Acronis Ransomware Protection

Sommario

1 Introduzione 3

1.1 Che cos'è Acronis Ransomware Protection? 3

1.2 Requisiti di sistema 3

1.3 Installazione di Acronis Ransomware Protection 4

1.4 Aggiornamento di Acronis Ransomware Protection 4

1.5 Assistenza tecnica 5

2 Guida rapida 6

2.1 Account Acronis 6

2.2 Introduzione a Acronis Cloud 6

2.2.1 Garanzia della sicurezza dei dati 7

3 Backup dei dati 8

3.1 Backup di file e cartelle 8

3.2 Rimozione dei dati da Acronis Cloud 9

4 Ripristino dei dati 10

4.1 Ripristino di dati da Acronis Cloud 10

4.2 Ripristino di una versione del file 10

5 Acronis Active Protection 11

5.1 Protezione dei dati dell'utente dal ransomware 13

5.2 Gestire Acronis Active Protection 13

6 Acronis Mobile 15

6.1 Installazione di Acronis Mobile 16

6.2 Backup del dispositivo mobile su Acronis Cloud 16

6.3 Ripristino dei dati mobili 16

6.4 Ripristino di dati su un nuovo smartphone 17

6.5 Impostazioni dell'app mobile 17

7 Glossario 20

Copyright © Acronis International GmbH, 2003-2018

1 Introduzione

1.1 Che cos'è Acronis Ransomware Protection?

Acronis Ransomware Protection è una suite software che garantisce la sicurezza delle informazioni presenti sul PC. Riunisce due caratteristiche che si completano a vicenda per garantire una protezione avanzata dei dati personali:

- **Acronis Active Protection**

  Questo servizio protegge il computer dal ransomware, un software dannoso che blocca l'accesso ad alcuni file o all'intero sistema richiedendo un riscatto per lo sblocco. Basata su un approccio euristico, Acronis Active Protection esegue il monitoraggio dei processi in esecuzione sul computer utilizzando la modalità in tempo reale. Al rilevamento di un processo di terze parti che stia cercando di crittografare i file o di inserire del codice dannoso in un processo integro, chiederà di consentire al processo di modificare i file o di arrestarlo. Anche quando i file vengono crittografati da un ransomware, è possibile ripristinarli da copie temporanee. Fare riferimento a Acronis Active Protection (p. 11) per maggiori dettagli.
- **Backup a livello di file in Acronis Cloud:**

  File come documenti, foto, file musicali e file video possono essere protetti dai rischi di danneggiamento o perdita eseguendone il backup nel sicuro Acronis Cloud. Poiché i file sono memorizzati in un archivio remoto, sono protetti anche in caso di smarrimento, furto o danneggiamento del computer. Se necessario, i dati potranno essere completamente ripristinati su un nuovo dispositivo. Le modifiche eseguite nei file protetti vengono automaticamente caricate nell'archivio nel cloud per mantenere in backup sempre aggiornato. Acronis Ransomware Protection offre 5 GB di spazio di archiviazione gratuito nel cloud. Se non dovesse essere sufficiente, l'utente è libero di acquistare altro spazio. Fare riferimento a Backup di file e cartelle (p. 8) per i dettagli.

Acronis Mobile

Quando si dispone di uno spazio di archiviazione su Acronis Cloud, è possibile utilizzarlo per proteggere non solo i dati sul computer, ma anche quelli sui dispositivi mobili. Acronis Mobile è un'applicazione gratuita che consente di eseguire il backup dei dati in Acronis Cloud e di ripristinarli in caso di perdita o danneggiamento sullo stesso dispositivo o su uno diverso. L'applicazione supporta smartphone e tablet con i sistemi operativi iOS o Android. Per ulteriori dettagli, fare riferimento ad Acronis Mobile (p. 15).

Con l'applicazione desktop Acronis True Image o l'applicazione NAS Acronis True Image, è possibile eseguire il backup dei dati dal dispositivo mobile al computer o a un dispositivo NAS. Per ulteriori dettagli, fare riferimento ad Aggiornamento di Acronis Ransomware Protection (p. 4).

1.2 Requisiti di sistema

Acronis Ransomware Protection richiede il seguente hardware:

- Processore Pentium 1 GHz
- 1 GB RAM
- 1,5 GB di spazio disponibile sul disco rigido
- Risoluzione dello schermo pari a 1024 x 768
- Mouse o altro dispositivo di puntamento (consigliato)

Copyright © Acronis International GmbH, 2003-2018

Altri requisiti:

- Una connessione a Internet.
- Privilegi di amministratore per eseguire Acronis Ransomware Protection.

