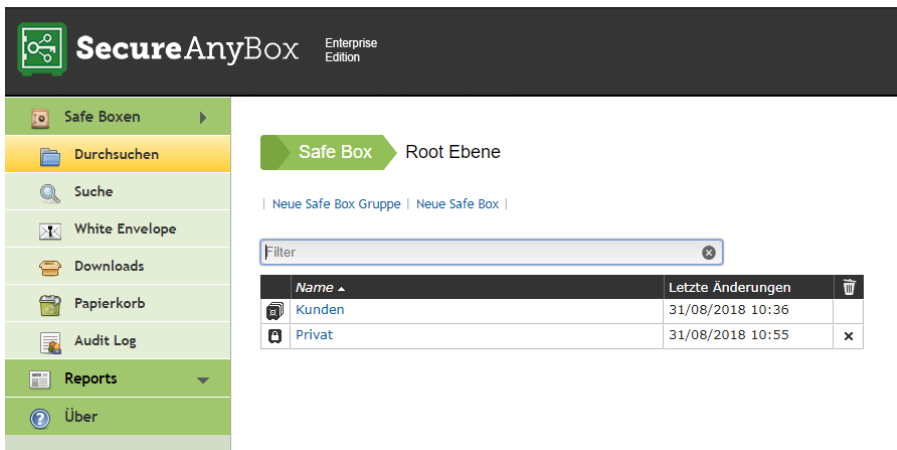


# SecureAnyBox

## Sicherheit und Kontrolle beim Teilen und Verwalten von Daten und Passwörtern

Speichern Sie Ihre Passwörter, Dokumente, Tabellen und Dateien sicher in Safeboxes in SecureAnyBox. So können die Mitarbeiter Ihrer Firma, Abteilung oder Organisation intern und in Zusammenarbeit mit externen Nutzern wie Partnern, Lieferanten und Kunden einfach und sicher auf sensible Daten zugreifen. SecureAnyBox ermöglicht es den Nutzern überall ein einzigartiges und sicheres Passwort zu haben. Diese Passwörter werden generiert und in privaten oder geteilten SafeBoxes geschützt.



### Komplexe Sicherheit

SecureAnyBox nutzt eine einzigartige Kombination verschiedener Berechtigungs- und Verschlüsselungsmechanismen zum Schutz der Inhalte.

### Einfache Handhabung

SecureAnyBox leitet den Nutzer intuitiv. Installation, Konfiguration und Implementation von SecureAnyBox gestalten sich wirklich einfach. Ein Administrator kann Strukturen vorgeben. Der Nutzer kann entscheiden mit wem er Inhalte teilt.

### Aufzeichnung des Datenzugriffes

Der Zugriff auf die gespeicherten Daten wird aufgezeichnet, wodurch feststellbar bleibt wer, wann auf die Daten zugegriffen hat.



## Lösung

Security & Identity

## Produkt

SecureAnyBox

## Highlights

Active Directory und eDirectory Unterstützung

Zwei-Faktor-Authentifizierung

Passwort-Audit

LDAP Benutzermanagement

Sicherung lokaler Windowskonten

# Komplettlösung zur Sicherung lokaler Windowskonten

## Jeden Tag ein anderes Passwort für jeden Firmencomputer

Windows-Arbeitsstationen, die von einem Image bereitgestellt wurden, verfügen normalerweise über dieselben lokalen Konten und Kennwörter wie die ursprüngliche Installation, die für die Image-Generierung verwendet wurden. Mit einem leicht zu merkenden, einheitlichen Kennwort erleichtert ein lokales Administratorkonto Ihrer IT-Abteilung das Leben, während der Sicherheitschef die letzten Spuren seiner Haare verliert - lokale Konten sind eine Sicherheitslücke, insbesondere auf eigenständigen PCs und Notebooks Ihrer Benutzer, Sie befinden sich außerhalb der Mauern Ihres Büros.

SecureAnyBox benötigt keine Verbindung zum Server, um ein eindeutiges und sicheres Tagespasswort für jedes lokale Konto auf allen Ihren Windows-Computern zu verwalten. Privilegierte Administratoren können das Arbeitsstationskennwort des Tages erhalten, wenn sie sich beim Server authentifizieren, und den Namen der Arbeitsstation eingeben. Das System eignet sich hervorragend für Standalone-Boxen / Laptops sowie als Ergänzung zu Endpoint-Sicherheitssystemen.



