arcserve®

DIE EINDRUCKSVOLLE WIRKUNG VON RANSOMWARE AUF VERBRAUCHERTREUE UND KAUFVERHALTEN

Wenn Sie glauben, dass Ihr Unternehmen immun ist, denken Sie noch einmal darüber nach. Neueste Studien zeigen, dass die Verbraucher nicht so nachsichtig sind, wie Sie vielleicht denken Sie werden erkennen, wie schnell sie sagen werden, genug ist genug – und dann sind sie weg.

Inhaltsverzeichnis

WISSENSWERTES ÜBER DIESE UNTERSUCHUNG

Cyberattacken haben Organisationen lahm gelegt. Die Medien haben ausführlich über ihre verheerenden Auswirkungen berichtet, und heute verstehen die meisten in der IT-Community, was auf dem Spiel steht. Was jedoch nicht verstanden wird - und was Organisationen selten diskutieren oder in Betracht ziehen - sind die quantifizierbaren kurz- und langfristigen Auswirkungen von Ransomware-Angriffen auf das Kaufverhalten und die Markentreue der Verbraucher.

Wann werden die Verbraucher nach einer Cyberattacke sagen, es reicht? Ab welchem Zeitpunkt werden sie sich nach einem konkurrenzfähigen Produkt oder einer Dienstleistung umsehen? Wir haben 1.998 Verbraucher in Deutschland, Großbritannien, Frankreich und USA befragt, um dies herauszufinden.

Über unsere Umfrageteilnehmer

Mehr als die Hälfte der Befragten machen Online-Transaktionen - drei Viertel der Befragten nutzen Konten für Online-Banking und fast 80 % für digitale Kommunikation. Interessanterweise ist sich die Mehrheit nicht nur der Bedrohungen für die Datensicherheit bewusst, sondern engagiert sich auch aktiv für bewährte Datenschutzverfahren. Sie verwenden Antiviren-Software, installieren Updates, verwenden Zwei-Faktor-Authentifizierung, halten Passwörter geheim und ändern sie regelmäßig.

Halten die Unternehmen auch ihren Teil der Abmachung ein?

Die Verbraucher scheinen nicht so zu denken. Fast 70% der Umfrageteilnehmer glauben, dass die Unternehmen nicht genug tun, um ihre vertraulichen Informationen angemessen zu schützen, und sie gehen davon aus, dass ihre Daten ohne ihr Wissen bereits kompromittiert wurden.

Dies sollte eine eindringliche Warnung sowohl für die Unternehmens- als auch für die IT-Führungskräfte sein, insbesondere angesichts der Tatsache, dass fast neun von zehn Befragten die Vertrauenswürdigkeit eines Unternehmens beurteilen, bevor sie ein Produkt oder eine Dienstleistung kaufen.

Wie viele Kunden verlieren Sie dadurch möglicherweise?

DIE WICHTIGSTEN ERKENNTNISSE

Die Verbraucher, die wir befragt haben, machten es überdeutlich: Wenn Sie es nicht schaffen, ihre Daten vor Ransomware-Angriffen zu schützen oder den Zugang zu ihren Informationen ermöglichen - und sei es auch nur einmal -, dann werden sie direkt die Seiten wechseln, und zwar zu einem Wettbewerber, der das kann.

70%

der Umfrageteilnehmer glauben, dass Unternehmen nicht genug tun, um ihre Informationen angemessen zu schützen - und sie vermuten, dass ihre Daten bereits gefährdet waren, ohne dass sie es wissen

39%

sagten, dass Sicherheitsbedenken bezüglich ihrer personenbezogenen Daten (pb-Daten) der einzige Grund dafür waren, dass sie kein Kundenkonto eröffnen oder keine Geschäfte mit einem Unternehmen tätigen wollten

93%

achten auf die Vertrauenswürdigkeit eines Unternehmens vor dem Einkauf

59%

teilten mit, dass sie es wahrscheinlich vermeiden würden, Geschäfte mit einem Unternehmen zu machen, das im vergangenen Jahr einen Cyberangriff erlebt hat - und dass der Grad ihrer Nachsicht sich auch langfristig nicht bessern wird.

