

CLOUDASHUR®

Der Schlüssel zu Ihren Daten

VERSCHLÜSSELN

Um den ultimativen Schutz Ihrer in der Cloud gespeicherten Daten auf Ihrem lokalen PC/MAC oder jedem anderen Speichergerät sicherzustellen

TEILEN

Sie Ihre verschlüsselten Daten mit autorisierten Benutzern in der Cloud sowie per E-Mail und über Datenübertragungsdienste in Echtzeit

VERWALTEN

und überwachen Sie Ihre cloudAshur-Geräte zentral

Für den Datenschutz ist die Datenverschlüsselung wichtig, der Schutz des Verschlüsselungsschlüssels ist entscheidend. Für eine wirklich sichere Lösung muss der Verschlüsselungsschlüssel unbedingt getrennt von den Daten gespeichert werden.

Aus diesem Grund haben wir das cloudAshur-Hardwaresicherheitsmodul entwickelt (Patent ausstehend), ein Sicherheitsmodul mit Hardwareverschlüsselung und PIN-Authentifizierung, das allen übertragenen und gespeicherten Daten mit einem FIPS-zertifizierten, zufällig erzeugten Verschlüsselungsschlüssel mit AES-256-Bit-Verschlüsselung verschlüsselt, dies ist in einem sicheren Mikroprozessor nach Common Criteria EAL5 + (Hardware Zertifizierter) gespeichert

Übersicht

cloudAshur ist die perfekte Lösung für alle, die Daten sicher in der Cloud speichern, teilen, verwalten und überwachen möchten. cloudAshur beseitigt die Sicherheitsanfälligkeiten von Cloudplattformen wie mangelnde Kontrolle und unbefugter Zugriff. Hacker entwickeln zahlreiche ausgefeilte Methoden, um arglose und anfällige Benutzer anzugreifen. Menschliches Versagen ist bei Datenleckvorfällen ebenfalls häufig anzutreffen.

Das Hacking eines Cloudkontos kann den Diebstahl und Verlust vertraulicher Daten zur Folge haben, was potenziell zum Verlust des Arbeitsplatzes, zu negativer Publizität, hohen Geldbußen und zum Untergang eines Unternehmens führen kann.

iStorage-Softwaresuite



cloudAshur-Client-App (Windows und macOS)

cloudAshur ist mit sowohl PCs als auch MACs kompatibel und funktioniert mit zahlreichen Cloud-Anbietern wie Amazon Drive, Google Drive, OneDrive, Dropbox, iCloud und vielen mehr.



cloudAshur-KeyWriter-App (Windows)

iStorage KeyWriter (Patent ausstehend) macht die gemeinsame Nutzung verschlüsselter Daten in der Cloud sowie per E-Mail und über Datenübertragungsdienste (z. B. WeTransfer) zwischen autorisierten Benutzern, mit ultimativer Sicherheit und Gelassenheit, zum Kinderspiel und ermöglicht den Benutzern, Daten unabhängig von ihrem Standort sicher und in Echtzeit gemeinsam zu nutzen.



cloudAshur-Remote-Management-App (Windows)

Die Konsole iStorage cloudAshur Remote Management gibt Ihnen die vollkommene Kontrolle über alle cloudAshur-Hardwaresicherheitsmodule, die in Ihrem Unternehmen eingesetzt werden, und bietet eine breite Palette an Funktionen zur Verwaltung und Überwachung aller Benutzer.



WICHTIGSTE FUNKTIONEN DES CLOUDASHUR-VERSCHLÜSSELUNGSMODULS

Cloud-Verschlüsselungsmodul mit PIN-Authentifizierung und Hardwareverschlüsselung (Patente ausstehend)

Ultrasichere 7- bis 15-stellige PIN zur Authentifizierung des cloudAshur-Moduls

Crypto-Chip im Gerät

AES-XTS- oder AES-ECB-256-Bit-Hardwareverschlüsselung der Militärklasse mit gemäß FIPS PUB 197 zertifizierter USB-3.0-Verschlüsselungssteuerung in 100 % Echtzeit.

