edv-buchversand.de

iolo System Mechanic

Für alle Funktionen / Produkte

Schritt für Schritt erklärt

Inhalt

Sollte Ihnen dieses FAQ eine Frage nicht beantworten können, stehen wir Ihnen gerne persönlich zur Verfügung. Schreiben Sie uns eine E-Mail an hallo@edv-buchversand.de oder kontaktieren Sie uns telefonisch:

0 21 91 - 99 11 88

(Mo.-Fr.: 9:30 – 17:00 Uhr)

Ihr Team vom edv-buchversand.de

Wofür brauche ich IOLO System Mechanic?

System Mechanic ist ein System-Utility, mit dem sich Windows tunen und von überflüssigem Datenmüll befreien lässt. Es hilft, Datenmüll von der Festplatte zu entfernen, grundsätzliche und kleinere Reparaturen vorzunehmen, die Registry aufzuräumen, sowie eine allgemeine Wartung von Windows nach einem vorgegebenen Zeitplan automatisch vorzunehmen.

In welchen Versionen ist System Mechanic verfügbar?

Neben dem bekannten System Mechanic stellt IOLO noch folgende Produkte zur Verfügung:

- IOLO System Mechanic Professional
- IOLO System Mechanic Ultimate Defense

Was sind die genauen Unterschiede zwischen den drei Produkten?

Funktionen	**System Mechanic**	**System Mechanic Professional**	**System Mechanic Ultimate Defense**
Optimieren der PC-Leistung	✔	✔	✔
Schutz der Online-Privatsphäre			✔
Sichere Verwaltung von Passwörtern			✔
Entfernen von Malware			✔
Blockieren von Malware		✔	✔
Löschen kompletter Laufwerke		✔	✔
Wiederherstellung gelöschter Dateien		✔	✔

Wo genau kann ich das Produkt herunterladen?

Nach erfolgreicher Bestellung stellen wir Ihnen den Link zum Download in Ihrem Kundenkonto zur Verfügung. Dort finden Sie parallel auch Ihre neue Seriennummer. Alternativ können Sie auch folgenden Link verwenden:

- IOLO SystemMechanic Standard
- IOLO SystemMechanic Professional
- IOLO SystemMechanic Ultimate Defense

Systemvoraussetzungen

Welche Systemvoraussetzungen muss mein PC erfüllen?

Für die Installation von IOLO System Mechanic sollte Ihr PC folgende Voraussetzungen erfüllen:

- Windows 10, 8, 8.1 oder 7
- Mindestens 512 MB RAM (optimal sind 2 GB)
- 270 MB freier Festplattenspeicher
- Internetverbindung (zur Lizenzaktivierung erforderlich)
- Windows Administrator-Benutzerkonto

Auf wie vielen Computern kann System Mechanic installiert werden?

Seit System Mechanic 11 vereinfacht iolo technologies auf radikale Weise die herkömmliche Art der Software-Lizenzierung. Installieren Sie die neueste Version auf allen in Ihrem Privathaushalt vorhandenen (und nicht gewerblich genutzten) PCs. Sie benötigen nur eine einzige Lizenz! Das Ganze nennt sich "Whole Home"-Lizenz.

Ist System Mechanic auch auf Mac-Rechnern verwendbar?

Bis jetzt ist System Mechanic ein reines PC-Produkt und speziell für Windows angepasst. Für ein Macbook Pro Dual System mit Windows-Umgebung übernehmen wir weder Verantwortung noch den Support.

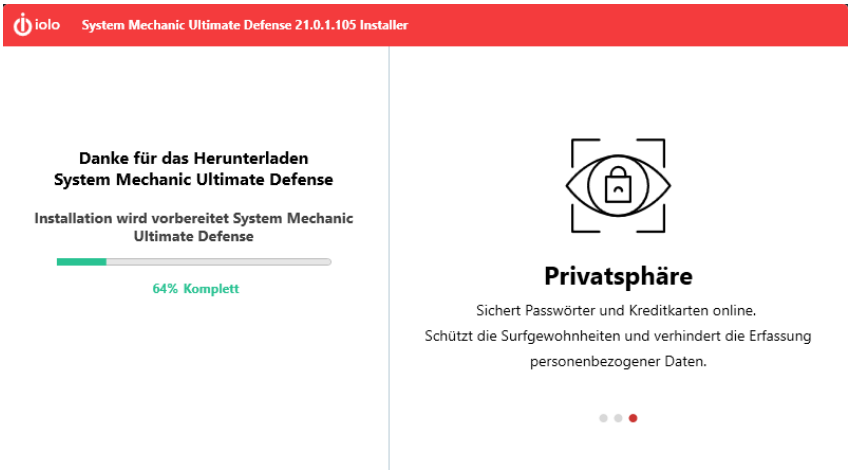
Ist System Mechanic auch zu 64-bit Rechnern kompatibel?

