą mieć trudności z nadążaniem za najnowszymi osiągnięciami w dziedzinie cyberbezpieczeństwa.

Atakujący nieuchronnie znajdują sposoby na wykorzystanie nowych trendów technologicznych, gdy te zyskują popularność na rynku. Od rozwiązań mobilnych | i chmurowych aż po podłączone urządzenia i IoT – im większe obietnice niesie dana technologia dla biznesu, tym bardziej pożądane jest jej wykorzystanie. Nadal działają oni w najbardziej podstawowy sposób – wykorzystując oszustwa związane z wyłudzaniem wiadomości e-mail, kradnąc urządzenia pamięci masowej USB czy niedbale strzeżone hasła.

[2] „Czterokrotny wzrost liczby cyberataków na łańcuch dostaw", cips.org, 2021

1
2
3
4
5
6

Nieustannie zmieniający się krajobraz →

Jednak dominującym trendem w 2021 roku stają się ataki na łańcuch dostaw. W swoim raporcie zatytułowanym „Krajobraz zagrożeń atakami na łańcuch dostaw" Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) ostrzega, że począwszy od 2020 r. spodziewany jest czterokrotny wzrost cyberataków. Te mniej dogodne przestępstwa są trudniejsze do przeprowadzenia, ale przynoszą większe korzyści przeciwnikom.

Niestety ponad połowa specjalistów w dziedzinie IT czuje, że nie jest w stanie nadążyć za natłokiem alertów, a ich zespoły ds. bezpieczeństwa nie mają wglądu we wszystkie urządzenia podłączone do infrastruktury informatycznej. Ponadto, jak donoszą, „trudno jest chronić obszar IT o rozszerzających się i zacierających granicach za pomocą IoT, BYOD, urządzeń mobilnych i chmury".[3]

Jednak skuteczni menadżerowie ds. zagrożeń po prostu nie mogą ryzykować reagowaniem na unikalne narażenia na niebezpieczeństwo występujące w każdym trendzie technologicznym, ponieważ przesunięcie uwagi oznacza otwarcie się ich organizacji na kolejne ataki. Specjaliści IT nie mogą powstrzymać atakujących przed podejmowaniem przez nich najgorszych prób, ale mogą stosować lepsze modele i metody, aby zapobiec naruszeniom.

[3] „Usuwanie luk w zabezpieczeniach IT - badanie globalne z 2020 r.", Ponemon Institute, 2020

2. Podstawy bezpieczeństwa „silicon-to-cloud”

Architektura zerowego zaufania chroni infrastrukturę

Potrzebujesz zabezpieczeń wykraczających poza zaporę ogniową i oprogramowanie, aby chronić serce swojej infrastruktury, zaczynając już od łańcucha dostaw. Od dostawców materiałów po usługi logistyczne i transportowe oraz od produkcji i montażu aż po magazynowanie i dystrybucję – dostawcy HPE są zobowiązani do przestrzegania zasad firmy, a także norm ISO i Suplementu Federalnego Prawa Zamówień Rządowych dotyczących Obronności (Defense Federal Acquisition Regulation Supplement).

Zgodność łańcucha dostaw HPE zapewniają audyty bezpieczeństwa oparte na ryzyku, monitorowanie programów, inspekcje części elektronicznych, identyfikowalność komponentów oraz procesy kontroli materiałów. Przeniesienie tej już bezpiecznej metodologii łańcucha dostaw na kolejny poziom to HPE Trusted Supply Chain, czyli „zaufany łańcuch dostaw HPE” – produkcja prowadzona w bardzo dobrze zabezpieczonych zakładach HPE w USA, które cechuje wzmocniona ochrona danych podczas procesu produkcyjnego, wspierająca klientów z różnych branż, w tym sektora federalnego, publicznego, bankowego i finansowego oraz organizacje opieki zdrowotnej, wymagających produktów o wysokim poziomie bezpieczeństwa pochodzących z USA. Uwzględnia to również zapotrzebowanie klientów na dodatkową bazę dostaw w celu zwiększenia odporności oraz identyfikacji i ograniczenia ryzyka w samym środku pandemii COVID-19, która wpłynęła na łańcuchy dostaw na całym świecie.

„Weź pod uwagę, że serwer rackowy zgodny ze standardami branżowymi składa się z aż

10 000 komponentów.

Dalej rozważ łańcuch kontroli pochodzenia takiego serwera, zanim dotrze on do centrum danych. Szansa na to, że serwer zostanie zaatakowany, jest prawdziwym zagrożeniem, które powinno martwić każdego specjalistę IT”.

„Usuwanie luk w zabezpieczeniach IT - badanie globalne z 2020 r.”, Ponemon Institute, 2020

Podstawy bezpieczeństwa „silicon-to-cloud”

