SCALITY

Fast
IT solutions

Więcej niż tylko niezmienność

5 poziomów odporności cybernetycznej niezbędnych w erze AI

Obietnica (i problem) niezmienności

Eksperci są zgodni: oprogramowanie ransomware jest obecnie największym zagrożeniem dla cyberbezpieczeństwa na świecie — *a sytuacja tylko się pogarsza*.

85%
organizacji było celem ataku oprogramowania ransomware co najmniej raz w ciągu ostatniego roku[1]

75%
ataków zdołało osłabić zdolność ich ofiar do odzyskania sprawności[2]

W świetle unikatowych wyzwań związanych z oprogramowaniem ransomware specjaliści ds. bezpieczeństwa podkreślają, jak ważne jest, by organizacje nadały priorytet zagadnieniu odporności cybernetycznej — tj. zdolności do szybkiego i łatwego radzenia sobie z cyberatakami — w swoich strategiach łagodzenia skutków ransomware.

Większość organizacji jako podstawę swoich ram odporności cybernetycznej przyjęła niezmienną pamięć masową. Tego typu systemy sprawiają, że kopie zapasowe są odporne na szyfrowanie lub niszczenie, dzięki czemu oferują kuszącą obietnicę: zawsze będziemy mieli dostęp do czystej kopii zapasowej i możliwości jej przywrócenia po ataku ransomware — bez względu na wszystko.

Mimo to zalecamy ostrożność... W praktyce nie wszystkie systemy „niezmiennej" pamięci masowej spełniają tę obietnicę.

„Największym globalnym zagrożeniem cybernetycznym, przed którym wciąż stoimy, jest oprogramowanie ransomware...

Ataki ransomware są silne i szybkie. Szybko ewoluują, są wszechobecne, a zorganizowane grupy przestępcze coraz częściej oferują je jako usługi, co obniża barierę wejścia w cyberprzestępczość".

Lindy Cameron

Dyrektor generalny Brytyjskiego Narodowego Centrum Cyberbezpieczeństwa (NCSC)

„Aktualne kopie zapasowe to najskuteczniejszy sposób na odzyskanie danych po ataku oprogramowania ransomware".

Wskazówki NCSC: łagodzenie skutków ataków złośliwego oprogramowania i ransomware

94% **liderów IT** obecnie polega na niezmiennej pamięci masowej[3]

1 Data Protection Trends Report 2023, Veeam [2] Ransomware Trends Report, Veeam [3] 2023 Data Immutability Survey, Vanson Bourne

Większość systemów „niezmiennej” pamięci masowej nie jest tak naprawdę niezmienna

Pamięć niezmienna odnosi się do paradygmatu przechowywania danych, w którym po zapisaniu danych nie można ich modyfikować ani usuwać przez z góry określony czas.

Takie podejście — jeśli zostanie poprawnie wdrożone — tworzy ostatnią linię obrony przed tradycyjnymi atakami ransomware, które mają na celu zaszyfrowanie lub usunięcie danych kopii zapasowych.

Niestety, większość dostępnych na rynku „niezmiennych” rozwiązań pozostawia luki w zabezpieczeniach, które mogą zostać wykorzystane przez atakujących do pokonania tych zabezpieczeń, wyłączenia ich lub ominięcia w inny sposób.

Np. tradycyjne systemy plików często czynią dane niezmiennymi poprzez tworzenie zaplanowanych, okresowych migawek. Mimo że systemy te zapewniają pewien stopień ochrony, nieuchronnie pozostawiają otwarte luki w zabezpieczeniach, ponieważ między migawkami może upłynąć czas liczony co najmniej w godzinach. W tych okresach dane są podatne na naruszenie, co naraża organizację na potencjalne ataki i utratę newralgicznych danych.

Jeśli możesz to zrobić, to samo może zrobić atakujący — podając się za Ciebie.