Die aktuelle System Mechanic-Version ist zu allen 64-bit Versionen von Windows 7, Windows 8/8.1 und Windows 10 kompatibel und einsetzbar.

System Mechanic installieren

1. Deinstallieren Sie alle bisherigen Versionen von System Mechanic, die Sie installiert haben.
2. Vergewissern Sie sich, dass Sie mit dem Internet verbunden sind.
3. Laden Sie sich die Installationsdatei aus Ihrem Account namens **„Mein Konto“** herunter und öffnen Sie die heruntergeladene EXE-Datei. Der Installationsassistent wird automatisch geöffnet. Bestätigen Sie nun den Button *„Jetzt installieren“*, um zu starten.

Der Installer lädt nun im Hintergrund die benötigten Dateien herunter und installiert dies automatisch auf Ihrem System

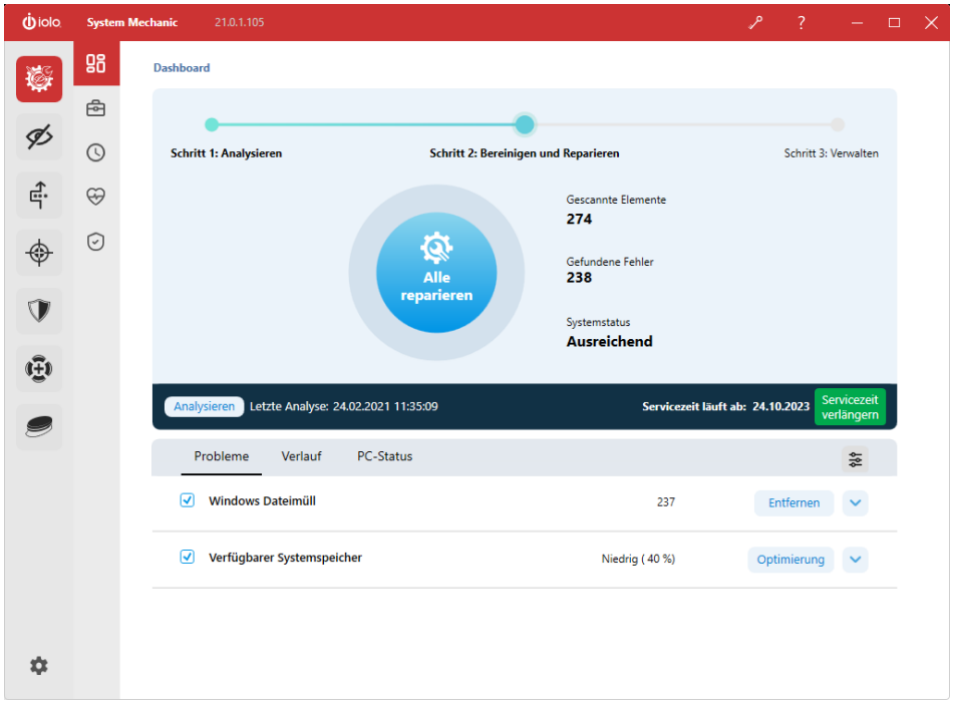


4. Nach erfolgreicher Installation startet das Programm automatisch.

System Mechanic wird nach der Installation normalerweise sofort ausgeführt und bietet Ihnen die Möglichkeit zur ersten Analyse an. Klicken Sie auf die Schaltfläche *„Analysieren“* im Dialogfeld, um fortzufahren.

Klicken Sie nach Abschluss der Analyse auf die blaue Schaltfläche *„Jetzt aktivieren“*, um Ihr Produkt mit Ihrer E-Mail-Adresse und danach mit dem Aktivierungsschlüssel freizuschalten.

Es stehen Ihnen nun alle Funktionen von IOLO System Mechanic (hier Ultimate Defense) zur Verfügung.