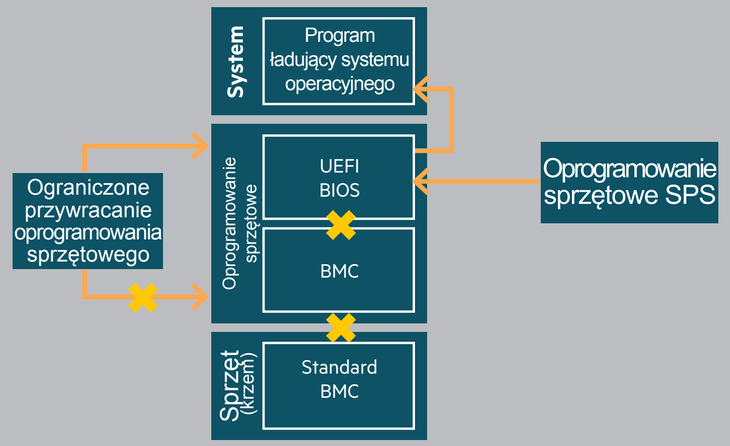
Na samym dole, tj. na poziomie krzemu, współdziałają ze sobą trzy innowacje w zakresie bezpieczeństwa HPE – certyfikaty platformy, mechanizm „Silicon Root of Trust from HPE” (krzemowy korzeń zaufania) firmy HPE oraz tożsamość kryptograficzna produktu (tj. identyfikator Initial Device Identifier, czyli iDevID), zapewniając krzyżujące się ze sobą zabezpieczenia, a w efekcie – spokojną głowę. Przy czym firma HPE stworzyła środki bezpieczeństwa stosowane, gdy nadejdzie czas na wycofanie lub zmianę przeznaczenia infrastruktury.

Certyfikaty platformy oparte są na manifeście sprzętowym serwera ustalanym po zakończeniu produkcji, a przed wysyłką z zakładu, dającym pewność, że integralność systemu w całym cyklu życia łańcucha dostaw nie została naruszona i pozostaje nienaruszona po przybyciu serwera do klienta i przed podłączeniem go do sieci. Dodatkowo można włączyć blokadę konfiguracji serwera Server Configuration Lock , zapewniając, że wszelkie wprowadzone zmiany spowodują brak możliwości uruchomienia serwera bez autoryzacji. Według ekspertów ds. rozwiązań cyberbezpieczeństwa „branże, które wymagają stosowania architektur typu «Zero Trust», skorzystają z nowego procesu weryfikacji platformy (firmy HPE), który gwarantuje, że systemy nie zostały zmienione w żadnym momencie od opuszczenia zakładu produkcyjnego do podłączenia do sieci o znaczeniu krytycznym, takich jak infrastruktura krytyczna sieci rządowych”.[4]

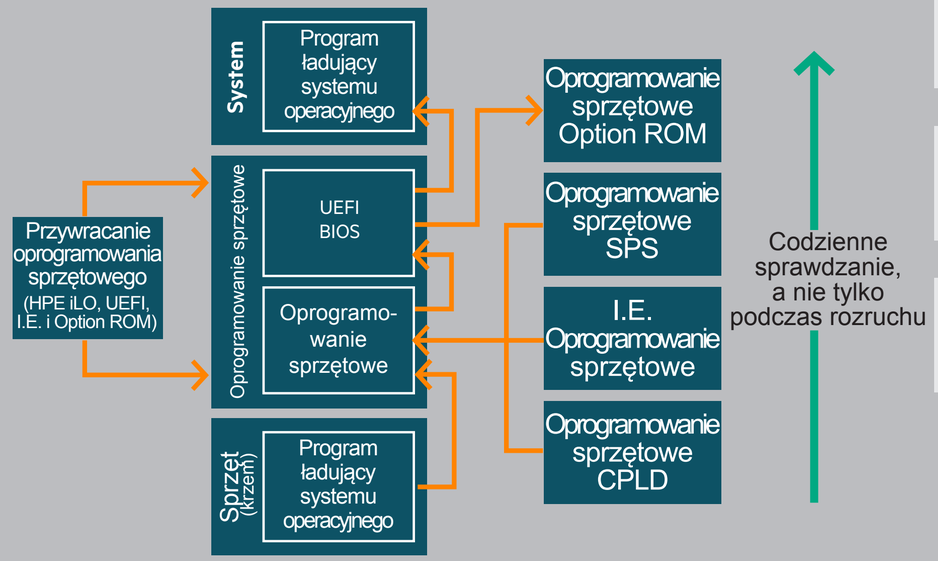
Standardowo stosowane w branży serwery HPE Gen10 Plus zawierają również program Cyber Catalyst by Marsh[SM]– wydzielony krzemowy korzeń zaufania firmy HPE wbudowany bezpośrednio w sam sprzęt. Wiąże on całe niezbędne oprogramowanie sprzętowe – UEFI BIOS, złożony programowalny układ logiczny, silnik innowacji i silnik zarządzania – w krzemie jeszcze przed zbudowaniem serwera. Identyfikator IDevID uwierzytelnia taki stosowany wyłącznie przez firmę HPE „niezmienny odcisk cyfrowy” na chipie HPE iLO , umożliwiając zdalne zarządzanie i monitorowanie w sposób bezdotykowy.