28%

sagten, dass sie ihr Geschäfte zu einem Wettbewerber bringen würden, wenn sie auch nur auf eine einzige Serviceunterbrechung, eine fehlgeschlagene Transaktion oder einen Fall von unzugänglichen Informationen stoßen würden - wobei fast 60 % sagten, es würde maximal zwei Unterbrechungen oder fehlgeschlagene Transaktionen erfordern

84%

gaben zu, dass sie ihre negativen, mit Ransomware -Forderungen verbundenen Erlebnisse mit ihrer Familie, ihren Freunden oder Kollegen teilen, ihre Erfahrungen online posten oder per E-Mail über die Vorfälle berichten

43%

sagten, ihre Datensicherheit sei so wichtig, dass sie bereit wären, mehr für Produkte und Dienstleistungen eines Unternehmens zu bezahlen, von dem sie glauben, dass es zuverlässig und sicher ist - wobei viele Branchen erleben, dass dieser Prozentsatz auf 50% oder mehr ansteigt

RANSOMWARE IST EINE IT-BEDROHUNG

So wie Plünderer inmitten eines Massenchaos die Großbildfernseher der Läden ausräumen, nutzen Cyberkriminelle größere Störungen aus - und machen Unternehmen zu Geiseln, wenn sie am verwundbarsten sind.

Sind Sie darauf vorbereitet? Viele sind es nicht.

Konfrontiert mit einer ganzen Palette von Gefahren - von COVID-19 über massive Waldbrände bis hin zu Hochwasser oder Wirbelstürmen und einfach nur unzufriedenen Mitarbeitern - erleben Unternehmen immer häufiger Systemausfälle.

Die Schwere und Häufigkeit von Ransomware-Angriffen wird zunehmen

Im Jahr 2019 fielen laut der CyberEdge Group 78% der Unternehmen wie das Ihre einem erfolgreichen Ransomware-Angriff zum Opfer. Wir erwarten, dass die Heftigkeit dieser Angriffe zunehmen wird. Warum?

Organisationen gehen beim Datenschutz und bei der Datensicherheit oft nur bruchstückhaft vor. Und im Zuge einer hastigen Umstrukturierung weisen fragmentierte Umgebungen, die über Jahre hinweg zusammengefügt wurden, Schwächen auf. Hinzu kommt, dass jeder Remote-Computer zu einem neuen Rechenzentrum wird, das Sie schützen müssen. Und unbeaufsichtigte Rechner, die von Mitarbeitern an entfernten Standorten einfach offen gelassen werden, werden zu bevorzugten Zielen für Cryptomining. Inmitten des Chaos und der Verwirrung bleiben fortgeschrittene Datensicherheit, Backup und Disaster Recovery (DR) oft auf der Strecke.

Die Lücken werden immer größer.

Und wenn es etwas gibt, dessen Sie sich sicher sein können, dann ist es dies: Cyberkriminelle werden die Chance in den Schwachstellen Ihres Unternehmens nutzen. Sie werden Ihren Schaden vervielfachen - und davon profitieren.

Die Wahrscheinlichkeit, dass Menschen auf die Tricks von Cyberkriminellen hereinfallen, ist größer denn je

Die Willensstärke der Menschen wird naturgemäß im Laufe des Arbeitstages immer geringer, sagt Dr. Kathleen Vohs. Und im Angesicht von Katastrophen - natürlichen, von Menschen verursachten oder digitalen - sind sie ausgelaugt. Sie sind emotionell. Ihre “Immunantwort” auf Phishing-Angriffe und Drive-by-Downloads wird zunehmend schwächer.

Auf der Suche nach entscheidenden Informationen und motiviert durch Nächstenliebe öffnen sie Dateien, klicken auf Links und übertragen Daten und Geld, was sie unter normalen Umständen vermieden hätten.

Ihre Arbeit war noch nie so heikel wie heute.

RANSOMWARE-ANGRIFFE WERDEN IHRE GEWINNE REDUZIEREN.

Die Verbraucher, getrieben vom Wunsch nach sofortiger Bedürfnisbefriedigung, wickeln ihre Geschäfte zunehmend online ab. Aber sie sind misstrauisch. Tatsächlich gaben fast drei Viertel der von uns befragten Verbraucher an, sie seien nicht der Meinung, dass Unternehmen ihre Daten angemessen schützen.

Diese Bedenken werden ihre Geschäfte zu Ihnen - oder Ihrer Konkurrenz - treiben

Wenn es um Unternehmen geht, die Daten nicht schützen können - sind die Verbraucher unversöhnlich

93%

prüfen, ob Ihr Unternehmen oder Ihre Website vertrauenswürdig ist , bevor Sie sich mit Ihnen Geschäfte machen.