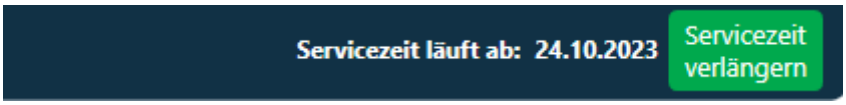
Gängige Fehler beim Eingeben der Lizenzinformationen:

- Leerzeichen im Aktivierungsschlüssel sind nicht zulässig.
- Vergewissern Sie sich, dass Sie Lizenzinformationen für das jeweilige Produkt eingeben, das Sie verwenden. Die Lizenzinformationen für IOLO-Produkte sind nicht mit anderen IOLO-Produkten kompatibel.

- Falls Ihre Lizenzinformationen weiterhin als falsch oder ungültig zurückgewiesen werden, überprüfen Sie, ob Sie die Informationen exakt wie gezeigt eingegeben haben.
- Manche Zeichen (z. B. die Ziffer 0 und der Buchstabe O) sehen sich sehr ähnlich. Überprüfen Sie Folgendes: Die Buchstaben O, l (kleines L), I (großes i) und die Ziffern 0 (null) und 1 (eins).

Wie kann ich feststellen, wie lange mein Produkt noch gültig ist?

Die Servicezeit wird Ihnen direkt auf der Startseite im sogenannten „Dashboard“ angezeigt. Dort finden Sie auch zusätzlich einen Button, um die Servicezeit bei Bedarf zu verlängern.



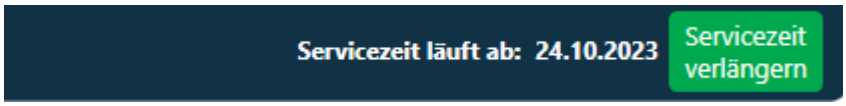
Ich habe eine Testversion installiert. Kann ich diese mit einem erworbenen Aktivierungsschlüssel in eine Vollversion freischalten?

Ja! Im geöffneten Dashboard finden Sie in der oberen roten Leiste ein „Schlüsselsymbol  “.
Hinter diesem Symbol befindet sich der Button „Produktinformationen“. Im dem nun geöffneten Fenster haben Sie die Möglichkeit, im obersten Feld Ihre Seriennummer einzugeben.

Wie kann ich IOLO System Mechanic verlängern?

Es gibt mehrere Möglichkeiten Ihr Programm zu verlängern.

1. **Direkt über die im Programm enthaltene Verlängerungsfunktion:**
   Auf der Startseite des Programms finden Sie die direkte Möglichkeit zur Verlängerung.



Sie werden direkt auf die Verlängerungsseite weitergeleitet, wo Sie dann die neue Laufzeit auswählen können. IOLO System Mechanic und IOLO System Mechanic Pro können maximal um 2 Jahre verlängert werden. Bei IOLO System Mechanic Ulimate Defense ist dies nur maximal 1 Jahr möglich. Die Eingabe eines neuen Lizenzschlüssels ist nicht erforderlich, da der vorhandene Lizenzschlüssel um die neue Laufzeit verlängert wird. Bei Ultimate Defense erhalten Sie allerdings einen neuen Schlüssel, den Sie über das Schlüsselsymbol, in der roten Leiste am oberen Rand des Fensters, registrieren können.

2. **Direkt über die Webseite:**

Unter folgenden Links können Sie direkt über unsere Website die Verlängerung bestellen:

- IOLO SystemMechanic Standard
- IOLO SystemMechanic Professional
- IOLO SystemMechanic Ultimate Defense

Bei der Standard- & Professional-Version tragen Sie zuerst Ihren vorhandenen Lizenzschlüssel ein.

Danach haben Sie die Möglichkeit, die gewünschte Laufzeit auszuwählen und führen den Bestellprozess dann fort. Bei Ultimate Defense erhalten Sie allerdings einen neuen Schlüssel, den Sie über das Schlüsselsymbol, in der roten Leiste am oberen Rand des Fensters, registrieren können.

System Mechanic Ultimate Defense

Welche Programmteile sind in IOLO System Mechanic Ultimate Defense enthalten und welche Funktionen beinhalten sie?

System Mechanic stellt alle Tools bereit, die notwendig sind, damit sich Ihr PC stets im optimalen Zustand befindet. Sie können Probleme beheben, den Computer bereinigen, die Leistung steigern, Abstürze reduzieren und mehr.

Privacy Guardian ist ein Feature zum Online-Schutz der Privatsphäre in System Mechanic Ultimate Defense. Es hilft dabei, den Zugang zu Ihren sensiblen Daten, Geräteinformationen und Gewohnheiten im Internet zu blockieren. So können Sie Ihr digitales Privatleben schützen – mit automatisiertem Löschen von Cookies, Deaktivierung der Windows-Datenerfassung und einer anonymen Suchfunktion.