Inne rozwiązania zawodzą, ponieważ implementują niezmienność tylko na poziomie API, ale nie w architekturze bazowej.

Jeśli system jest oparty na architekturze bazowej, która z natury nie zapobiega usuwaniu lub nadpisywaniu danych, każdy atakujący, który pokona warstwę API — np. uzyskując dostęp administratora — może po prostu ominąć zabezpieczenia API, aby usunąć, zaszyfrować lub wyłączyć kopie zapasowe.

Jedynym sposobem na ochronę przed tego typu atakami „eskalacji uprawnień” jest upewnienie się, że nikt nie jest w stanie usunąć ani zastąpić kopii zapasowych — nawet superadministrator systemu.

Czym jest prawdziwa niezmienność?

Prawdziwie niezmienny system przechowywania danych musi mieć wszystkie następujące właściwości, a każde niedopatrzenie skutkuje osłabieniem jego nadrzędnej funkcji:

- Dane muszą zyskiwać niezmienność natychmiast w momencie ich zapisu. Minimalizuje to ryzyko utraty danych, ponieważ nigdy nie zabraknie czystej, aktualnej kopii zapasowej do przywrócenia.
- Niezmienność musi być zaimplementowana na poziomie architektury bazowej. Oznacza to, że nawet atakujący z najwyższym poziomem dostępu nie może usuwać ani zastępować kopii zapasowych.
- System musi umożliwiać precyzyjną kontrolę niezmienności danych, aby zapewnić zgodność z przepisami biznesowymi i rządowymi.

Niezmienność nie jest w stanie powstrzymać ataków eksfiltracyjnych

Współczesne metody działania ransomware nie ograniczają się już tylko do prostych ataków szyfrujących. Ze względu na wzrost liczby niezmiennych kopii zapasowych atakujący częściej stosują ataki polegające na „podwójnym wymuszeniu", których celem jest kradzież poufnych danych. Taktykę tę spopularyzowało złośliwe oprogramowanie takie jak Maze i DoppelPaymer.

Wykradzione dane są następnie wykorzystywane do szantażowania organizacji: przestępcy grożą opublikowaniem poufnych informacji w Internecie lub sprzedaniem ich konkurencji, jeśli nie zostanie zapłacony okup. Obecnie większość ataków ransomware obejmuje komponent eksfiltracji.

Zatrzymanie tego typu ataków wymaga wdrożenia wielu warstw zabezpieczeń wszędzie tam, gdzie można znaleźć poufne dane — w danych produkcyjnych organizacji, w strumieniach danych przesyłanych przez sieć, a nawet w kopiach zapasowych. Co najważniejsze, ataki eksfiltracyjne nie polegają na szyfrowaniu lub modyfikowaniu danych w celu uzyskania okupu, dlatego sama niezmienność danych nie zapobiegnie tego typu zagrożeniom.

91%

współczesnych ataków ransomware obejmuje eksfiltrację[1]

FIRMY SĄ

2,5x

bardziej skłonne do zapłacenia okupu, gdy dane zostały wykradzione, a nie tylko zaszyfrowane[2]

Nie eliminuje też problemu przechowywania w pojedynczych lokalizacjach

Dane przechowywane w jednej fizycznej lokalizacji od zawsze są narażone na utratę w wyniku pożarów, powodzi i innych klęsk żywiołowych. Taktyki stosowane obecnie przez zorganizowane grupy przestępcze zajmujące się oprogramowaniem ransomware sprawiają, że ta ryzykowna praktyka stała się o wiele bardziej niebezpieczna.

Przestępcy nauczyli się atakować wiele organizacji jednocześnie, obierając za cel całe centra danych. Zwiększa to ich potencjalny zarobek, jednocześnie stwarzając zagrożenie katastrofalnej utraty danych, przestojów operacyjnych i znaczących konsekwencji finansowych po stronie wszystkich dotkniętych organizacji.