Abwehrmechanismus gegen Brute-Force-Hacker-Angriffe

Wenn die Benutzer-PIN 10 Mal hintereinander falsch eingegeben wird, wird die Benutzer-PIN gelöscht und es kann ausschließlich durch Eingabe der Admin-PIN auf das Laufwerk zugegriffen werden, um die Benutzer-PIN zurückzusetzen. (Der Administrator kann dies von der 10-maligen falschen Standard-PIN-Eingabe auf 1 - 9, nur für den Benutzer, ändern)

Wenn die Admin-PIN 10 Mal hintereinander falsch eingegeben wird, gehen alle PINs und der verschlüsselte Verschlüsselungsschlüssel für immer verloren.

Fünffaktorauthentifizierung

Was Sie haben:

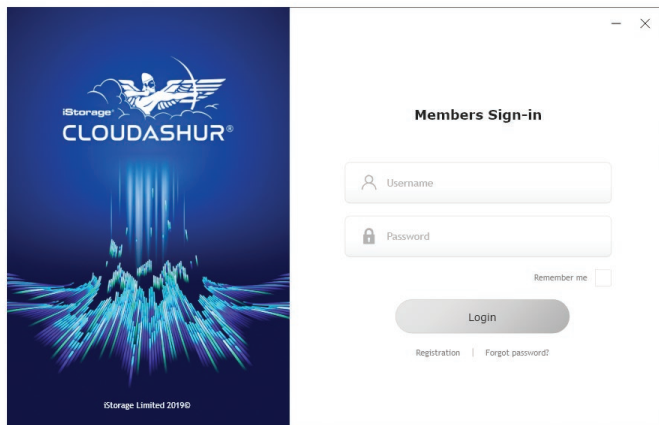
1. Das cloudAshur-Hardwaresicherheitsmodul.

Was Sie wissen:

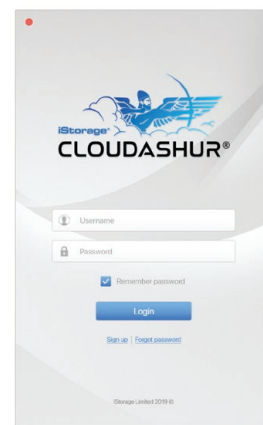
2. 7- bis 15-stellige, vom Administrator/Benutzer konfigurierbare PIN
3. Benutzername und Kennwort für die Client-App iStorage cloudAshur Windows oder macOS
4. Wo die Daten gespeichert werden, welcher Cloudanbieter
5. Benutzername und Kennwort für das Cloudkonto

Kompatibel mit Windows und macOS

Die cloudAshur-Clientanwendungen sind kompatibel mit Windows (7/8/10) und macOS (Sierra/High Sierra/Catalina).



(Windows-Client-App)



(macOS-Client-App)

Zwei Verschlüsselungsmodi

cloudAshur kann in zwei Verschlüsselungsmodi konfiguriert werden: AES-ECB 256-Bit (FIPS-konform) und AES-XTS 256-Bit.

Manipulationssicheres und sicherheitsverpacktes Design gemäß FIPS 140-2 Ebene 3

Alle kritischen Komponenten im cloudAshur-Gehäuse sind von einer äußerst strapazierfähigen Epoxidharzschicht überzogen. Diese lässt sich praktisch nicht entfernen, ohne dass die kritischen Komponenten irreversiblen Schaden nehmen.

Bei Verletzungen bietet das sicherheitsverpackte Design der cloudAshur-Module den sichtbaren Nachweis einer eingetretenen Manipulation.

Enthält ein Common Criteria EAL5+ (Hardware Zertifizierter) sicherer Mikroprozessor

der u. a. mit folgenden Funktionen ultimative Sicherheit vor Hackern bietet, Manipulationen erkennt und darauf reagiert:

- Spezielle Hardware zum Schutz vor SPA-/DPA-/SEMA-, DEMA-Angriffen
- Erweiterter Schutz vor physischen Angriffen, u. a. Active Shield, Enhance-Protection-Object, CStack-Checker, Slope-Detector und Paritätsfehler
- Umgebungsschutzsystem für Spannungsüberwachung, Frequenzüberwachung, Temperaturüberwachung und Lichtschutz
- Sicheres Speichermanagement/Zugriffsschutz

WICHTIGSTE FUNKTIONEN DES CLOUDASHUR-VERSCHLÜSSELUNGSMODULS (Fortsetzung)

Polymerbeschichtete, verschleißfeste alphanumerische On-board-Tastatur

cloudAshur ist authentifiziert (entsperrt) und alle Funktionen werden mit der On-board-Tastatur unter null Hostbeteiligung ausgeführt. cloudAshur ist weder für Keylogger noch für Brute-Force-Angriffe anfällig.