Malware Killer ist eine einzigartige Malware-Erkennungssoftware und verwendet Scan Cloud-basierte Scans und Analysen, unterstützt von einem sorgfältig entwickelten heuristischen Algorithmus, um die Erkennungszeit für brandneue Ausbrüche drastisch zu reduzieren. Durch diese Methode ist Malware Killer in der Lage, seine riesige „Reputationsdatenbank“ ständig auszubauen und auch vorher unbekannte Bedrohungen zu erkennen.

Andere marktübliche Malware-Entfernungstools sind dazu nicht in der Lage. Diese Tools überwachen zwar das Verhalten verdächtiger Dateien, sind jedoch oft ungeschickt oder zu aggressiv und entfernen versehentlich harmlose Dateien, die wichtig für die Benutzer sind.

System Shield schützt Ihren Computer vor vielen verschiedenen Arten von Malware. Die Software wird automatisch mit neuen Virendefinitionen aktualisiert, um Sie vor den neuesten Bedrohungen zu schützen. System Shield scannt Ihr System außerdem auf vorhandene Bedrohungen durch Malware.

Mit **DriveScrubber** können Sie jedes Byte an Daten von einem angegebenen Laufwerk, inklusive Wechselmedien wie tragbare Laufwerke oder Flash-Laufwerke, löschen. Außerdem erlaubt Ihnen die Software, ein Boot-Medium zu erstellen und alle Daten vom Systemlaufwerk, inklusive des Betriebssystems, zu löschen.

Mit **Search and Recover** können Sie viele Arten von verlorenen Dateien wiederherstellen, indem Sie ein Laufwerk Ihrer Wahl durchsuchen.

ByePass ist eine Browsererweiterung, die Ihre Passwörter auf all Ihren Geräten plattformunabhängig verwaltet. ByePass enthält eine universelle Remote-Abmeldefunktion namens „Login Guardian“, mit der Sie sich von überall bei allen Websites abmelden können. ByePass schützt außerdem Ihre Onlinekäufe, indem Sie Kreditkarten verschlüsselt speichern und anschließend nur für Onlinekäufe verwenden können, um sie vor Hackern und Keyloggern zu verbergen. Mit einer ähnlichen lokalen Verschlüsselungsoption für Notizen können Sie sensible Daten wie PINs sicher speichern.

Was ist ActiveCare?

Was ist ActiveCare und welche Funktionen sind enthalten?

ActiveCare überwacht wichtige Kennzahlen für die PC-Leistung und führt benötigte Reparaturen automatisch aus. Es arbeitet unbeaufsichtigt im Hintergrund, wenn Ihr PC eingeschaltet ist aber nicht verwendet wird, und führt nur bei Bedarf Aktionen aus. Wenn Sie während der ActiveCare-Verarbeitung an Ihren PC zurückkehren, können Sie den Vorgang entweder abbrechen oder fortsetzen.

Folgende Funktionen können aktiviert werden:

On-Demand Boost
Entscheiden Sie, ob unnötige Hintergrunddienste automatisch beendet werden sollen, indem Sie den On-Demand Boost aktivieren, wenn ActiveCare ausgeführt wird.

Registrierungsprobleme bereinigen und reparieren
Entfernen Sie unnötige und ungültige Einträge, um die allgemeine Effizienz und Stabilität des Computers zu verbessern.

Unnötige oder gefährliche Startprogramme eliminieren
Diese Einstellung sucht nach nicht-kritischen Anwendungen, die zusammen mit Ihrem PC gestartet werden und den Startvorgang oder die allgemeine Systemgeschwindigkeit beeinträchtigen. ActiveCare erstellt automatisch eine Liste dieser Programme, und Sie können diese Liste bei jeder Systemanalyse überprüfen.

Systemlaufwerk defragmentieren
Defragmentieren Sie Ihre Festplatten regelmäßig, um verstreute Dateifragmente zu konsolidieren, Programmstart und Dateizugriff zu beschleunigen und die allgemeine Geschwindigkeit und Stabilität des Systems zu verbessern.

Internet-Junk-Dateien bereinigen
Bereinigen Sie regelmäßig Ihren Browsercache, Cookies und andere Arten von Internet-Junk, um freien Speicherplatz auf der Festplatte zu schaffen, Ihr System zu beschleunigen und Ihre Privatsphäre zu schützen. Klicken Sie auf den Pfeil „nach unten“ rechts neben der

Umschaltfläche, um auszuwählen, welche Arten von Internet-Junk regelmäßig bereinigt werden.