Aby zminimalizować te zagrożenia, przechowywanie kopii zapasowych w wielu lokalizacjach musi być proste, praktyczne i niedrogie. Niestety, w tym aspekcie zawodzi wiele rodzajów niezmiennych pamięci masowych, ponieważ nie obsługują one replikacji danych w wielu lokalizacjach albo jej wdrożenie byłoby nieopłacalne lub niepraktyczne.

70%

małych i średnich przedsiębiorstw upada w ciągu roku od zdarzenia, w którym doszło do utraty dużej ilości danych[3]

1 The State of Ransomware Annual Report 2023, Blackfog [2] Cybersecurity Trends 2023, Allianz [3] 11 Common Causes of Data Loss, Consoltech

Poprzeczka coraz wyżej: czyli jak sztuczna inteligencja zmienia środowisko zagrożeń ransomware

Technologie AI i uczenia maszynowego rozwijają się w zawrotnym tempie. Cyberprzestępcy już teraz wykorzystują ich osiągnięcia, aby tworzyć skuteczniejsze, bardziej szkodliwe i trudniejsze do wykrycia formy oprogramowania ransomware.

Aby przetrwać, organizacje muszą być przygotowane na brutalną serię wydarzeń: drastyczny wzrost zarówno liczby, jak i stopnia wyrafinowania ataków ransomware.

Brytyjskie Narodowe Centrum Cyberbezpieczeństwa przewiduje, że sztuczna inteligencja wpłynie na środowisko ransomware poprzez:

- Obniżenie progu wejścia do „biznesu" ransomware, co będzie skutkować dużą liczbę początkujących przestępców
- Łatwiejsze wykrywanie luk w zabezpieczeniach i omijanie zabezpieczeń przez doświadczonych i zdolnych przestępców
- Pomaganie przestępcom w opracowywaniu ataków socjotechnicznych w łatwiejszy i znacznie bardziej precyzyjny sposób, dzięki czemu ataki z wykorzystaniem eskalacji uprawnień staną się łatwiejsze do przeprowadzenia
- Znaczne zwiększenie szybkości ataku — strategiczne atakowanie newralgicznych danych, neutralizowanie kopii zapasowych i unieruchamianie mechanizmów obronnych

„AI już dziś jest wykorzystywana w szkodliwych działaniach cyberprzestępców i niemal na pewno w najbliższej przyszłości zwiększy liczbę i wpływ cyberataków — w tym oprogramowania ransomware".

Brytyjskie Narodowe Centrum Cyberbezpieczeństwa (NCSC)

Jak wykorzystuje się AI/ML we współczesnych atakach ransomware?

- Korzystanie z narzędzi AI i LLM w celu znacznego zwiększenia ilości i precyzji ataków socjotechnicznych, co czyni je bardziej skutecznymi i trudniejszymi do wykrycia
- Opracowywanie adaptacyjnego złośliwego oprogramowania, które zmienia własny kod, aby unikać algorytmów wykrywania
- AI i ML stosowane przeciwko systemom wykrywania włamań w celu maskowania złośliwego ruchu sieciowego
- Stosowanie ML do szybszego i zautomatyzowanego wykrywania niezałatanych luk w zabezpieczeniach i zagrożeń zero-day
- Korzystanie z AI/ML do rozpoznawania i wyodrębniania kodów PIN, haseł i innych czynników uwierzytelniających ze zhakowanych danych z czujników urządzeń przenośnych (mikrofonu, akcelerometru itp.)