[4] „HPE podnosi bezpieczeństwo łańcucha dostaw”, InfusionPoints, LLC., 2021

Konkurencja



Silicon Root of Trust from HPE



Podstawy bezpieczeństwa „silicon-to-cloud” →

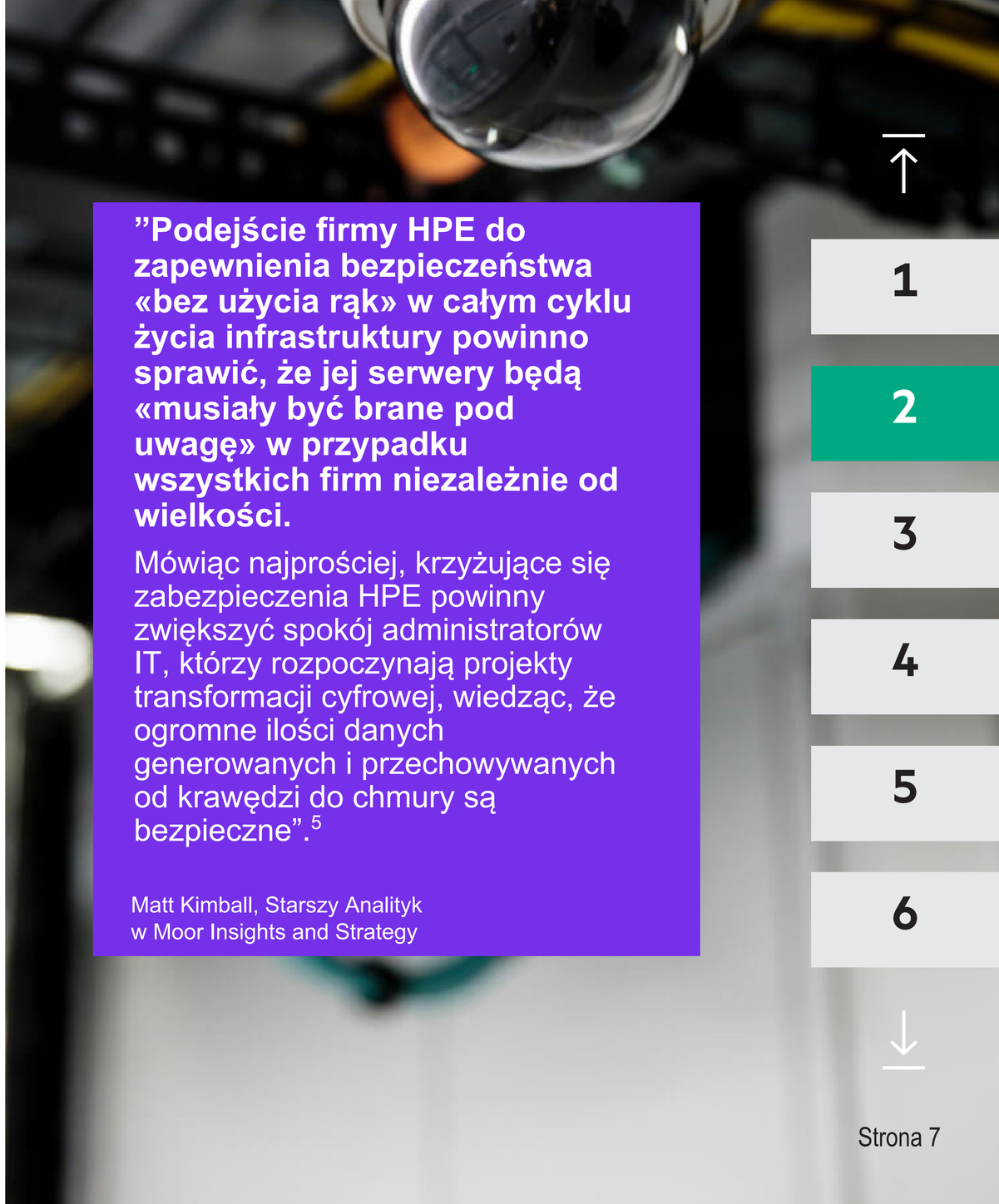
Taki chipset, który jest praktycznie niemożliwy do zmiany, zapewnia bezprecedensowy poziom bezpieczeństwa sprzętowego, który umożliwia uwierzytelnianie oprogramowania sprzętowego począwszy od łańcucha dostaw, zapewniając bezpieczny proces uruchamiania.

W momencie uruchamiania serwera oprogramowanie sprzętowe szuka unikalnego odcisku palca ukrytego w krzemie, aby sprawdzić, czy pasuje on do odcisku palca oprogramowania sprzętowego. Po zweryfikowaniu odcisku palca w krzemie pozostała część niezbędnego oprogramowania sprzętowego – ponad 4 milionów wierszy kodu – uzyskuje zgodę na uruchomienie i wykonanie autoskanowania.

Jeśli w którymkolwiek momencie haker wprowadził wirusa lub zmieniony kod, funkcja weryfikacji oprogramowania sprzętowego w środowisku uruchomieniowym wykryje go, o czym klient zostanie natychmiast powiadomiony. W przypadku wykrycia naruszenia klienci mają trzy możliwości: przywrócenie oprogramowania sprzętowego serwera do ostatniego znanego dobrego stanu, przywrócenie ustawień fabrycznych lub wyłączenie w celu umożliwienia zespołom ds. bezpieczeństwa przeprowadzenia śledztwa.

Gdy nadchodzi czas na wycofanie lub zmianę przeznaczenia serwerów, firma HPE zapewnia kryptograficzne usuwanie danych na poziomie National Institute of Standards and Technology (NIST). Bezpieczne usuwanie za pomocą jednego przycisku umożliwia klientom łatwe usunięcie wszystkich danych użytkownika – dając pewność, że żadne dane nie będą mogły zostać odzyskane w niegodziwych celach – w celu łatwej zmiany przeznaczenia i ponownego wdrożenia serwerów. Ponadto dział HPE Pointnext Services zapewnia usługi odzyskiwania zasobów gwarantujące, że wycofanie infrastruktury jest bezpieczne, również dla środowiska.