Windows-Junk-Dateien bereinigen
Bei der regelmäßigen Nutzung Ihres Computers sammeln sich temporäre Dateien und andere unnötige Daten an. Wir empfehlen, diese unnötigen Systemdaten regelmäßig zu löschen, um freien Speicherplatz auf der Festplatte zu schaffen und die Systemgeschwindigkeit zu verbessern. Klicken Sie auf den Pfeil „nach unten“ rechts neben der Umschaltfläche, um auszuwählen, welche Dateitypen von ActiveCare regelmäßig bereinigt werden.

Was ist LiveBoost – Echtzeit-Boost?

Der Echtzeit-Boost umfasst verschiedene automatische Echtzeit-Tuningfunktionen:

- **OptiCore** und **PowerSense** optimieren Ihre Prozessoreinstellungen für die jeweilige Aufgabe.
- **RAMJet** gibt reservierten Arbeitsspeicher von Apps frei, die ihn nicht mehr benötigen.
- **AcceleWrite** beschleunigt die E/A-Vorgänge der Laufwerke, indem Daten in fortlaufenden Batches auf die Festplatten geschrieben werden, um Fragmentierung vorzubeugen.

Was ist Privacy Guardian?

Was bewirkt der Schutz der Online-Privatsphäre von Privacy Guardian?

Privacy Guardian ist eine Desktop-Software, die bei jeder Nutzung des Internets den Zugriff auf Ihre sensiblen Online-Daten, auf Geräteinformationen und auf Ihre Surfgewohnheiten blockiert. Die Desktop-App bietet eine Übersichtsseite, über die Sie Ihre Privacy Guardian-Einstellungen verwalten können und auf der alle Versuche Sie zu verfolgen, an einer zentralen Stelle angezeigt werden.
Privacy Guardian verhindert, dass Online-Werber Sie im Internet verfolgen und erlaubt Ihnen, sich im Internet anonym zu bewegen und private Suchvorgänge durchzuführen. Noch wichtiger aber ist, dass Privacy Guardian dafür sorgt, dass Dritte keine persönlichen

Informationen, die auf Ihrem Standort, Ihrem Suchverlauf und Ihren Einkaufsgewohnheiten basieren, gewinnen können.

Bin ich nicht geschützt, wenn ich häufig meine Browser-Cookies lösche?

Privacy Guardian erlaubt Ihnen zwar, die Löschung von Cookies und des Browsercache für mehrere Webbrowser aus dem Dashboard heraus automatisch zu planen und festzulegen, jedoch ist das Löschen von Internet-Cookies nicht ausreichend, um Ihre Privatsphäre wirklich zu schützen.

Was, neben Cookies, beeinträchtigt denn noch meine Online-Privatsphäre?

Die meisten Softwareprodukte zum Schutz der Online-Privatsphäre sind nur in der Lage, Cookie-basiertes Tracking (Nachverfolgung) zu blockieren. Dabei handelt es sich um eine in die Jahre kommende und bald schon veraltete Technik, die Online-Entitäten dazu verwenden, um Ihnen Werbung anzuzeigen, die für Sie interessant erscheint. Eine weitaus größere und ständig wachsende Bedrohung für Ihre Privatsphäre ist allerdings der digitale "Fingerabdruck".

Aktuell bietet nur Privacy Guardian einen Schutz vor Entitäten, die Ihren digitalen Fingerabdruck – eine neue und hochentwickelte Technik zur Sammlung persönlicher Daten – erfassen. Dabei werden Informationen gewonnen, die spezifisch für Ihren Computer sind und sehr persönliche Details über Ihre Identität beinhalten. Dazu gehören Informationen über:

- geografische Lokation
- durchgeführte Online-Suchen
- angesehene Videos
- besuchte Webseiten
- Urlaubsgewohnheiten
- Interesse an Medikamenten
- Fahrzeugkäufe
- Einkommen und Schulden
- Familienstatus, Kinder
- und vieles mehr

Warum ist Privacy Guardian gegenüber herkömmlicher Datenschutz-Software die bessere Wahl?