39%

nennen Sicherheitsbedenken als den einzigen Grund, warum sie mit einem Unternehmen keine Geschäfte gemacht haben.

59%

werden wahrscheinlich vermeiden, Geschäfte mit Ihnen zu machen, wenn Sie einen Cyberangriff im vergangenen Jahr hatten.

45%

werden keine Geschäfte mit Ihnen machen, wenn Sie in den letzten drei Jahren von Cyberkriminellen angegriffen wurden.

Das beweist, negative Erinnerungen bleiben bestehen.

Sie können Ransomware-Angriffe nicht vertuschen - nicht mehr

Es gab eine Zeit, in der Unternehmen das Lösegeld zahlten und einen Cyberangriff verborgen halten konnten. Das ist nicht mehr der Fall. Cyberkriminelle machen nun Übergriffe öffentlich - selbst wenn Lösegeld gezahlt wurde.

Wenn man bedenkt, wie wichtig Vertrauen und Datensicherheit für die Präferenzen der Verbraucher sind, sollte Sie sich selbst fragen:

Tun Sie Ihr Möglichstes, um sich ihre Loyalität zu verdienen?

WENN IHRE DIENSTLEISTUNGEN OFFLINE SIND - WERDEN IHRE KUNDEN DIE GESCHÄFTE WOANDERS HIN VERLAGERN

Wenn es in Ihrem Unternehmen zu Ausfallzeiten kommt, die mit Lösegeldforderungen in Zusammenhang stehen, müssen Sie davon ausgehen, dass jeder vierte Ihrer Kunden weg ist. Denn in der heutigen On-Demand-Wirtschaft fühlt sich eine einzige Serviceunterbrechung, eine fehlgeschlagene Transaktion oder ein Fall von unzugänglichen Ressourcen wie eine Ewigkeit an.

Es ist diese Intoleranz gegenüber Serviceunterbrechungen, die wohl die verheerendste Auswirkung von Ransoware ist, die wir in unserer Umfrage aufgedeckt haben. Und die Nachwirkungen reichen weit über die unmittelbaren Folgen eines Angriffs hinaus.

Verbraucher werden Service-Unterbrechungen im Zusammenhang mit Ransomware nicht tolerieren

58%

wechseln zu einem Konkurrenten, wenn sie zwei oder weniger Störungen erleben.

28%

werden direkt nach der ersten Unterbrechung gehen.

46%

werden ihre Bank oder Sicherheitsdienste nach einer einzigen Unterbrechung verlassen.

45%

verlassen ein Einzelhandelsunternehmen nach einer einzigen Unterbrechung.

43%

werden sich nach einer einzigen Unterbrechung von ihren Kommunikations- und Versicherungsanbietern abwenden.

Verbraucher werden nicht darauf warten bis Sie sich von Ihrem Ransomwareangriff erholen.

Nach einem Cyberangriff stoppen viele Organisationen den Betrieb, indem sie Systeme und Anwendungen offline nehmen, während sie den Schaden bewerten und Backup-Daten wiederherstellen. Aber für viele Verbraucher ist gerade Zeit ein Faktor von entscheidender Bedeutung

37%

werden zu einem Wettbewerber wechseln, wenn Ihre Systeme und Anwendungen nicht innerhalb von 24 Stunden wieder online sind.

41%

werden gehen, wenn sie nicht innerhalb von zwei bis drei Tagen auf Systeme und Anwendungen zugreifen können.

49%

werden zu einem Konkurrenten wechseln, wenn ihre Bank- oder Sicherheitsdienste und Anwendungen nicht innerhalb von 24 Stunden wieder online sind.

45%

werden ihr Kommunikationsprodukt oder ihren Kommunikationsanbieter wechseln, wenn sie nicht innerhalb von 24 Stunden Zugang haben.