Sistemi operativi:

- Windows 7 SP1 (tutte le edizioni)
- Windows 8 (tutte le edizioni)
- Windows 8.1 (tutte le edizioni)
- Windows 10 (tutte le edizioni)

1.3 Installazione di Acronis Ransomware Protection

Installazione di Acronis Ransomware Protection

Per installare Acronis Ransomware Protection:

1. Avviare il file di installazione. Prima di avviare la procedura di installazione, Acronis Ransomware Protection cercherà sul sito Web una versione più aggiornata. Se disponibile, verrà proposta l'installazione della versione più recente.
2. Fare clic su **Installa**.

   Acronis Ransomware Protection sarà installato nella partizione di sistema (solitamente C:).
3. Nella finestra visualizzata, accedere all'account Acronis.

   Fare riferimento a Account Acronis (p. 6) per maggiori dettagli.

Rimozione di Acronis Ransomware Protection

Selezionare **Start** -> **Impostazioni** -> **Pannello di controllo** -> **Installazione applicazioni** -> **Acronis Ransomware Protection** -> **Rimuovi**. Quindi seguire le istruzioni sullo schermo. Potrebbe essere necessario riavviare il computer in seguito al completamento dell'operazione.

Se si utilizza Windows 10, fare clic su **Start** -> **Impostazioni** -> **Sistema** -> **App e funzionalità** -> **Acronis Ransomware Protection** -> **Disinstalla**.

Se si utilizza Windows 8, selezionare l'icona Impostazioni, quindi selezionare **Pannello di controllo** -> **Disinstalla un programma** -> **Acronis Ransomware Protection** -> **Disinstalla**.

Se si utilizza Windows 7, fare clic su **Start** -> **Pannello di controllo** -> **Disinstalla un programma**-> **Acronis Ransomware Protection**-> **Disinstalla**.

1.4 Aggiornamento di Acronis Ransomware Protection

Acronis Ransomware Protection consente di eseguire il backup solo di file e cartelle e solo in Acronis Cloud. Se si desidera eseguire il backup di tutti i dati presenti nel computer o su partizioni distinte, è necessario passare a Acronis True Image. Questo prodotto fornisce un set completo di funzionalità per la protezione dei dati, tra cui backup a livello di file e disco nell'archivio NAS locale o in Acronis Cloud, archiviazione e sincronizzazione dei dati, protezione dei dati su dispositivi mobili e molto altro ancora.

Per effettuare l'aggiornamento, è sufficiente installare Acronis True Image su un computer in cui sia installato Acronis Ransomware Protection. Acronis True Image può essere acquistato sul sito Web Acronis.

Per acquistare ulteriore spazio di archiviazione su Acronis Cloud:

Copyright © Acronis International GmbH, 2003-2018

1. Avviare Acronis Ransomware Protection.
2. Fare clic sull'icona dell'account e quindi su **Acquista più spazio**. Si aprirà il sito Web Acronis.
3. Scegliere la quota adatta alle proprie esigenze, quindi fornire le informazioni sul pagamento.

1.5 Assistenza tecnica

Il supporto per Acronis Ransomware Protection è reperibile nella comunità e tramite la Knowledge Base Acronis e il forum di Acronis Ransomware Protection.

Copyright © Acronis International GmbH, 2003-2018

2 Guida rapida

In questa sezione

Account Acronis 6
Introduzione a Acronis Cloud 6

2.1 Account Acronis

Per far funzionare Acronis Ransomware Protection, è necessario aver effettuato l'accesso con l'account Acronis. Quando ci si disconnette, Acronis Active Protection continua a funzionare, ma l'applicazione smette di aggiornare il backup nel cloud.

Come creare un account Acronis

Dopo aver avviato Acronis Ransomware Protection per la prima volta, viene visualizzato il modulo di registrazione.

Se non si dispone ancora di un account Acronis:

1. Compilare il modulo di registrazione.

   Per proteggere i propri dati personali, scegliere una password complessa, evitare che finisca nelle mani sbagliate e modificarla periodicamente.

2. Selezionare **Crea account**.
3. Verrà inviato un messaggio di posta elettronica all'indirizzo specificato. Aprire il messaggio e confermare che si desidera creare un account.