Przedstawiamy CORE5

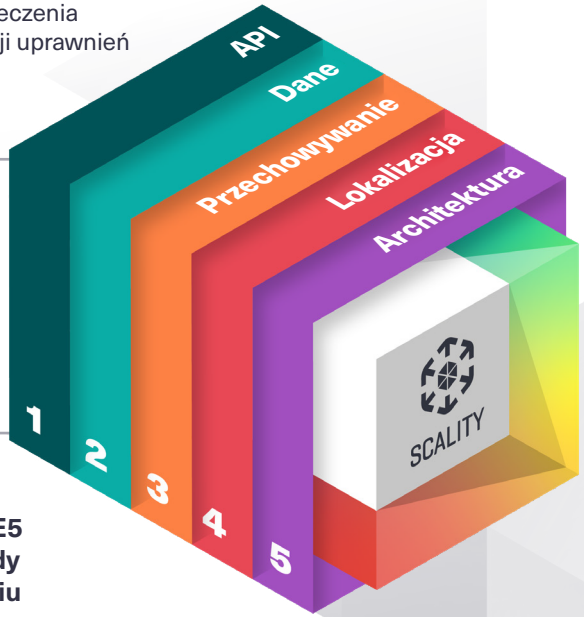
Nowy standard cyberodpornej pamięci masowej

Tzw. niezmienne kopie zapasowe — niegdyś uznawane za złoty standard w ochronie przed oprogramowaniem ransomware — nie wystarczają już, aby zapewnić ochronę przed pełną gamą obecnych i przyszłych zagrożeń ransomware.

Aby właściwie reagować na szybko zmieniające się wyzwania, przed którymi stoją obecnie organizacje, branża pamięci masowych musi wyjść poza samą koncepcję niezmienności i przyjąć nowy, bardziej złożony standard kompleksowej **odporności cybernetycznej**.

Podejście to musi obejmować nie tylko najsilniejszą formę rzeczywistej niezmienności, ale także solidne, wielowarstwowe zabezpieczenia przed atakami polegającymi na eksfiltracji danych i eskalacji uprawnień oraz innymi nowo powstającymi wektorami zagrożeń.

Firma Scality określiła pięć newralgicznych poziomów zabezpieczeń, które są niezbędne do osiągnięcia tak ambitnego poziomu ochrony danych. Nazwaliśmy je podejściem CORE5.



W dalszej części szczegółowo przyjrzymy się CORE5 — w tym sposobowi, w jaki wdrożyliśmy jego zasady w ARTESCA, naszym nagradzanym oprogramowaniu pamięci masowej odpornym na ataki ransomware.

1. Odporność na poziomie API

Niezmienność zaimplementowana na poziomie API oferuje wydajną ochronę najwyższej klasy przed atakami ransomware. Takie rozwiązanie zapewnia niezmienność kopii zapasowych od momentu ich utworzenia.

2. Odporność na poziomie danych

Wielowarstwowe środki bezpieczeństwa na poziomie danych uniemożliwiają atakującym dostęp do przechowywanych danych i ich eksfiltrację.

3. Odporność na poziomie pamięci masowej

Wdrażamy zaawansowane techniki kodowania, aby zapobiec niszczeniu lub eksfiltracji kopii zapasowych. Dzięki tym technikom dane przechowywane w systemie stają się niemożliwe do odczytania dla przestępców — nawet tych, którzy używają skradzionych uprawnień dostępu, aby ominąć zabezpieczenia na wyższym poziomie.

4. Odporność na poziomie geograficznym

Proste i niedrogie kopie przechowywane w wielu lokalizacjach zapobiegają utracie danych — nawet jeśli celem ataku padnie całe centrum danych.

5. Odporność na poziomie architektury

Wewnętrznie niezmienna architektura bazowa sprawia, że dane są zawsze przechowywane w pierwotnej formie — nawet jeśli atakujący uzyska niezbędne uprawnienia dostępu, które pozwolą mu ominąć niezmienność na poziomie API.

1. Odporność na poziomie API

Cyberprzestępcy często podejmują próby naśladowania poleceń aplikacji, aby zaszyfrować, zmodyfikować lub usunąć zapisane kopie zapasowe. Zapewnienie niezmienności na poziomie API zapobiega próbom nadpisania danych przez użytkownika lub aplikację, która wydaje polecenia S3 w odniesieniu do zestawu danych.