Die cloudAshur-Tastatur ist für zusätzlichen Schutz mit einer verschleißfesten Polymerschicht überzogen.

Whitelisting in Netzwerken

Konfiguriert mit einer eindeutigen VID/PID und interner/ externer Seriennummer mit Barcode, was die einfache Integration in Standard-End-Point-Managementsoftware (Whitelisting) ermöglicht, um die internen Unternehmensanforderungen zu erfüllen.

Benutzer-PIN-Registrierung

Der Administrator kann eine Beschränkungsrichtlinie für die Benutzer-PIN einrichten. Dies umfasst die Festlegung der Mindestlänge der PIN sowie die Anforderung, ein oder mehrere „Sonderzeichen“ einzugeben.

Funktionen „Sonderzeichen“ wie „UMSCHALTASTE (↑) +-Zeichen“

Automatische Sperre bei Inaktivität

Zum Sperren nach Ablauf einer voreingestellten Zeit der Inaktivität konfigurierbar. cloudAshur sperrt automatisch, wenn keine Verbindung zum Hostcomputer oder keine Stromversorgung mehr zum USB-Anschluss besteht.

Immun gegen Bad-USB

Sowohl in den USB-Cryptochip als auch in den sicheren Mikroprozessor ist ein digital signierter Speicherstick-Sperrmechanismus integriert, der cloudAshur gegen Bad-USB immunisiert.

Anpassungs-Services verfügbar

Mit einem In-House-Service für PIN-Konfiguration und Laserätzen kann die cloudAshur-Hülle oder die Seite des Moduls mit Ihrem Namen, Unternehmensnamen und/ oder Logo, Ihrer Web-/E-Mail-Adresse, Telefonnummer personalisiert werden.

IP68-zertifiziert

Staub- und wasserresistent Einschließlich harter eloxierter und robuster Schutzhülle aus stranggepresstem Aluminium.

Separate Admin- und Benutzermodie

Unterstützt unabhängige Admin- und Benutzer-PINs

Selbsterstörungsfunktion

Programmieren Sie cloudAshur mit einer Selbsterstörungs-PIN, nach deren Eingabe der verschlüsselte Verschlüsselungsschlüssel und alle PINs gelöscht werden.

Einmalige Benutzer-PIN zur Wiederherstellung

Der Administrator kann cloudAshur mit einer einmaligen Wiederherstellungs-PIN programmieren. Das ist äußerst nützlich, wenn ein Benutzer die PIN zur Authentifizierung des cloudAshur vergessen hat.

Diese Funktion ermöglicht dem Benutzer, die Wiederherstellungs-PIN einzugeben und eine neue Benutzer-PIN zu konfigurieren.



CLOUDASHUR KEYWRITER (PATENT AUSSTEHEND)

Macht die gemeinsame Nutzung von Daten in der Cloud per E-Mail und über Datenübertragungsdienste zwischen autorisierten Benutzern, mit ultimativer Sicherheit und Gelassenheit, zum Kinderspiel!