Come accedere

Per accedere all'account Acronis:

1. Per passare dal modulo di registrazione al modulo di accesso, fare clic su **Dispongo già di un account**.
2. Immettere l'indirizzo e-mail e la password di registrazione, quindi fare clic su **Accedi**.

Come uscire

Per uscire dall'account Acronis:

1. Avviare Acronis Ransomware Protection.
2. Fare clic sull'icona dell'account e quindi su **Esci**.

2.2 Introduzione a Acronis Cloud

Acronis Cloud potrebbe non essere disponibile nella propria area geografica. Per maggiori informazioni, fare clic qui: https://kb.acronis.com/content/4541 https://kb.acronis.com/content/4541

Archiviazione remota

Da un lato, Acronis Cloud è un archivio remoto protetto utilizzabile per memorizzare i backup di file e cartelle: Acronis Ransomware Protection offre 5 GB di spazio di archiviazione gratuito nel cloud. Se non dovesse essere sufficiente a proteggere i file, l'utente è libero di acquistare altro spazio. Per ulteriori dettagli, fare riferimento ad Aggiornamento di Acronis Ransomware Protection (p. 4).

Copyright © Acronis International GmbH, 2003-2018

Poiché i file sono memorizzati in un archivio remoto, sono protetti anche in caso di furto del computer o d'incendio dell'abitazione. In caso di emergenza o danneggiamento dei dati, sarà possibile ripristinare i file.

Con un account, è possibile salvare i dati provenienti da più computer e da tutti i dispositivi mobili con sistemi operativi iOS e Android.

Applicazione Web

Acronis Cloud è anche un'applicazione Web che consente di ripristinare e gestire i dati archiviati in Acronis Cloud. Per lavorare con l'applicazione, è possibile utilizzare qualsiasi computer collegato a Internet.

Per accedere all'applicazione, visitare il sito https://www.acronis.com/my/online-backup/webrestore/ ed effettuare l'accesso al proprio account Acronis.

2.2.1 Garanzia della sicurezza dei dati

Quando si utilizza Acronis Cloud per l'archiviazione di backup, archivi o dati sincronizzati, è consigliabile assicurarsi che i dati personali non rischino di finire nelle mani sbagliate. Si potrebbe essere preoccupati in particolare per il proprio dispositivo mobile, poiché tutti i dati verranno trasferiti attraverso Internet.

Possiamo assicurare che tutti i dati saranno al sicuro. Prima di tutto, utilizziamo protocolli crittografati (SSL, TLS) per trasferire tutti i dati tramite Internet e LAN . Per accedere ai dati, effettuare l'accesso al proprio account fornendo l'indirizzo di posta elettronica e la password per l'account.

Inoltre, archiviamo i dati sui nostri server in forma crittografata. Solo l'utente avrà accesso ai suoi dati crittografati.

Copyright © Acronis International GmbH, 2003-2018

3 Backup dei dati

In questa sezione

Backup di file e cartelle 8
Rimozione dei dati da Acronis Cloud 9

3.1 Backup di file e cartelle

Acronis Ransomware Protection consente di eseguire il backup di documenti, foto, file musicali e video in Acronis Cloud. Se vengono danneggiati o persi, potranno essere facilmente ripristinati dall'archivio nel cloud.

Per eseguire il backup di file e cartelle:

1. Avviare Acronis Ransomware Protection.
2. Aprire il passaggio di configurazione del backup del tutorial o la finestra principale dell'applicazione.
3. Per specificare i file e le cartelle di cui si desidera eseguire il backup, procedere in uno dei seguenti modi:
   - In Esplora risorse o in un altro file manager selezionare i file e le cartelle, quindi trascinarli nella finestra di Acronis Ransomware Protection.
   - Fare clic su **Aggiungi manualmente** quindi passare alle cartelle memorizzate sul computer.

   Il backup inizierà automaticamente.

Il completamento del primo backup potrebbe richiedere diverso tempo. Le procedure di backup successive saranno probabilmente molto più rapide perché verranno trasferite via Internet solo le modifiche ai file. Acronis Ransomware Protection controlla i file ogni 15 minuti e ne carica automaticamente le modifiche in Acronis Cloud.

Per modificare le impostazioni di backup, fare clic sull'icona dell'ingranaggio nella finestra principale dell'applicazione.