Wprowadzenie interfejsu API niezmienności (S3 Object Lock) w popularnym API AWS S3 zaowocowało stworzeniem de facto standardowego interfejsu dla aplikacji ochrony danych, który pozwala na optymalne zarządzanie niezmiennością pamięci masowej. Umożliwia on aplikacjom, takim jak Veeam Data Platform, włączanie blokowania obiektów, określanie zasad przechowywania i wymuszanie egzekwowania trybu zgodności bezpośrednio w magazynie obiektów.

Dostęp aplikacji do pamięci masowej za pośrednictwem interfejsu API S3 daje użytkownikowi w pełni zintegrowane rozwiązanie do tworzenia kopii zapasowych, które — w połączeniu z uwierzytelnianiem komend i zasadami kontroli dostępu w stylu AWS — blokuje złośliwy dostęp.

Scality ARTESCA w praktyce

Obsługa interfejsów API S3 Object Lock przez rozwiązanie ARTESCA gwarantuje niezmienność kopii zapasowych od momentu ich utworzenia. Takie podejście zapewnia również pewien stopień elastyczności i niezwykle szczegółową kontrolę, której nie da się osiągnąć w przypadku starszych rozwiązań pamięci masowej.

Aby zapewnić niezmienność danych w określonych horyzontach czasowych — zgodnie z wymogami zasad biznesowych i przepisów regulacyjnych:

- **Konfigurowalne zasady przechowywania** pozwalają dostosować czas, w którym dane pozostają w pełni niezmienne, niezależnie od tego, czy są to dni, lata, czy czas nieokreślony.
- **Tryb zgodności** zapewnia dodatkowe wzmocnienie, ponieważ zapobiega zmianie konfiguracji niezmienności nawet przez superadministratora systemu.

Tak duży stopień personalizacji jest korzystny dla wszystkich przedsiębiorstw i jest absolutnie niezbędny w branżach, które przetwarzają dane wrażliwe — takich jak opieka zdrowotna i finanse, gdzie przestrzeganie rygorystycznych przepisów ma priorytetowe znaczenie.

2. Odporność na poziomie danych

Ochrona przed atakami polegającymi na eksfiltracji danych wymaga rygorystycznych protokołów bezpieczeństwa — wszędzie tam, gdzie można znaleźć poufne dane: od danych produkcyjnych po system przechowywania kopii zapasowych, a także wszędzie pomiędzy nimi.

Odpowiednio zabezpieczone rozwiązanie pamięci masowej powinno zawierać wiele warstw zabezpieczeń na poziomie danych, obejmujących kompleksowe zarządzanie tożsamością i dostępem (IAM) i funkcje kryptograficzne. To pozwoli mieć pewność, że dane kopii zapasowych nie zostaną przechwycone ani udostępnione nieupoważnionym osobom.

Scality ARTESCA w praktyce

Aby chronić najbardziej wrażliwe dane przed niepożądanymi osobami, ARTESCA korzysta z kompleksowego zestawu zabezpieczeń na poziomie danych:

- **Uwierzytelnianie zgodne ze standardem AWS** oraz **funkcje IAM w stylu AWS** zapewniają niezwykle szczegółową kontrolę dostępu, co pozwala organizacjom na definiowanie i egzekwowanie zasad regulujących dostęp użytkowników do zasobów danych. Takie podejście gwarantuje, że tylko upoważnieni użytkownicy z odpowiednimi uprawnieniami będą mogli uzyskać dostęp do wrażliwych danych, co zmniejszy ryzyko eksfiltracji danych przez osoby nieupoważnione.
- **Architektura zerowego zaufania (ZTA)** ogranicza złośliwy dostęp, wymuszając podejście „nigdy nie ufaj, zawsze weryfikuj” w procesie uwierzytelniania użytkowników — urządzeń i użytkowników nie uznaje się domyślnie za zaufanych, nawet jeśli podłączają się do sieci z uprawnieniami lub zostali wcześniej zweryfikowani.
- **Bezpieczne zakończenie protokołu HTTPS/TLS w punktach końcowych S3 i automatyczna konfiguracja reguł zapory sieciowej** zapobiega przechwytywaniu i podsłuchiwaniu na poziomie połączeń, co zapewnia poufność i integralność danych podczas ich przesyłu.
- **Szyfrowanie danych w stanie spoczynku za pomocą 256-bitowego algorytmu AES** gwarantuje, że nawet w przypadku nieautoryzowanego dostępu dane pozostaną niezrozumiałe i bezużyteczne dla atakującego bez odpowiednich kluczy deszyfrujących.