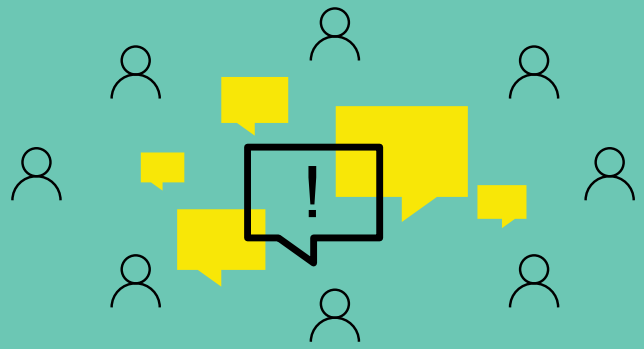
16%

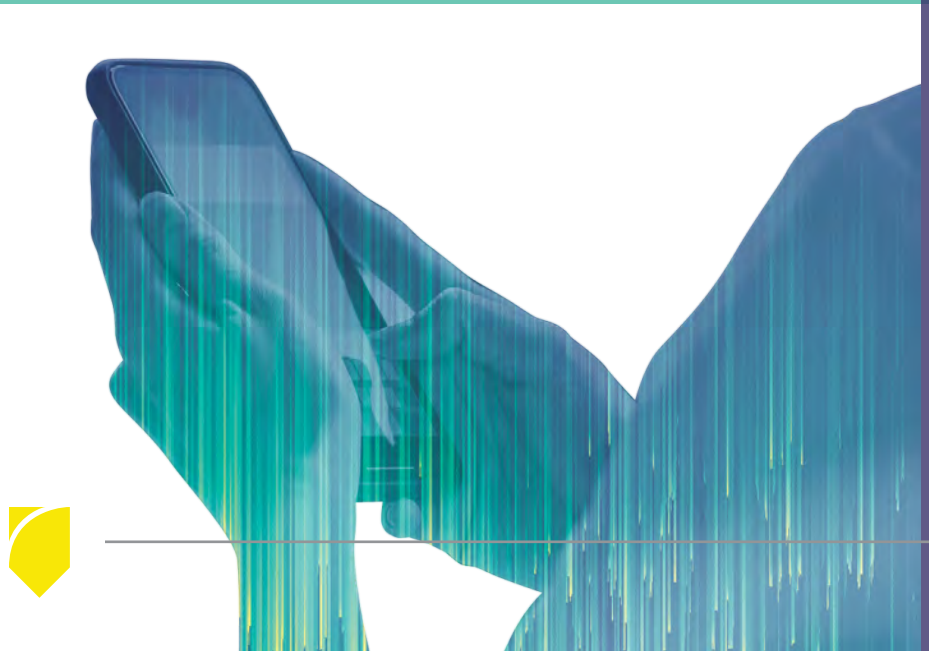
werden ihre Bank- oder Sicherheitsdienste sofort kündigen.

VERBRAUCHER SCHEUEN SICH NICHT, IHRER FRUSTRATION AUSDRUCK ZU VERLEIHEN

Die Nachwirkungen von Cyberattacken werden Sie wahrscheinlich schockieren. Tatsächlich hat die Mehrheit der Verbraucher ihre früheren Erfahrungen mit Ransomware mit Familie, Freunden und Kollegen geteilt - und ein Viertel hat diese Erfahrungen online verbreitet.

Kurz gesagt, ein unzufriedener Verbraucher ist auch ein lautstarker Verbraucher. Wenn Sie also einem Cyberangriff zum Opfer fallen, bereiten Sie sich auf eine Flut von schlechten Nachrichten vor.





Verbraucher äußern sich lautstark über ihre Ransomware-bezogenen Erfahrungen

45%

haben negative Erfahrungen mit Familie, Freunden oder Kollegen geteilt.

25%

haben ihre Erfahrungen in einem Gemeinschaftsforum, Blog oder auf einer Website veröffentlicht.

24%

haben Erfahrungen per E-Mail ausgetauscht.

23%

haben negative Online-Rezensionen veröffentlicht oder Erfahrungen in sozialen Medien ausgetauscht.

Tieni pronta la macchina delle pubbliche relazioni

28%

werden Sie als weniger vertrauenswürdig und zuverlässig ansehen.

24%

werden denken, dass Sie nicht genug für die Sicherheit ausgeben.

17%

werden glauben, dass Sie inkompetent sind – mehr um Ihre Profite als um die Sicherheit der Kunden besorgt.

DER SCHUTZ VON VERBRAUCHERDATEN VOR RANSOMWARE KANN IHREN GEWINN STEIGERN

Cyberangriffe lasten schwer auf den Verbrauchem, wenn sie Kaufentscheidungen treffen. Aber unsere Umfrage ergab einige gute Nachrichten - der Schutz vor Ransomware ist eine Chance für Unternehmen. Tatsächlich wären mehr als vier von zehn Verbrauchern bereit, mehr für Produkte und Dienstleistungen zu bezahlen, wenn sie glauben, dass Sie ihre Daten zuverlässig schützen können. Und in einigen Branchen, wie dem Bank- und Finanzdienstleistungssektor, steigt diese Zahl auf fünf von zehn.