Während weniger weit entwickelte Cookie-basierte Tracking-Blocker sich nur auf Werbung konzentrieren, konzentriert sich Privacy Guardian auf das Fingerabdruck-basierte Tracking und sucht nach den spezifischen Verhaltensweisen bekannter Fingerabdruck-Skripte und macht die Daten, die zur Ausspähung sensibler Informationen notwendig sind, unbrauchbar. Tracking/Nachverfolgungsversuche erkennt Privacy Guardian unabhängig davon, ob Anzeigen mit Tracking-Cookies auf einer Website existieren oder nicht. Benutzer von Privacy Guardian werden jedes Mal darüber informiert, wenn versucht wurde/wird sie online zu verfolgen – auch wenn gar keine Werbung sichtbar ist. Außerdem kann das einfache Blockieren von Cookies auch dazu führen, dass „legitime“ Inhalte unterdrückt und ausgeblendet werden.

Wie können die (ohne Privacy Guardian) aus meinem digitalen Fingerabdruck gesammelten Infos gegen mich verwendet werden?

Hier sind nur einige der Möglichkeiten, wie ein Ausspähen Ihres digitalen Fingerabdruckes Sie beeinflussen, Ihnen Unannehmlichkeiten bereiten oder sich auf Ihr Leben auswirken kann:

- Online-Werbung verfolgt Sie
- Sie sehen auf allen Webseiten, die Sie besuchen, die gleichen lästigen Werbeanzeigen.
- Sie erhalten nervende Spam-E-Mails von Onlinehändlern.
- Ihre Daten stehen zum Verkauf
- Ihr Internetprovider könnte in die Lage versetzt werden, Ihre persönlichen Daten an Internethändler weiterzuverkaufen.
- Personalisierte Preisgestaltung
- Onlinehändler identifizieren Sie anhand Ihrer Postleitzahl und passen die Preise – z.B. wenn Sie in einer teureren Nachbarschaft wohnen – nach oben an (mit diesem Konzept arbeiten aktuell speziell Hotels und Fluggesellschaften)
- Rufschädigung
- Über Ihre Einkäufe und Einkaufsgewohnheiten gesammelte Daten könnten dazu führen, dass Sie als kreditunwürdig eingestuft werden.

Würde ein virtuelles privates Netzwerk (VPN) meine Privatsphäre nicht schützen?

Im Allgemeinen ja, jedoch haben VPNs mehrere Nachteile: Ein VPN verschlüsselt Ihre Daten und verändert Ihren Datenverkehr so, als käme er von einer anderen IP-Adresse. Das Einbinden eines VPN in den Datenfluss belastet jedoch die CPU-Ressourcen und die Bandbreite. Auch werden VPNs inzwischen von mehr und mehr Webanbietern (z.B. Netflix) blockiert, wenn ein privates Netzwerk erkannt wird. Aus diesen Gründen ist Privacy Guardians proprietäre Methode zur Unterbindung des Fingerabdruck-basierten Trackings auch VPNs überlegen.

Sammelt und überwacht Privacy Guardian meine Daten, um mich zu schützen?

Nein, Privacy Guardian sammelt, speichert, überwacht oder analysiert KEINE Ihrer persönlichen Benutzerdaten. Privacy Guardian verschlüsselt Daten mit einem speziell entwickelten, proprietären „Scrambling“-Algorithmus, um damit die modernen und aggressiven Fingerabdruck-basierten Tracking-Skripte zu täuschen. Dadurch wird verhindert, dass Dritte an sinnvolle Daten gelangen.

Wie unterscheidet Privacy Guardian sich vom „Inkognito“-Modus (anonym/privat Surfen) meines Web-Browsers?

Privacy Guardian arbeitet auch beim Surfen im Inkognito-Modus perfekt und unterbindet Tracking-Versuche, die der Inkognito-Modus eventuell nicht abdeckt. Der Inkognito-Modus verhindert die lokale Speicherung von Browsing-Daten, so dass Elemente wie z.B. Cookies, der Suchverlauf und Autofill-Informationen nicht gespeichert werden. Der Inkognito-Modus verhindert allerdings nicht, dass Tracking-Skripte geladen werden, die Datensammler dann dazu einsetzen, um Ihren digitalen Fingerabdruck zu erstellen. Bei diesem „Fingerprinting“ wird, durch das Sammeln unzähliger Metriken aus dem Web-Browser des Benutzers, ein detailliertes Profil erstellt – ein Prozess, der auch durch anonymes Surfen im Inkognito-Modus des Browsers nicht unterbunden werden kann.
Aktivieren Sie einmal zum Test Privacy Guardian beim Surfen im Inkognito-Modus und überzeugen Sie sich selbst, wie viele Tracking-Versuche dabei von Privacy Guardian noch erkannt werden.

Wie beeinflusst Privacy Guardian meine Internetverbindung?