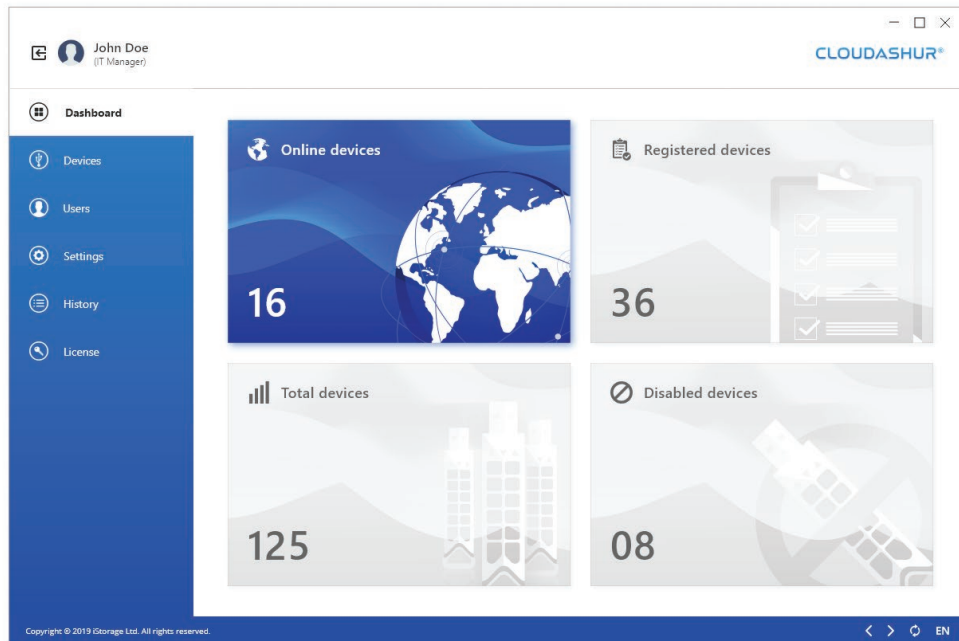
KEYWRITER-FUNKTIONEN

- iStorage KeyWriter kopiert unter Verwendung eines im Handel erhältlichen USB-Hubs alle kritischen Sicherheitsparameter einschließlich des zufällig erzeugten Verschlüsselungsschlüssels und alle PINs zwischen dem cloudAshur-Mastermodul und so vielen sekundären cloudAshur-Modulen wie benötigt. Dies ermöglicht den autorisierten Benutzern, Daten in Echtzeit und unabhängig von ihrem Standort gemeinsam zu nutzen.
- Die kritischen Sicherheitsparameter verlassen zu keiner Zeit das cloudAshur-Modul und werden im sicheren, Common Criteria EAL5+ (Hardware Zertifizierter), sicherer Mikroprozessor gespeichert.
- Der Prozess des Kopierens des verschlüsselten Verschlüsselungsschlüssels und aller kritischen Anmeldedaten zwischen dem cloudAshur-Mastermodul und den sekundären cloudAshur-Modulen ist durch ein sicheres Protokoll geschützt, das in den sicheren iStorage-cloudAshur-Microcontroller integriert ist. Das Protokoll ist unter Verwendung FIPS-zertifizierter kryptografischer Algorithmen integriert. Jedes cloudAshur verfügt über ein eindeutiges Zertifikat, das von einem vertrauenswürdigen Stamm ausgegeben ist. Hierdurch wird sichergestellt, dass während des Schlüsselaustauschprozesses ausschließlich iStorage-cloudAshur-Module verwendet werden können.
- Der erstellte Sitzungsschlüssel wird von den cloudAshur-Modulen beim Ausführen des sicheren Protokolls niemals ausgegeben und die kopierten sensiblen Daten werden ausschließlich im validierten cloudAshur-Empfängermodul entschlüsselt. Die auf dem PC ausgeführte iStorage-KeyWriter-Software koordiniert die aufgrund des sicheren Protokolls erforderlichen Abläufe. Jedoch sind weder der Sitzungsschlüssel noch die entschlüsselten Daten in der Software sichtbar, wodurch Hackern verunmöglicht wird, auf im cloudAshur-Modul gespeicherte Sicherheitsparameter zuzugreifen oder diese abzurufen.

iStorage KeyWriter ist kompatibel mit Windows (Vista/7/8/10).

CLOUDASHUR-REMOTE-MANAGEMENT-KONSOLE

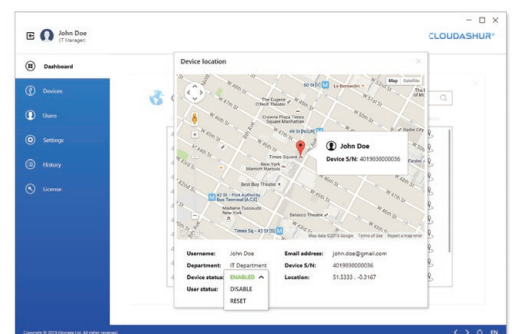
Gibt Ihnen die volle Kontrolle über alle cloudAshur-Hardwaresicherheitsmodule, die in Ihrem Unternehmen eingesetzt werden, und bietet eine breite Palette an Funktionen zur Verwaltung aller Benutzer.