Könnten Sie für Ihre Produkte und Dienstleistungen tatsächlich mehr verlangen?

43%

würden mehr ausgeben – im Allgemeinen – für Produkte und Dienstleistungen von einem Unternehmen das sie für zuverlässiger und sicherer halten.

51%

würden mehr für Bank- und Sicherheitsdienste bezahlen.

44%

würden bei Anbietern für Kommunikation, Datenspeicherung und Public-Clouds mehr bezahlen.

39%

würden mehr bei Mediendiensten, Bildung und Transportorganisationen zahlen .

43%

würden mehr für behördliche Dienste beisteuern.

45%

würden mehr für Gesundheits- und Versicherungsdienstleistungen ausgeben.

42%

würden mehr für Versorgungsunternehmen zahlen.

41%

würden mehr für Einkäufe im Einzelhandel bezahlen.

VERKÜPFEN SIE RANSOMWARE- UND DATENSCHUTZ UM DEN GEWINN IHRES UNTERNEHMENS ZU STEIGERN

Sie spüren den Druck. Sie wissen, dass Sie für den Schutz des Herzblutes Ihrer Organisation - ihrer Daten - verantwortlich sind, und Sie wissen, dass Sie nicht optimal aufgestellt sind. Wie helfen Sie den Entscheidungsträgern, über den reinen Anschaffungspreis für Daten- und Ransomware-Schutz hinwegzublicken und stattdessen den Wert für das Unternehmen zu berücksichtigen?

Helfen Sie den Entscheidungsträgern, sich ein kristallklares Bild vom Ransomwarerisiko für Ihr Unternehmen zu machen..
Informieren Sie sie darüber, dass Cyberkriminelle im vergangenen Jahr 78% der Organisationen erfolgreich mit Lösegeldforderungen bedroht haben - und zeigen Sie aktuelle Beispiele aus der Branche auf, um eine überzeugende Geschichte zu erzählen (siehe rechter Kasten).

Halten Sie sich von technischen Details fern und konzentrieren Sie sich stattdessen auf die unmittelbaren Auswirkungen auf die Geschäftskontinuität.
Erklären Sie, was Ihr Unternehmen verliert, wenn es für eine Minute, eine Stunde, einen Tag oder eine Woche ausfällt. Informieren Sie über die Auswirkungen auf das Geschäftsergebnis, wie z. B. potenzielle Lösegeldforderungen, verlorene Daten und Einnahmen, unerwünschte Berichterstattung, Bußgelder und unproduktive Zeiten von Mitarbeitern.

Zeichnen Sie ein Bild von den unmittelbaren und langfristigen Auswirkungen von Ransomware auf die Loyalität und Kaufentscheidungen der Verbraucher.
Berechnen Sie z. B. die Auswirkungen auf den Gewinn Ihres Unternehmens, wenn 28 % Ihrer Kunden nach einer einzigen Unterbrechung im Zusammenhang mit Ransomware der Firma den Rücken kehren würden.

Zeigen Sie, dass der Schutz vor Ransomware ein Wettbewerbsvorteil sein kann.
Die Verbraucher schätzen die Sicherheit ihrer Daten. Stellen Sie sicher, dass die Entscheidungsträger verstehen, dass sie auch bereit sind, mehr zu zahlen, wenn Sie ihnen ein beruhigendes Gefühl vermitteln können.

Begeistern Sie die Entscheidungsträger für die Marke, nicht für das Produkt.
Die meisten interessieren sich nicht für Funktionen und technische Spezifikationen. Was sie jedoch interessiert, ist die Reputation einer Marke.

Teilen Sie unseren Ein-Seiter: “Glauben Sie, dass Ihre Verbraucher eine Ransomware-Angriff verzeihen werden?„
Dieser Überblick liefert die dringend benötigte Perspektive, die für das Kalkül Ihrer Entscheidungsträger entscheidend ist.

Beginnen Sie das Gespräch mit Ihrem IT-Direktor oder Ihrem CIO.
Wenn Sie sich frühzeitig einen technisch versierten Fürsprecher ins Boot holen, haben Sie einen Verbündeten, der Ihnen helfen kann, das Gespräch von den Investitionskosten auf den Wert für Ihr Unternehmen zu verlagern.