Privacy Guardian ist keine Software zur Optimierung. Sie erhöht den Schutz Ihrer Privatsphäre und die Surfgeschwindigkeit kann – vor allem beim Surfen auf besonders „aufdringlichen“ Webseiten – durch den für Ihren Schutz notwendigen und erforderlichen Aufwand zur Verschlüsselung Ihrer Daten, eventuell auch sinken. Webseiten mit hohem und invasiven Tracking zwingen Privacy Guardian zu einer stärkeren Verschlüsselung, die potenziell auch Auswirkungen auf die Internetgeschwindigkeit hat. Ein „Whitelisting“ (die Aufnahme in einer Ausnahmeliste) vertrauenswürdiger Seiten kann helfen, eine Verlangsamung zu vermeiden.

Was ist ByePass?

ByePass ist eine Browsererweiterung, die Ihre Passwörter auf all Ihren Geräten plattformunabhängig verwaltet. ByePass enthält eine universelle Remote-Abmeldefunktion namens „Login Guardian“, mit der Sie sich von überall bei allen Websites abmelden können.

ByePass schützt außerdem Ihre Onlinekäufe, indem Sie Kreditkarten verschlüsselt speichern und anschließend nur für Onlinekäufe verwenden können, um sie vor Hackern und Keyloggern zu verbergen.

Mit einer ähnlichen lokalen Verschlüsselungsoption für Notizen können Sie sensible Daten wie PINs sicher speichern.

Welche Vorteile bietet ByePass?

- Unbegrenzter Passwortspeicher
- Intelligente Autofill-Funktion
- Vergessen Sie nie wieder ein Passwort
- Sicherer Passwortgenerator
- Automatische Synchronisierung und Sicherung auf all Ihren Geräten
- Browserverlauf aus der Ferne löschen
- Remote-Abmeldung bei allen Websites von überall mit Login Guardian
- Schützen Sie Ihre Kreditkarten
- Erstellen Sie sichere Notizen, z. B. für PINs
- Auch für Android-Mobilgeräte verfügbar

Was sind die ByePass-Systemanforderungen?

ByePass ist eine sichere Webbrowser-Erweiterung, die mit den meisten Betriebssystemen kompatibel ist, auf denen die neueste Version von Google Chrome, Firefox, Safari und Edge ausgeführt wird. ByePass ist auch für Android- und iOS-Mobilgeräte verfügbar.

Kann ich ByePass in Chrome, Firefox und Safari unter Mac OS verwenden?

Ja. ByePass installiert dasselbe auf der ByePass-Aktivierungsseite in Chrome-, Firefox- und Safari-Browsern unter Mac OS. Eine gültige und aktive ByePass- oder System Mechanic Ultimate Defense-Lizenz ist erforderlich. (Wenn Sie über eine aktive Phoenix 360-Lizenz verfügen, erhalten Sie automatisch System Mechanic Ultimate Defense, wenn Sie Ihr Produkt nach der Veröffentlichung aktualisieren.) Funktioniert auch in Brave, einem Chromium-basierten Browser.

Was sind „Konten“ im Zusammenhang mit der Verwendung von ByePass?

Konten beziehen sich auf separate Anmeldeinformationen für die verschiedenen von Ihnen verwendeten Websites. Sie werden lokal verschlüsselt und in ByePass gespeichert, so dass Sie sie niemals unsicher in Ihrem Webbrowser speichern, aufschreiben oder speichern müssen. Beispiele für „Konten“ im ByePass-Kontext sind Ihre Benutzernamen und Kennwörter für die Anmeldung bei: Facebook, Twitter, Google Mail, Instagram, Online-Banking, Nachrichtenseiten usw

Wie kann ich Passwörter generieren und sicher speichern?

Nach der ersten Anmeldung bei ByePass wird eine Liste mit Vorschlägen für Konten angezeigt, die Sie hinzufügen können. Klicken Sie auf eines der vorgeschlagenen Konten für Facebook, Twitter, Google oder PayPal, um die Anmeldeinformationen zu ByePass hinzuzufügen. ByePass kann für jedes dieser Anmeldekonten ein sicheres Passwort für Sie generieren.

Was sind sichere Notizen?

Neben Passwörtern können Sie mit ByePass auch Notizen verschlüsselt speichern, so dass sie niemand zu Gesicht bekommt.

Meldet mich die Login Guardian-Funktion aus der Ferne nur aus den Sites ab, die ich in ByePass eingerichtet habe?