Regole di conservazione

Dal momento cheAcronis Ransomware Protection monitora costantemente la copia di backup dei dati e carica le modifiche in Acronis Cloud, lo spazio di archiviazione disponibile per il backup potrebbe esaurirsi abbastanza in fretta. Per ridurre il numero di versioni dei file e ottimizzare il consumo di spazio nel cloud, Acronis Ransomware Protection conserva solo le seguenti versioni dei file:

- Tutte le versioni dell'ultima ora
- Le prime versioni di ogni ora delle ultime 24
- La prima versione di ogni giorno dell'ultima settimana
- La prima versione di ogni settimana dell'ultimo mese
- La prima versione di ogni mese

Tutte le altre versioni vengono eliminate automaticamente. Le regole di conservazione sono preimpostate e non è possibile modificarle.

Copyright © Acronis International GmbH, 2003-2018

3.2 Rimozione dei dati da Acronis Cloud

Poiché lo spazio disponibile in Acronis Cloud è limitato, è necessario gestire lo spazio del cloud cancellando i dati obsoleti o quelli che non sono più necessari. La cancellazione può essere effettuata in modi diversi.

Eliminazione di un intero backup

Quello più "drastico" consiste nell'eliminazione di tutto il backup da Acronis Cloud.

Per eliminare un backup completo:

1. Visitare il sito https://www.acronis.com/my/online-backup/webrestore/ e accedere al proprio account Acronis.
2. Nella scheda **Stato dell'archivio** accedere al backup da eliminare, fare clic sull'icona dell'ingranaggio e quindi su **Elimina**.

Eliminazione di file e cartelle specifici

Inoltre è possibile gestire Acronis Cloud eliminando i singoli file e le singole cartelle.

1. Visitare il sito https://www.acronis.com/my/online-backup/webrestore/ e accedere al proprio account Acronis.
2. Selezionare i file e le cartelle da eliminare e fare clic su **Elimina**.

Copyright © Acronis International GmbH, 2003-2018

4 Ripristino dei dati

In questa sezione

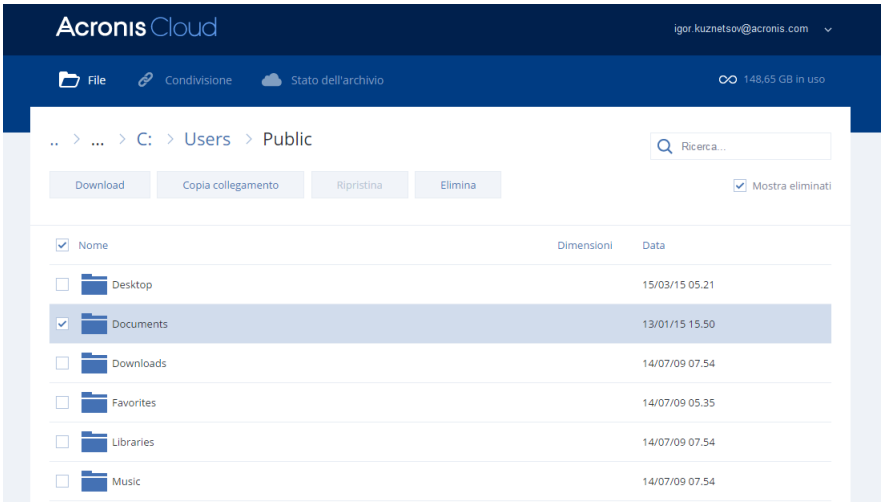
Ripristino di dati da Acronis Cloud 10
Ripristino di una versione del file 10

4.1 Ripristino di dati da Acronis Cloud

Una volta eseguito il backup dei file in Acronis Cloud, è possibile ripristinarli in un computer utilizzando l'applicazione Web Acronis.

Per ripristinare file e cartelle da Acronis Cloud:

1. Per aprire l'applicazione Web Acronis Cloud, eseguire una delle seguenti azioni:
   - Visitare il sito https://www.acronis.com/my/online-backup/webrestore/ e accedere al proprio account.
   - Nella finestra principale di Acronis Ransomware Protection fare clic sull'icona dell'account, quindi su **Sfoglia i miei dati**, effettuare l'accesso al proprio account e infine fare clic su **Backup**.
2. Dopo l'apertura della scheda **File** sul sito Web Acronis Cloud selezionare il backup online richiesto nell'area **Backup**.
3. Selezionare i file e le cartelle da ripristinare. Fare clic sul pulsante **Download** per avviare il ripristino.



Se sono stati selezionati diversi file e cartelle, verranno posizionati in un archivio zip.