3. Odporność na poziomie pamięci masowej

Jeśli zaawansowany przestępca będzie w stanie uzyskać dostęp do konta root serwera pamięci masowej, możliwe będzie ominięcie zabezpieczeń wyższego poziomu zaimplementowanych na poziomie API.

W przypadku braku silnych zabezpieczeń na poziomie pamięci masowej taki przestępca mógłby odczytać, nadpisać lub zniszczyć dane bezpośrednio na fizycznych dyskach pamięci masowej, narażając tym samym na szwank fundamenty systemu tworzenia kopii zapasowych.

Zaawansowane, oparte na sztucznej inteligencji metody pokonywania kontroli uwierzytelniania — takie jak rozpoznawanie haseł wyłącznie na podstawie dźwięku wciskanych klawiszy — sprawiają, że w przyszłości zapobieganie takim atakom będzie coraz trudniejsze.

Aby zapewnić odporność w obliczu tak szybko rozwijających się zagrożeń, system pamięci masowej musi gwarantować bezpieczeństwo danych, nawet jeśli atakujący będzie w stanie przeniknąć do najgłębszego poziomu systemu pamięci masowej.

Scality ARTESCA w praktyce

Aby zapewnić odporność na przyszłe zagrożenia związane z warstwą pamięci masowej, ARTESCA wdraża technologię rozproszonego kodowania wymazywania.

Takie podejście chroni dane poprzez ich fragmentację na mniejsze „części", rozszerzanie i kodowanie przy użyciu nadmiarowych danych, a następnie inteligentne rozpraszanie tych części na wszystkich dyskach w systemie. ARTESCA wykracza poza standardy branżowe, chroniąc dane lokalizacyjne tych fragmentów w bezpiecznym, **wzmocnionym repozytorium** za pomocą własnego, odrębnego, niewspółdzielonego uwierzytelniania i kontroli dostępu.

Zablokowanie atakującym dostępu do lokalizacji każdej przechowywanej części danych sprawia, że wszelkie uzyskane dane stają się niemożliwe do odczytania, a co za tym idzie — bezwartościowe.

Co więcej, zastosowanie nadmiarowego kodowania pozwala ARTESCA na pełną rekonstrukcję danych, które zostały uszkodzone lub utracone na skutek ataku, nawet jeśli dojdzie do fizycznego zniszczenia wielu dysków lub całego serwera.

4. Odporność na poziomie geograficznym

Szczególnie narażone na cyberzagrożenia są dane przechowywane w jednej lokalizacji. Atakując wartościowe cele — takie jak centra danych — cyberprzestępcy starają się wymusić okup od wielu organizacji jednocześnie, zwiększając tym samym swoje szanse na jego skuteczne zebranie.

Co ważne, nawet systemy odizolowane od sieci mogą zostać zaatakowane przez osoby z nieautoryzowanym dostępem fizycznym, a nawet ulec zniszczeniu w wyniku pożarów, powodzi lub innych klęsk żywiołowych.

Aby zapewnić ochronę przed tymi i innymi lukami w zabezpieczeniach pojedynczych lokalizacji, aktualne najlepsze praktyki w zakresie pamięci masowej zalecają przechowywanie wielu kopii zapasowych poza siedzibą firmy, w różnych lokalizacjach geograficznych. Nowoczesne, odporne rozwiązanie do przechowywania danych musi sprawić, że stanie się to nie tylko wykonalne, ale też łatwe do zrealizowania.