[5] „Zero Trust to wysiłek w całym cyklu życia”, Moor Insights & Strategy, 2021



”Podejście firmy HPE do zapewnienia bezpieczeństwa «bez użycia rąk» w całym cyklu życia infrastruktury powinno sprawić, że jej serwery będą «musiały być brane pod uwagę» w przypadku wszystkich firm niezależnie od wielkości.

Mówiąc najprościej, krzyżujące się zabezpieczenia HPE powinny zwiększyć spokój administratorów IT, którzy rozpoczynają projekty transformacji cyfrowej, wiedząc, że ogromne ilości danych generowanych i przechowywanych od krawędzi do chmury są bezpieczne”.[5]

Matt Kimball, Starszy Analityk w Moor Insights and Strategy

Pozostawanie o krok przed zagrożeniami

HPE kontynuuje dostosowywanie się i inwestycje w nowe technologie

Do oceny nowych innowacyjnych technologii bezpieczeństwa w serwerach HPE Gen10 Plus zaproszona została firma InfusionPoints, niezależny ekspert ds. rozwiązań cyberbezpieczeństwa.

„Konieczność zapewnienia odpowiedniego pochodzenia, bezpieczeństwa i wiarygodności sprzętu oraz oprogramowania sprzętowego i użytkowego generującego dzisiejsze obciążenia ma fundamentalne znaczenie dla ochrony przed współczesnymi zagrożeniami. HPE kontynuuje wprowadzanie innowacji i odgrywa wiodącą rolę w procesie wbudowywania do swojego ekosystemu funkcji bezpieczeństwa, które zapewniają ten poziom bezpieczeństwa”.[7]

W drugim swoim raporcie eksperci zewnętrzni przedstawili kolejny kontekst, stwierdzając, że „z chwilą wypuszczenia na rynek w 2017 r. mechanizmu «Silicon Root of Trust from HPE» stosowanego wyłącznie przez firmę HPE wraz z serwerami HPE Gen10, które dokładnie przetestowaliśmy w tamtym czasie, firma HPE rozpoczęła tworzenie podstaw możliwości zastosowania technologii Zero Trust”. Ustalili oni, że mechanizm „Silicon Root of Trust from HPE” zapewnia funkcje walidacji i odzyskiwania dla serwerów z UEFI i HPE iLO, rozszerzając je o walidację oprogramowania sprzętowego komponentów. „Dzięki serwerom HPE ProLiant Gen10 Plus firma HPE kontynuuje wprowadzanie funkcji Zero Trust do swoich produktów kolejnych generacji.”[7]

Eksperci z firmy InfusionPoints przypominają, że uwierzytelnianie urządzeń nie różni się zbytnio od uwierzytelniania użytkowników będących osobami: dane uwierzytelniające są na tyle dobre, na ile dobry jest ich wystawca i na ile dokładnie potwierdzają tożsamość podmiotu przed powiązaniem go z danymi uwierzytelniającymi.[6]

Oprócz modułu TPM (Trusted Platform Module) należy wprowadzić certyfikat platformy serwera HPE oraz identyfikator iDevID. Jako zwolennik Trusted Computing Group (TCG), firma HPE pracuje nad zapewnieniem wdrożenia certyfikatów platform w oparciu o otwarte standardy TCG. Natomiast w Stanach Zjednoczonych systemy te będą produkowane w oparciu o program HPE Trusted Supply Chain, który zapewnia klientom silniejsze walidacje dzięki wzmocnionym funkcjom bezpieczeństwa włączanym bezpośrednio w zakładzie przez sprawdzonych pracowników HPE w bardzo bezpiecznych obiektach zlokalizowanych na terenie USA.[8]

Raport kończy się stwierdzeniem, że „w związku z trwającymi atakami na łańcuch dostaw i stosowaniem przez przeciwników na coraz to nowych taktyk, dostrzeżenie, że firma HPE stosuje podejście pozostawania o krok przed zagrożeniami powinno pozwolić konsumentom móc spać spokojnie, wiedząc, że firma HPE podziela ich interesy”.