## Lösung

Security & Identity

## Produkt

SecureAnyBox

# Passwort Audit

Der Passwort-Audit Report zeigt alle Einträge, auf welche der angemeldete Benutzer Zugriff hat an und zeigt zusätzlich die ermittelten Werte für Passwort-Entropie, benötigte Zeit, um das Passwort zu knacken und Warnungen für Passwörter welche Duplikate sind.

Nach der Eingabe des Access Codes überprüft SecureAnyBox alle Einträge, welche mit dem Access Code entschlüsselt werden können, und ermittelt die Ergebnisse für den Report.

Zur Ermittlung der Entropie und der anderen Werte verwendet SecureAnyBox den Passwortprüfer nbvcxz. Der Passwortprüfer wurde durch Passwort-Cracker inspiriert.

Die Schätzung der Stärke eines Passwortes wird ermittelt, indem das Passwort verschiedene Algorithmen durchläuft und durch Prüfen auf Übereinstimmung, von Teilen des Passwortes, mit Wort-Listen (mit Fuzzy Matching), gebräuchliche Daten, Jahreszahlen, Anordnungsmustern, sich wiederholende Zeichen, sich wiederholende Zeichenketten und Buchstabenfolgen.

Jeder von diesen Prüfinhalten stellt eine Art und Weise dar, wie Angreifer versuchen Passwörter zu knacken.

## Highlights

Active Directory und eDirectory Unterstützung

Zwei-Faktor-Authentifizierung

Passwort-Audit

LDAP Benutzermanagement

Sicherung lokaler Windowskonten

Name	Passwort Entro...	Zeit um das Passwort o...	Zeit um das Passwort of...	Duplizität	Letzte Passwortän...	Zeit seit Änderung
Management	62.51			1.50		
Business-Abteilung	60.29					
Finanzabteilung	64.73			2.00		
ERP admin login	64.73	infinite (>100000 centuries)	infinite (>100000 centuries)	2	04/06/2018 10:52	
ERP back-ups	64.73	infinite (>100000 centuries)	infinite (>100000 centuries)	2	01/06/2018 16:29	2 days
Marketing	57.19					
Technisch	59.94					
Server CMCK	60.29					
Server TDP	62.36					
MODE 1	60.29	infinite (>100000 centuries)	infinite (>100000 centuries)		01/06/2018 16:29	2 days
LDAP server	64.43	infinite (>100000 centuries)	infinite (>100000 centuries)		01/06/2018 16:29	2 days
Testserver	57.35					

## DSGVO-konform

Die DSGVO hat grundsätzlich zwei Anforderungen – keine personenbezogenen Daten zu erfassen und gegen den Willen oder ohne Zustimmung der Eigentümer zu speichern und wenn wir solche Daten speichern, diese zu schützen, so dass sie nicht in falsche Hände gelangen.

Obwohl bereits viele Lösungen zur Sicherheit und Kontrolle beim Teilen und Verwalten von Daten und Passwörtern existieren, gibt es nach wie vor viele erfolgreiche Angriffe auf IT-Systeme und Anmeldedaten werden missbraucht. Wie kann das sein?

**Warum also bieten bereits existierende Lösungen zur Sicherheit und Kontrolle beim Teilen und Verwalten von Daten und Passwörtern oftmals keinen ausreichenden Schutz?**

Viele Nutzer verwenden dieselben Zugangsdaten für verschiedene Dienste. Angriffe erfolgen oft aufgrund gleichlautender Zugangsdaten und diese Angriffe sind meist nicht leicht zu entdecken. Ein Angreifer kann z.B. einen Web Dienst erstellen um seine Opfer zur Registrierung für Rabatte, Schnäppchen, Gewinnspiele usw. zu bringen. Dann muss er nur noch ausprobieren, wo die erhaltenen Logindaten noch funktionieren. Zu leicht vergessen wir das Prinzip des Passwortes – beide Seiten kennen es. Ein Server, der einen Nutzer authentifizieren kann, kennt das Passwort. Deshalb ist es gefährlich, dasselbe Passwort mehr als einmal zu nutzen.

Das menschliche Gehirn funktioniert ziemlich perfekt. Doch mehr als zehn Passwörter können wir uns meist nicht merken. Außerdem benutzen viele Menschen ein System, um Passwörter zu erstellen, die leichter merkbar sind. Das Problem dieser meist einfachen Systeme ist, dass sie von einem Angreifer herausgefunden werden können.



### Lösung

Security & Identity

### Produkt

SecureAnyBox

### Highlights

Active Directory und  
eDirectory  
Unterstützung

Zwei-Faktor-  
Authentifizierung

Passwort-Audit

LDAP  
Benutzermanagement

Sicherung lokaler  
Windowskonten