Scality ARTESCA w praktyce

Aby zminimalizować ryzyko związane z przechowywaniem danych w jednej lokalizacji, rozwiązanie ARTESCA zostało zaprojektowane z myślą o prostej, praktycznej i niedrogiej redundancji geograficznej w wielu lokalizacjach.

- **Replikacja w wielu lokalizacjach** umożliwia łatwe kopiowanie danych do zdalnych miejsc docelowych ARTESCA w innych centrach danych lub do pamięci masowej w chmurze w AWS, Azure, Google oraz coraz większej liczby regionalnych dostawców usług.
- **Wdrożenia w wielu lokalizacjach:** w przypadku aplikacji do tworzenia kopii zapasowych, które samodzielnie zarządzają wieloma kopiami i warstwami, rozwiązanie ARTESCA można łatwo wdrożyć i zarządzać nim zdalnie.
- **Elementy sterujące IAM specyficzne dla danej lokalizacji** utrudniają dostęp do zdalnych lokalizacji osobom, które przedostały się do pierwszej lokalizacji. Elementy te tworzą wiele „domen bezpieczeństwa”, które atakujący musiałby przekroczyć, aby uzyskać dostęp do wszystkich instancji danych.

5. Odporność na poziomie architektury

Wiele rozwiązań pamięci masowej zaprojektowanych przed erą oprogramowania ransomware jest narażonych na ataki na poziomie architektury bazowej. Te starsze rozwiązania są oparte na systemach plików, które umożliwiają łatwe usuwanie lub zastępowanie danych, co jest krytyczną wadą projektową, która działa na korzyść przestępców.

W trakcie aktywnego ataku ransomware jednym z priorytetów atakującego jest eskalacja jego uprawnień. Jeśli uda mu się uzyskać poświadczenia administratora, będzie w stanie wyłączyć lub obejść niezmienność danych na poziomie interfejsu API, przez co system stanie się bezbronny, a dane całkowicie narażone na atak.

Jeżeli przestępca, który posiada skradzione dane uwierzytelniające, jest w stanie po prostu wyłączyć niezmienność w systemach kopii zapasowych, wówczas taka „niezmienność" jest jedynie iluzją bezpieczeństwa. Biorąc pod uwagę to, jak szybko rozprzestrzeniają się narzędzia hakerskie i złośliwe oprogramowanie oparte na sztucznej inteligencji, każdy system pamięci masowej bazujący na tak podatnej architekturze staje się coraz bardziej narażony na ataki ransomware na poziomie samej architektury.

Scality ARTESCA w praktyce

ARTESCA została zaprojektowana tak, aby zapewnić możliwie najsilniejszą ochronę przed oprogramowaniem ransomware — począwszy od sposobu, w jaki jej architektura bazowa obsługuje zapis danych na dysku:

- Gdy aplikacja wydaje polecenie nadpisania danych, architektura rozwiązania ARTESCA, która **sama w sobie jest niezmienna**, implementuje to żądanie jako zapis nowego „obiektu", zachowując jednocześnie zapis lokalizacji pierwotnych, nietkniętych danych.
- Żądania usunięcia danych tworzą znacznik logiczny zdarzenia, pozostawiając przy tym oryginalne dane w nienaruszonym stanie.
- **Wzmocniony pod względem bezpieczeństwa system operacyjny Linux** domyślnie nie zezwala na dostęp do konta root, co zmniejsza ryzyko wystąpienia typowych luk i zagrożeń (CVE) oraz szerokiej gamy zagrożeń.

Efekt jest prosty: nigdy nie nastąpi usunięcie ani nadpisanie danych.

Najczęstsze rodzaje ataków ransomware są blokowane.