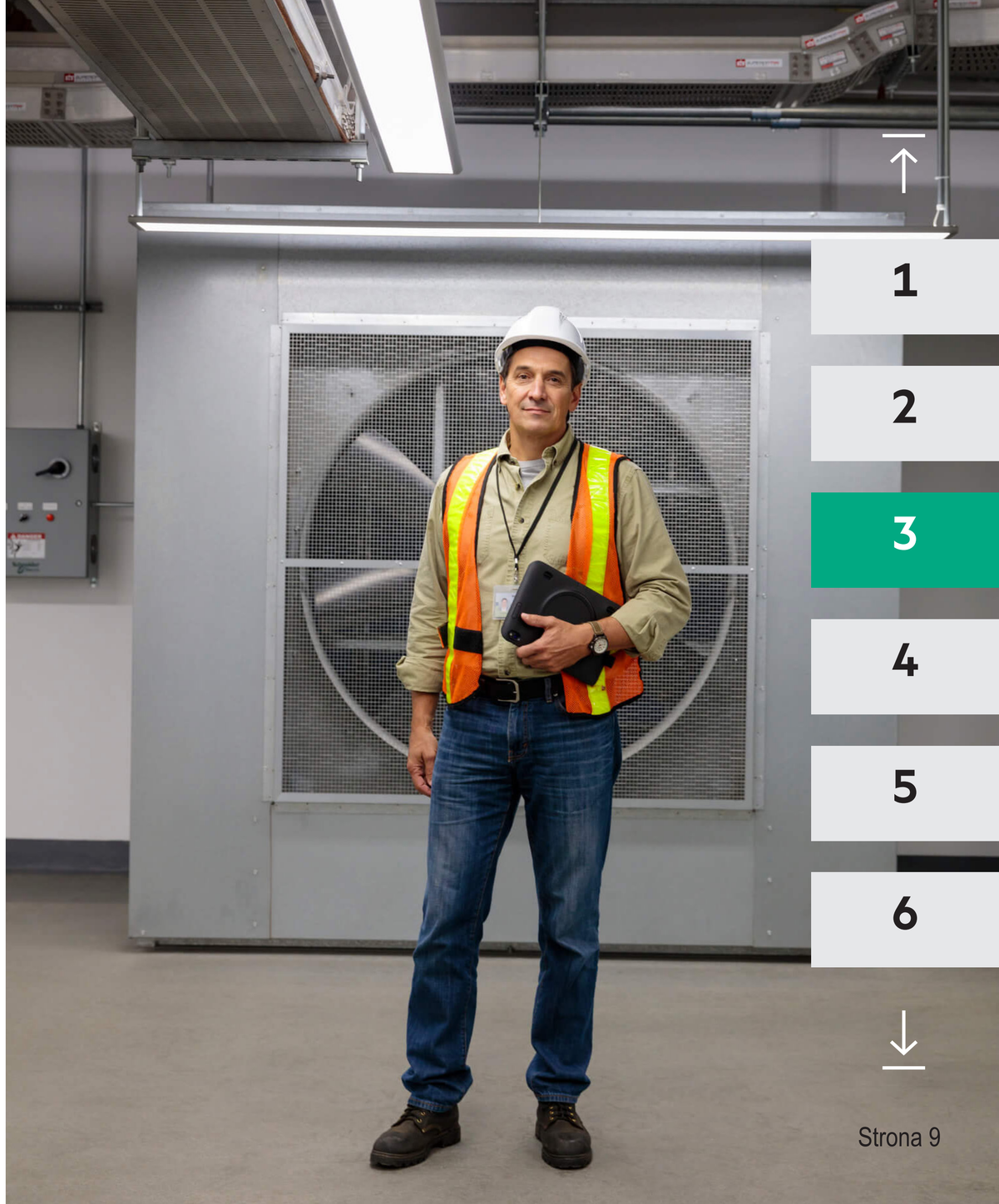
[6] „Zero Trust to wysiłek w całym cyklu życia”, Moor Insights & Strategy, 2021
[7] „Przeniesienie identyfikacji urządzeń i uwierzytelniania komponentów na serwery HPE Gen10 Plus”, InfusionPoints, LLC., 2021
[8] „HPE podnosi bezpieczeństwo łańcucha dostaw”, InfusionPoints, LLC., 2021

3. Zabezpieczenia dla każdej firmy

Wysokie bezpieczeństwo bez względu na branżę czy wielkość firmy

Jedynie serwery HPE Gen10 Plus mogą zapewnić przedsiębiorstwom, podmiotom rządowym lub małym i średnim firmom najwyższy poziom ochrony przed atakami na oprogramowanie sprzętowe, przy czym linia produktów HPE Gen10 Plus oferuje architekturę zerowego zaufania, która swój początek ma już w łańcuchu dostaw, rozciągając się dzięki potwierdzonemu kryptograficznie niezmiennemu łańcuchowi zaufania na krzem i dalej – niezależnie od zakupionej linii serwerów.

Przedsiębiorstwom i agencjom rządowym oferujemy serwery HPE ProLiant do montażu w szafie serwerowej, moduły obliczeniowe HPE Synergy oraz serwery HPE Apollo Systems o wysokiej gęstości i wysokiej wydajności obliczeniowej (HPC). W przypadku mniejszych firm i oddziałów zdalnych serwery w obudowie typu „tower” serii HPE ProLiant ML oferują taki sam mechanizm „Silicon root of trust from HPE” jak serwery o większej mocy.



Zabezpieczenia dla każdej firmy →

Rząd

Postępy firmy HPE w dziedzinie bezpieczeństwa cieszą się jeszcze większym zainteresowaniem sektora rządowego. W rozporządzeniu wykonawczym wydanym przez Administrację Joe Bidena z dnia 12 maja 2021 r. modele bezpieczeństwa Zero Trust są w wielu miejscach zachwalane jako najlepsza praktyka, której przestrzegać muszą agencje rządowe. Dalej wspomina się o usługach w chmurze, w tym Infrastructure as a Service (IaaS), Platform as a Service (PaaS) i Software as a Service (SaaS).[9]

Zapewniając elastyczny zakres konfiguracji, serwery HPE Gen10 Plus mogą być wdrażane jako część chmury prywatnej, stanowić podstawę maszyn wirtualnych, ułatwiać stosowanie bezpiecznych środowisk kontenerowych, przechowywać aplikacje baz danych i przetwarzać transakcje typu „Big Data" w prawie każdym federalnym środowisku IT.

Ponadto technologia HPE iLO 5 oferuje cztery różne poziomy bezpieczeństwa, w zależności od potrzeb klientów i regulacji sektora. Serwery HPE Gen10 Plus są wysyłane w trybie produkcyjnym, ale można je uaktualnić do trybu wysokiego bezpieczeństwa w celu zwiększenia stopnia zaawansowania szyfrowania, do trybu Federalnych Standardów Przetwarzania Informacji (FIPS) w celu zapewnienia zgodności z federalnymi standardami przetwarzania oraz do trybu Commercial National Security Algorithm (CNSA), który zapewnia najwyższy poziom algorytmów kryptograficznych spełniających standardy określone przez Agencję Bezpieczeństwa Narodowego.