Per impostazione predefinita, i dati verranno scaricati nella cartella **Download**. È possibile modificare il percorso di download.

4.2 Ripristino di una versione del file

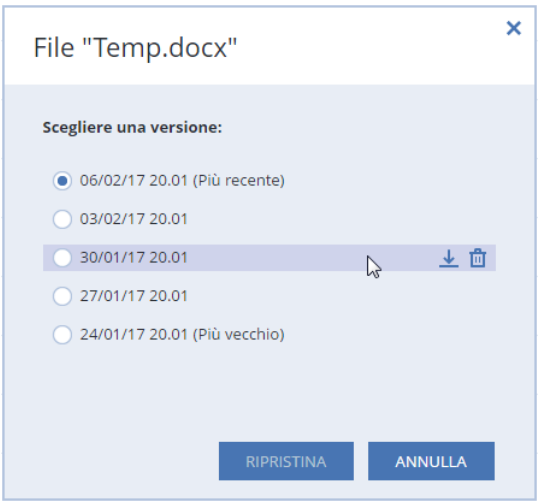
Per impostazione predefinita, Acronis Ransomware Protection seleziona le versioni più recenti rispetto alla data specificata. Tuttavia, per ogni file è possibile selezionare una versione specifica del file da ripristinare.

Copyright © Acronis International GmbH, 2003-2018

Notare che questa opzione non è applicabile alle cartelle.

Per ripristinare una versione specifica del file:

1. Nel contenuto del backup, selezionare il file di cui si desidera ripristinare la versione, quindi fare clic sull'icona dell'ingranaggio sul lato destro. Selezionare **Visualizza versioni** nel menu aperto.
2. Nella finestra visualizzata, selezionare la versione richiesta e fare clic sull'icona **Scarica**.



Per impostazione predefinita, i dati verranno scaricati nella cartella **Download**.

Per ulteriori informazioni sulle regole di conservazione dei backup, consultare Backup di file e cartelle (p. 8).

5 Acronis Active Protection

Che cosa è il ransomware?

Il ransomware è un software dannoso che blocca l'accesso ad alcuni file o all'intero sistema richiedendo un riscatto per lo sblocco. Il software visualizza una finestra che informa del blocco dei file e della necessità di pagare al più presto un riscatto per non perdere per sempre l'accesso ai file. Il messaggio può essere anche camuffato da dichiarazione ufficiale di autorità come ad esempio la polizia. Lo scopo del messaggio consiste nell'intimidire l'utente e spingerlo a non richiedere l'aiuto a uno specialista IT o alle autorità. Inoltre, non esiste alcuna garanzia di recuperare il controllo dei dati dopo il pagamento del riscatto.

Il computer può essere infettato da ransomware durante la visita di siti web non sicuri, l'apertura di messaggi e-mail provenienti da persone sconosciute o il clic su collegamenti sospetti di social network e messaggi istantanei.

Il ransomware può bloccare l'accesso a:

- **Intero computer**

  Impossibile utilizzare Windows o eseguire operazioni sul computer in uso. In generale, in questi casi il ransomware non esegue la crittografia dei dati dell'utente.
- **File specifici**

  Di solito, si tratta di dati personali come documenti, fotografie e video. Il ransomware esegue la crittografia dei file richiedendo denaro per ricevere la chiave di decodifica, l'unico metodo per decodificare i file.

Copyright © Acronis International GmbH, 2003-2018

- **Applicazioni**

  Il ransomware blocca alcuni dei programmi in uso in modo da impedirne l'utilizzo. Spesso questo software attacca il browser web in uso.

In che modo Acronis Ransomware Protection protegge i dati in uso dal ransomware?

Per proteggere il computer da ransomware, Acronis Ransomware Protection utilizza la tecnologia Acronis Active Protection. Basata su un approccio euristico, questa tecnologia esegue il monitoraggio dei processi in esecuzione sul computer utilizzando la modalità in tempo reale. Al rilevamento di un processo di terze parti che stia cercando di crittografare i file o di inserire del codice dannoso in un processo integro, chiederà di consentire al processo di modificare i file o di arrestarlo. Fare riferimento a Protezione dei dati dal ransomware (p. 13) per ulteriori informazioni.