Vorfälle wie diese können dazu beitragen, die Notwendigkeit dringender Maßnahmen hervorzuheben.

Munson Healthcare

Als 29 Mitarbeiter dieser Gesundheitsorganisation im Norden Michigans einer Phishing-Kampagne zum Opfer fielen, verschafften sich Cyberkriminelle zweieinhalb Monate lang still und leise Zugang zu Patientendaten - einschließlich Behandlungsinformationen, Bankdaten und Sozialversicherungsnummern.

Travelex

Nach einem REvil-Angriff verlangten die Cyberkriminellen nicht nur 6 Mio. USD von dem britischen Finanzinstitut, sondern behaupteten auch, sie hätten die persönlichen Daten und Kreditkartendaten der Verbraucher. Unter dem Vorwand einer “geplanten Wartung” nahm Travelex seine IT-Systeme und Websites für mehr als drei Wochen vom Netz.

MGM Resorts International

Ransomware-Angreifer verschafften sich Zugang zum Cloud-Server der Hotelkette und zu den persönlichen Daten von mehr als 10 Millionen ihrer Gäste - darunter Popsänger Justin Bieber und Twitter -CEO Jack Dorsey.

ARCSERVE LÖSUNGEN - SECURED BY SOPHOS

Sie wissen, dass Ihre Kunden ransomwarebedingte Ausfallzeiten oder Datensicherheitsverletzungen nicht tolerieren werden. Also, entscheiden Sie sich für Arcserve.

Durch den Einsatz vollständig integrierter Sophos Technologien bieten wir Ihnen umfassenden Schutz vor Cyberangriffen, großen Katastrophen, menschlichem Versagen und anderen ungeplanten Ausfällen. Vertrauen Sie den Spezialisten - nutzen Sie die einzige bewährte Lösung, die von Herstellern mit zusammengenommen über 70 Jahren Erfahrung entwickelt wurde.

- Erreichen Sie eine schnellere IT-Resilienz, indem Sie das Jonglieren mit mehreren Anbietern, SLAs und Support-Teams eliminieren.
- Erhalten Sie umfassenden SaaS-basierten, standortbasierten und Cloud-Datenschutz von einem Anbieter mit einheitlichen Backup-, Cybersicherheits-, DR- und Cloud-Diensten
- Halten Sie den Betrieb aufrecht und erfüllen Sie SLAs mit sofortiger VM- und Bare-Metal-Wiederherstellung (BMR), lokalem und remotem Virtual Standby, anwendungskonsistenter Sicherung und granularer Wiederherstellung, Unterstützung von Hardware-Snapshots und Erweiterungen für Hochverfügbarkeit und Bandunterstützung.
- Stellen Sie sicher, dass Sie bei Ausfällen vor Ort keine Sekunde verlieren - mit virtuellem Remote-Standby für Notfall-Failover und Failback in die Cloud, manuell ausgelöstem Failover auf Remote-Ressourcen und sofortiger VM-Wiederherstellung
- Beseitigen Sie Kopfschmerzen durch absichtliches oder unabsichtliches Löschen, programmtechnische Probleme, externe Sicherheitsbedrohungen - Aspekte, die von Microsoft nicht abgedeckt werden - mit vollständigem Datenschutz für Exchange Online, OneDrive for Business und SharePoint Online
- Erkennen Sie bekannte und unbekannte Malware, ohne sich auf Signaturen verlassen zu müssen, dank des vollständig integrierten Sophos Intercept X Advanced mit modernsten Technologien für Deep Learning (KI)
- Verhindern Sie die wichtigsten Hacking Techniken, inklusive Credential Harvesting, Lateral Movement, und Privilege Escalation mittels Exploit Prävention
- Stoppen Sie Ransomware-Angriffe auf Backup-Daten mit CryptoGuard und Master-Boot-Record-Angriffe mit WipeGuard
- Stellen Sie mit AES-Verschlüsselung und rollenbasierter Zugangskontrolle sicher, dass die Compliance-Anforderungen erfüllt werden
- Halten Sie mit dem Datenwachstum Schritt, indem Sie den Speicherbedarf Drastisch reduzieren, durch die integrierte globale Deduplizierung, die bis zu 20-mal mehr Speicherplatz freigibt.

BRAUCHEN SIE UNTERSTÜTZUNG?

Zählen Sie auf Arcserve. Wir stehen immer bereit, die Ärmel hochzukrempeln und zu helfen..

arcserve®

+49 699 675 9111
arcserve.com/de