KONSOLENFUNKTIONEN

Die iStorage-Remote-Management-Konsole gibt dem Administrator vollständige Sichtbarkeit und Kontrolle für Folgendes:

- cloudAshur-Module von Benutzern vorübergehend deaktivieren oder zurücksetzen (Remote-Kill) - bei verdächtigen Aktivitäten oder wenn Mitarbeiter aus dem Unternehmen ausscheiden, ohne ihr cloudAshur-Verschlüsselungsmodul zurückzugeben.
- Dateitypen beschränken – steuern Sie, welche Dateitypen hochgeladen und in der Cloud gemeinsam genutzt werden (EXE, PNG, PDF usw.)
- Benutzerprotokolldateien anzeigen – vollständige Sichtbarkeit dessen, was die einzelnen Benutzer in der Cloud tun, z. B., welche Dateien sie hoch- und herunterladen, ändern usw.
- Benutzerstandort anzeigen – Sie können den Standort der Benutzer der cloudAshur-Module mit einer Bildschirmskarte anzeigen.
- Geofencing und Timefencing - beschränken Sie die Zeit und den Standort, wann und wo das cloudAshur-Verschlüsselungsmodul von den einzelnen Benutzern verwendet werden kann.




Die iStorage-Remote-Management-Konsole ist kompatibel mit Windows (Vista/7/8/10).

WARUM CLOUDASHUR?

- Sie halten den Verschlüsselungsschlüssel für Ihre Daten in der sichersten möglichen Weise - Sie müssen nicht mehr befürchten, dass Ihre Daten in der Cloud angezeigt, gestohlen und weitergegeben werden.
- Fünffaktoraufentifizierung - macht es praktisch unmöglich, Ihre Daten zu hacken.
- DSGVO-konform – Die Geschäftsbedingungen großer Cloudanbieter enthalten eine Klausel zur „Haftungsbeschränkung“, durch die die Haftung für die Datensicherheit in der Cloud auf den Benutzer/Kunden übergeht, auch wenn die Daten auf den Servern der Anbieter gespeichert sind. AWS beispielsweise gibt in seinen AGB an, dass AWS keinerlei Haftung übernimmt, „wenn bei Ihren Inhalten oder sonstigen Daten ein unbefugter Zugriff, eine Veränderung, Löschung, Vernichtung, Beschädigung, ein Verlust oder eine Nicht-Speicherung eintritt“. cloudAshur gibt Ihnen ultimativen Schutz: Wenn ein Hacker Zugriff auf Ihr Cloudkonto erlangt, ist er nicht in der Lage, Ihre Daten zu entschlüsseln.
- Wenn es einem Hacker gelingt, durch „Phishing“ oder andere, hochentwickelte Methoden in den Besitz Ihrer Cloud-Anmeldedaten zu gelangen, ist er nicht in der Lage, Ihre Daten zu entschlüsseln.
- Menschliches Versagen ist kein Problem mehr.
- Schutz vor bei Cloudanbietern beschäftigtem Administrationspersonal, das die Möglichkeit hat, auf Ihre Daten zuzugreifen, da es die Kontrolle über die Verschlüsselungsschlüssel hat.
- Schutz vor Datenschutzproblemen. Google, Microsoft und andere Unternehmen erhalten jedes Jahr Abertausende an Anfragen von Behörden. Diese Unternehmen übergeben in einem Großteil der Fälle zumindest einige Daten, wenn auch nicht den vollständigen Inhalt...

Technische Daten

Hardware	Hardware Sicherheitsmodul (Patent ausstehend)
Schnittstelle	Nach FIPS PUB 197 zertifizierte USB-3.0-Verschlüsselungssteuerung
Batterie	Wiederaufladbare Li-Polymerbatterie mit 3,7 V
Abmessungen - H/B/T	87,40 mm/19,40 mm/13,40 mm
Gewicht	Ohne Hülle: Ungef. 28 Gramm Mit Hülle: Ungef. 37 Gramm
Kompatibilität	cloudAshur ist mit sowohl PCs als auch MACs kompatibel und funktioniert mit zahlreichen Cloud-Anbietern wie Amazon Drive, Google Drive, OneDrive, Dropbox, iCloud und vielen mehr.
Hardwaredatenverschlüsselung	Kann in zwei Verschlüsselungsmodi konfiguriert werden: AES-ECB 256-Bit (FIPS-konform) und AES-XTS 256-Bit.
Zertifizierungen	FIPS 140-2 Ebene 3, NLNCSA BSPA und NATO Beschränkte Ebene (ausstehend, Q3/Q4)
Zulassungen	
Bestellinformationen	IS-EM-CA-256
Garantie	3 Jahre Garantie mit kostenlosem lebenslangem technischem Support



Entworfen und entwickelt in Großbritannien
Montiert in China