Sprzedaż detaliczna

Na współczesnych platformach sprzedaży internetowej ponad 90% prób logowania w witrynach sprzedaży detalicznej to zautomatyzowane ataki inicjowane przez hakerów. W 2020 r. skradziono ponad 1,8 mld nazw użytkowników i haseł w wyniku 117 wycieków danych uwierzytelniających, w porównaniu z 77 w 2019 r.[10]

I nie chodzi tylko o kradzież haseł. Na poziomie przedsiębiorstwa sprzedawcy detaliczni wykonują znacznie więcej czynności niż samo tylko przetwarzanie transakcji online – przemieszczają produkty po całym świecie oraz pozyskują nowe i istniejące materiały za pomocą zaawansowanych systemów planowania zasobów przedsiębiorstwa (ERP), starając się chronić kluczowe informacje o pracownikach i klientach.

[9] „Rozporządzenie wykonawcze w sprawie poprawy stanu cyberbezpieczeństwa w kraju", whitehouse.gov, 2021
[10] „6 rzeczy na temat ataków ransomware, o których musi wiedzieć każda mała firma", inc.com, 2021

Zabezpieczenia dla każdej firmy →

Produkcja i dystrybucja

W każdym punkcie kontaktowym – w każdym zakładzie produkcyjnym, magazynie, przy każdym transferze i każdej dostawie – pojawia się okazja do zaistnienia dla złych aktorów, którzy mogą wprowadzić niechciane modyfikacje w produktach w drodze do użytkownika końcowego. To powszechny problem.

Firma HPE przezwyciężyła go, zabezpieczając swój łańcuch dostaw poprzez dostawy z użyciem identyfikatora iDevID, certyfikatów platformy i mechanizmu „Silicon Root of Trust from HPE”. Te bezpieczne rozwiązania, osadzone w krzemie serwerów Gen10 Plus, dają głównym służbom działającym w branży logistycznej i dostawczej wystarczającą pewność, pozwalając im wdrażać serwery HPE w swoich centrach danych.

Małe i średnie firmy

O ile w przypadku większych przedsiębiorstw naruszenia bezpieczeństwa mogą powodować uciążliwości, kary grzywny i problemy z lojalnością, to te same zagrożenia mogą mieć druzgocący wpływ na małe i średnie firmy. W rzeczywistości większość małych i średnich firm nie przetrwa takiego naruszenia – 60% rezygnuje z działalności po sześciu miesiącach. Nie pomaga to, że od 50% do 70% ataków ransomware nakierowanych jest właśnie na małe firmy. Co gorsza, około 80% ofiar zostaje zaatakowanych po raz drugi.[11]

Dzięki osadzeniu walidacji oprogramowania sprzętowego bezpośrednio w krzemie firma HPE stara się uczynić z bezpieczeństwa możliwie jak najbardziej zasadniczą sprawę i to jest dobra wiadomość dla małych i średnich firm, które często nie dysponują budżetami i personelem informatycznym pozwalającym im toczyć codzienną walkę o bezpieczeństwo.

[11] „2021 Raport o wypełnianiu poświadczeń”, f5.com, 2021

4. Bezpieczeństwo Twoich danych w każdym miejscu

Dane w stanie spoczynku, w ruchu, w użyciu

Ochrona informacji dotyczących klientów i innych wrażliwych danych to najbardziej problematyczne kwestie dla specjalistów IT. Firma HPE zapewnia zestaw rozwiązań w zakresie bezpieczeństwa danych na różnych etapach: dane w stanie spoczynku, dane w ruchu, dane w użyciu.

Dane w stanie spoczynku

Serwery HPE z Utimaco ESKM zapewniają kompletne rozwiązanie umożliwiające ujednolicenie i automatyzację kontroli szyfrowania organizacji poprzez bezpieczne tworzenie, zabezpieczanie, obsługiwanie, kontrolowanie oraz kontrolę dostępu do kluczy szyfrowania o znaczeniu krytycznym dla firmy i dla zapewnienia zgodności z przepisami w przypadku przesyłania danych w stanie spoczynku znajdujących się w pamięci masowej lub na serwerze lokalnym do innego węzła w sieci WAN. Serwer HPE ProLiant DL360/DL380 Gen10 Plus został zaprojektowany jako w pełni zintegrowane rozwiązanie i stanowi bezpieczne urządzenie serwerowe zatwierdzone przez Federalne Standardy Przetwarzania Informacji (FIPS) 140-2.

Dane w ruchu

Serwer HPE ProLiant z kartą usług rozproszonych Pensando zapewnia rozwiązania w zakresie bezpieczeństwa danych w ruchu i szereg innych zaawansowanych funkcji. W przeciwieństwie do faktu, że znaczna część mocy procesora serwerów jest wykorzystywana do celów zarządzania usługami sieciowymi, to rozwiązanie nie ma praktycznie żadnego wpływu na procesor serwera hosta. Zapewniając elastyczność biznesową, uproszczenie infrastruktury informatycznej i niższy całkowity koszt posiadania, to rozwiązanie firmy HPE jest dostępne w modelu wdrożeniowym CAPEX (wydatki inwestycyjne) oraz OPEX (wydatki operacyjne) za pośrednictwem rozwiązania HPE GreenLake.