Kompleksowa odporność cybernetyczna: jak radzą sobie systemy pamięci masowej?

Aby skutecznie stawić czoła szybko zmieniającym się wyzwaniom, z jakimi borykają się współczesne organizacje, branża pamięci masowych musi wykroczyć poza samą niezmienność na poziomie API i przyjąć kompleksowe podejście do cyberodporności.

	Poziomy odporności CORE5				
	API	Dane	Przechowywanie	Lokalizacja	Architektura
ARTESCA	SILNY	SILNY	SILNY	SILNY	SILNY
Pamięć obiektowa oparta na RAID lub systemach plików	SILNY	SŁABY	ZALEŻNY OD DOSTAWCY	SILNY	ZALEŻNY OD DOSTAWCY
Migawki NAS/systemu plików	BRAK	SŁABY	SŁABY	ZALEŻNY OD DOSTAWCY	BRAK
Urządzenia deduplikujące	BRAK	ZALEŻNY OD URZĄDZENIA	SILNY	SILNY	SILNY
Repozytoria Linux wzmocnione przez hardening	BRAK	BRAK	SILNY	BRAK	CZĘŚCIOWY

Scality ARTESCA to *jedyne* rozwiązanie do przechowywania kopii zapasowych, które zapewnia **kompleksową odporność cybernetyczną** połączoną z niezawodną ochroną danych na każdym poziomie systemu — od interfejsu API po architekturę.

Odporność to wybór.

Ataki ransomware — wręcz przeciwnie.

W erze oprogramowania ransomware ochrona danych kopii zapasowych stała się ważniejsza niż kiedykolwiek wcześniej.

Rozwój sztucznej inteligencji powoduje, że ataki ransomware stają się coraz częstsze i bardziej wyrafinowane. Przestępcy przyjęli przy tym określone strategie, takie jak eksfiltracja danych i podnoszenie poziomu uprawnień, próbując w ten sposób obejść zabezpieczenia oferowane przez rozwiązania do tworzenia niezmiennych kopii zapasowych.

W obliczu szybko zmieniających się zagrożeń cybernetycznych nawet technologie pamięci masowej, które w przeszłości były najlepsze, dziś mogą okazać się nieskuteczne.

Nowa era ataków ransomware wymaga nowego standardu odporności cybernetycznej — takiego, w którym niezmienność będzie tylko jednym z elementów wielopoziomowej strategii ochrony danych.

Aby szybko i łatwo radzić sobie w obliczu nieuniknionych i coraz częstszych cyberataków, konieczne jest uzyskanie kompleksowej odporności cybernetycznej. Tylko Scality ARTESCA spełnia ten nowy, rygorystyczny standard.

Jak odporne jest Twoje obecne rozwiązanie kopii zapasowych?

OCEŃ SWOJĄ ODPORNOŚĆ CYBERNETYCZNĄ

Uwielbiasz Veeam? My też!

PRZECZYTAJ 6 POWODÓW, DLA KTÓRYCH ARTESCA JEST NAJLEPSZYM ROZWIĄZANIEM DO VEEAM

Poznaj możliwości ARTESCA

OBEJRZYJ PREZENTACJĘ I ROZPOCZNIJ 30-DNIOWY OKRES PRÓBNY

Kopie zapasowe najwyższej klasy.

ARTESCA to rozwiązanie opracowane przez Scality — globalnego lidera w dziedzinie pamięci masowych odpornych na zagrożenia cybernetyczne w erze AI. Firma Scality ośmiokrotnie uzyskała tytuł Gartner Magic Quadrant Leader. Z naszych rozwiązań korzysta obecnie ponad 500 przedsiębiorstw i 700 milionów użytkowników na całym świecie. Scality rozwiązuje główne problemy organizacji związane z przechowywaniem danych, jakimi są bezpieczeństwo, wydajność i koszty.

SCALITY

San Francisco • Paryż • Waszyngton • Tokio • Londyn