Ja. Bedenken Sie, dass ByePass die Sites, die Sie besuchen und bei denen Sie sich anmelden, immer automatisch zur sicheren Datenbank hinzufügt. Auf diese Weise werden Sie davor geschützt, versehentlich bei einer Site angemeldet zu bleiben, wenn Sie die Login Guardian-Funktion für die Remote-Abmeldung verwenden.

Wie kann ich mein ByePass-Konto schließen?

Im ByePass-Dashboard:

- Klicken Sie auf die rote Menüleiste, um das Dropdownmenü zu öffnen.
- Klicken Sie auf Einstellungen.
- Scrollen Sie zum letzten Eintrag, Konto schließen, der ausgegraut angezeigt wird.
- Klicken Sie auf Ja.

Was ist DriveScrubber?

Mit DriveScrubber können Sie jedes Byte an Daten von einem angegebenen Laufwerk löschen, inklusive Wechselmedien wie tragbare Laufwerke oder Flash-Laufwerke. Mit DriveScrubber können Sie außerdem ein Boot-Medium erstellen und alle Daten vom Systemlaufwerk löschen, inklusive des Betriebssystems.

Wann sollte ich „DriveScrubber“ verwenden?

Das sichere Löschen aller Spuren von Daten auf Ihrer Festplatte ist eine empfohlene Vorgehensweise vor der Entsorgung oder beim Verkauf eines Computers. Die Löschung ist auch hilfreich, wenn Sie ein Laufwerk einem anderen Zweck zuführen oder ein beschädigtes Laufwerk reparieren.

Was ist Malware Killer?

Wenn ein Computer bereits mit Malware infiziert ist, haben Sie mit Malware Killer eine „nukleare“ Option, mit der Sie die Malware finden und auslöschen können. Malware Killer ist die perfekte Ergänzung zum Echtzeitschutz und kann Malware finden und auslöschen, wenn alle anderen Maßnahmen fehlschlagen.

Wann sollte ich den „Malware Killer“ verwenden?

Malware Killer ist eine einzigartige Malware-Erkennungssoftware und verwendet Scan Cloud-basierte Scans und Analysen, unterstützt von einem sorgfältig entwickelten heuristischen Algorithmus, um die Erkennungszeit für brandneue Ausbrüche drastisch zu reduzieren. Durch diese Methode ist Malware Killer in der Lage, seine riesige „Reputationsdatenbank“ ständig auszubauen und auch vorher unbekannte Bedrohungen zu erkennen.

Andere marktübliche Malware-Entfernungstools sind dazu nicht in der Lage. Diese Tools überwachen zwar das Verhalten verdächtiger Dateien, sind jedoch oft ungeschickt oder zu aggressiv und entfernen versehentlich harmlose Dateien, die wichtig für die Benutzer sind.

Was geschieht, wenn eine schädliche Datei gefunden wurde?

Malware Killer schließt den Scan ab und zeigt die Nachricht „Schädliche Objekte gefunden!“ an. Im Dropdownmenü rechts neben den schädlichen Dateien haben Sie verschiedene Optionen zur Auswahl.

Wählen Sie eine der folgenden Optionen aus:

- Dateien in die Quarantäne verschieben
- Dateien löschen
- Dateien von zukünftigen Scans ausschließen
- Dateien als sicher melden

Entscheiden Sie, wie Sie mit den schädlichen Dateien verfahren möchten, und klicken Sie auf Weiter, um den Prozess abzuschließen.

Was ist System Shield?

System Shield schützt Ihren Computer vor vielen verschiedenen Arten von Malware. Die Software wird automatisch mit neuen Virendefinitionen aktualisiert, um Sie vor den neuesten Bedrohungen zu schützen. System Shield scannt Ihr System außerdem auf vorhandene Bedrohungen durch Malware.

Wann sollte ich System Shield verwenden?

Manche Viren und andere bösartige Programme sind in der Lage, den Virenschutz Ihres Betriebssystems zu umgehen. System Shield verwendet den modernen Dual-Engine-Virenschutz, um noch mehr Bedrohungen zu erkennen.

Was ist Search and Recover?

Mit Search and Recover können Sie viele Arten von verlorenen Dateien wiederherstellen, indem Sie ein Laufwerk Ihrer Wahl durchsuchen.

Wann sollte ich „Search and Recover“ nutzen?

Mit Search and Recover können Sie versehentlich gelöschte kritische Daten wiederherstellen, egal ob von einer Festplatte, CD, Digitalkamera, einem MP3-Player oder einem anderen digitalen Gerät.