Bezpieczeństwo Twoich danych w każdym miejscu →

Dane w użyciu

To rozwiązanie wykorzystuje serwer HPE ProLiant DL380T Trusted Supply Chain Server z procesorami Intel® Ice Lake SGX, zapewniając jedno okienko do zarządzania bezpiecznymi enklawami w obrębie poufnych węzłów obliczeniowych opartych na technologii SGX w centrum danych. Fortanix Confidential Computing Manager pomaga w zorkiestrowaniu krytycznych polityk bezpieczeństwa, takich jak weryfikacja tożsamości, kontrola dostępu do danych i poświadczanie kodu w enklawach, które są wymagane w przypadku poufnego przetwarzania danych.

Natomiast serwery HPE ProLiant do montażu w szafie rackowej z platformą XYGATE SecurityOne (XS1) firmy XYPRO Technology zapewniają ujednoliconą platformę do zarządzania bezpieczeństwem i analizą danych, która obejmuje zarządzanie ryzykiem w czasie rzeczywistym, wykrywanie zagrożeń, ocenę podatności na zagrożenia, raportowanie zgodności i monitorowanie integralności przy użyciu nowoczesnego interfejsu opartego na przeglądarce, zapewniającego kompleksowe bezpieczeństwo typu „ZERO Trust". Platforma XS1 aktywnie wykrywa zagrożenia bezpieczeństwa, przeglądając dane w czasie rzeczywistym i inteligentnie zaznaczając zdarzenia, które wymagają natychmiastowej uwagi.

Ochrona informacji dotyczących klientów i innych wrażliwych danych to najbardziej problematyczne kwestie dla specjalistów IT. Firma HPE zapewnia zestaw rozwiązań w zakresie bezpieczeństwa danych na różnych etapach: dane w stanie spoczynku, dane w ruchu oraz dane w realizacji.

Projekt Aurora

Włączenie architektury zabezpieczeń typu „edge-tocloud" zerowego zaufania firmy HPE

Projekt Aurora rozciąga nasz mechanizm „Silicon Root of Trust from HPE", zapewniając kompletną architekturę zabezpieczeń z nowymi wbudowanymi i zintegrowanymi rozwiązaniami bezpieczeństwa, począwszy od poziomu krzemu. Inicjowany w łańcuchu dostaw, ustanawia on niezmienny łańcuch zaufania aż do poziomu infrastruktury, systemu operacyjnego, platformy oprogramowania i obciążeń, nie wymagając podpisów, znaczących kompromisów w zakresie wydajności czy blokad.

Dzięki Projektowi Aurora możesz zapobiegać i wykrywać naruszenia bezpieczeństwa w komponentach sprzętowych i programowych zdalnie zarządzanego systemu HPE poprzez standaryzowane ciągłe pomiary, uwierzytelnianie i weryfikację każdego elementu. Projekt pomaga przekształcić bezpieczeństwo z bariery w przyspieszenie innowacji – od poziomu krzemu aż po obciążenia.

Takie ciągłe uwierzytelnianie umożliwi firmie HPE szybkie wykrywanie zaawansowanych zagrożeń w ciągu kilku sekund, minimalizując utratę danych i autoryzowane szyfrowanie (oraz uszkodzenie) cennych danych i własności intelektualnej.

5. Ochrona na przyszłość

W ostatnim czasie liczba i złożoność ataków na dane i systemy stale rośnie, przenosząc się z granic sieci, oprogramowania i aplikacji na samą fizyczną platformę. Jednak zapory sieciowe, skanowanie antywirusowe, a nawet narzędzia do monitorowania bezpieczeństwa są niewystarczające, ponieważ nie wykrywają ingerencji w oprogramowanie sprzętowe.

Mimo że zagrożenia te stale się rozwijają, HPE pozostaje jedynym producentem serwerów o standardzie przemysłowym z zabezpieczeniami wyprzedzającymi konkurencję o dwa pokolenia. Budowanie tego zaufania zaczyna się od bezkompromisowego i zaufanego łańcucha dostaw, pełniącego funkcję pierwszej linii obrony i zapewniającego bezpieczeństwo jeszcze przed przybyciem infrastruktury. W okresie eksploatacji serwerów HPE Gen10 Plus – wyposażonych w cyfrowy odcisk palca specyficzny dla danego serwera i automatyczne zabezpieczenia, w tym funkcję wczesnego wykrywania i odzyskiwania – ponad 4 miliony wierszy oprogramowania sprzętowego będzie chronionych przed złośliwym oprogramowaniem, złośliwym kodem i oprogramowaniem typu ransomware. A gdy nadchodzi czas wycofania z eksploatacji lub zmiany przeznaczenia starej infrastruktury, użytkownik również jest chroniony: bezpieczne usuwanie haseł, ustawień konfiguracyjnych i danych jest proste.

Zaangażowanie firmy HPE w zwiększanie bezpieczeństwa we wszystkich trzech kluczowych filarach środowiska – ochrona, wykrywanie i odzyskiwanie – zapewnia zaufanie już od poziomu oprogramowania sprzętowego.

Potrzebujesz pomocy w zakresie bezpieczeństwa? Dział HPE Pointnext Services oferuje najlepsze w swojej klasie usługi projektowe i wdrożeniowe w celu dalszego rozszerzania i uzupełniania wbudowanych funkcji serwerów HPE Gen10 Plus.

Chroń przyszłość swojej firmy dzięki HPE.

6. Zasoby

Strona internetowa

Zabezpieczenia HPE

Gra szkoleniowa

Pokój ucieczki

Broszura

Ograniczenie ryzyka dzięki bezpieczeństwu zarządzanemu przy użyciu HPE GreenLake Management Services

Raporty analityczne

- „Usuwanie luk w zabezpieczeniach IT - badanie globalne z 2020 r.”, opracowany przez Ponemon Institute
- „HPE podnosi bezpieczeństwo łańcucha dostaw”, opracowany przez InfusionPoints CyberSecurity Solutions
- „Przeniesienie identyfikacji urządzeń i uwierzytelniania komponentów na serwery HPE Gen10 Plus”, opracowany przez InfusionPoints CyberSecurity Solutions

Biała Księga

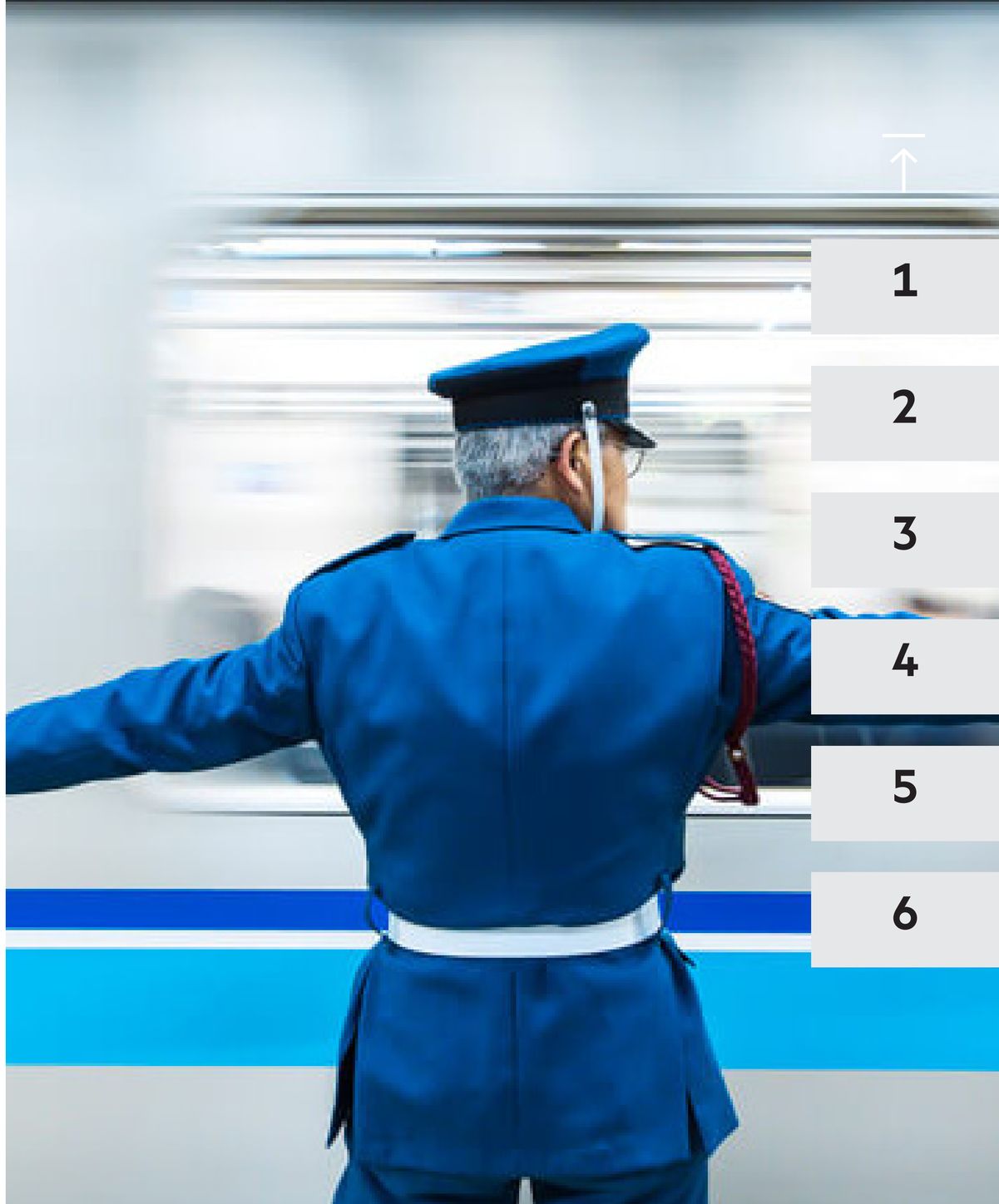
- „Zero Trust to wysiłek w całym cyklu życia”
- „HPE umożliwia architekturę Zero Trust dzięki Projektowi Aurora”

Przewodnik referencyjny

„Bezpieczeństwo Gen10 and Gen10 Plus”

Uzyskaj bezpieczeństwo 360° – wszędzie, gdzie potrzebujesz i zawsze, gdy potrzebujesz

Dowiedz się więcej na stronie
hpe.com/security/compute



1
2
3
4
5
6

Podejmij właściwą decyzję zakupową. Skontaktuj się z naszymi specjalistami obsługi przedsprzedażowej.

Rozpocznij czat (sprzedaż)

Zadzwoń teraz

Uzyskaj aktualizacje

Hewlett Packard Enterprise

Odwiedź HPE GreenLake

a50005077ENW, wersja 1