L'approccio euristico è largamente utilizzato nei moderni software antivirus in quanto efficace per proteggere i dati dai malware. Contrariamente a un approccio basato sulla firma che può rilevare solo un campione, l'euristica rileva famiglie di malware che includono campioni con un comportamento simile. Un ulteriore vantaggio di questo approccio è la possibilità di individuare nuove tipologie di malware che non dispongono ancora di firma.

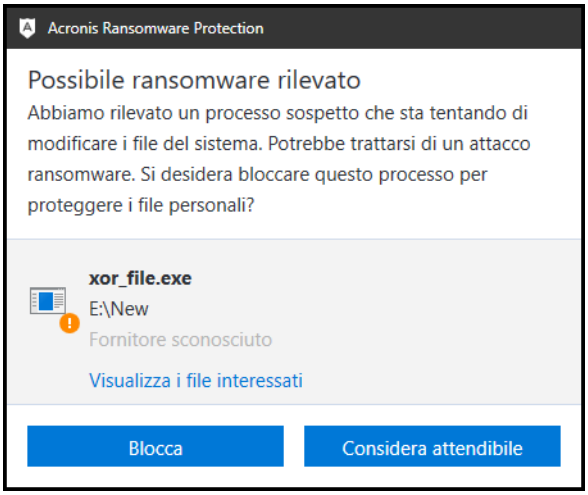
Acronis Active Protection utilizza l'euristica comportamentale e analizza le catene di azioni eseguite da un programma, che vengono poi confrontate con la catena di eventi in un database di schemi comportamentali dannosi. Dato che il metodo non è preciso, ammette i cosiddetti falsi positivi, quando un programma affidabile viene rilevato come malware. Per eliminare situazioni di questo tipo, Acronis Active Protection chiede all'utente di confermare se il processo rilevato è attendibile. Quando lo stesso processo viene rilevato per la seconda volta, è possibile aggiungerlo all'elenco delle autorizzazioni e impostare l'azione predefinita per il processo contrassegnandolo come affidabile o bloccato. In caso contrario, sarà possibile aggiungere il processo alla blacklist. In questo caso, il processo verrà bloccato ogni volta che cercherà di modificare i file.

Active Protection Acronis utilizza l'apprendimento automatico per raccogliere quanti più schemi diversi. Questa tecnologia si basa sull'elaborazione matematica dei big data ricevuti con la telemetria. Si tratta di un approccio di apprendimento automatico in quanto, maggiore è il quantitativo di dati elaborati, più elevata è la precisione con la quale un processo può essere identificato come ransomware o meno.

 Copyright © Acronis International GmbH, 2003-2018

5.1 Protezione dei dati dell'utente dal ransomware

All'attivazione di Active Protection Acronis, esegue il controllo dei processi in esecuzione sul computer in uso utilizzando la modalità in tempo reale. Al rilevamento di un processo di terze parti che stia cercando di crittografare i file, il servizio chiederà se consentire al processo di modificare i file o arrestarlo.



Prima di prendere una decisione, è possibile visualizzare l'elenco dei file che il processo sta per modificare.

Per consentire al processo di modificare i file, fare clic su **Consenti**. In caso di dubbi sulla sicurezza e la legalità del processo, consigliamo di fare clic su **Blocca**. In ogni caso, alla successiva esecuzione del processo, Acronis Ransomware Protection ripeterà la domanda. Per fornire al processo un permesso permanente o bloccarlo a ogni tentativo di modifica dei file dell'utente, selezionare la casella **Ricorda la mia scelta per questo processo** , quindi fare clic su **Blocca** o **Consenti**. Il processo verrà aggiunto all'elenco delle autorizzazioni. È possibile gestire l'elenco nelle impostazioni.

Dopo l'arresto del processo, verificare se i file sono stati crittografati o danneggiati in qualsiasi modo. In questo caso, fare clic su **Recupera file modificati**. Acronis Ransomware Protection cercherà le ultime versioni dei file e ripristinerà i file dalle copie temporanee preliminarmente create durante la verifica del processo.

Per rendere predefinita questa azione, selezionare la casella **Esegui sempre il ripristino dei file dopo il blocco di un processo**.

5.2 Gestire Acronis Active Protection

All'attivazione di Active Protection Acronis, esegue il controllo dei processi in esecuzione sul computer in uso utilizzando la modalità in tempo reale. Al rilevamento di un processo di terze parti che stia cercando di crittografare i file, il servizio chiederà se consentire al processo di modificare i file o arrestarlo. Fare riferimento a Acronis Active Protection (p. 11) per maggiori dettagli.

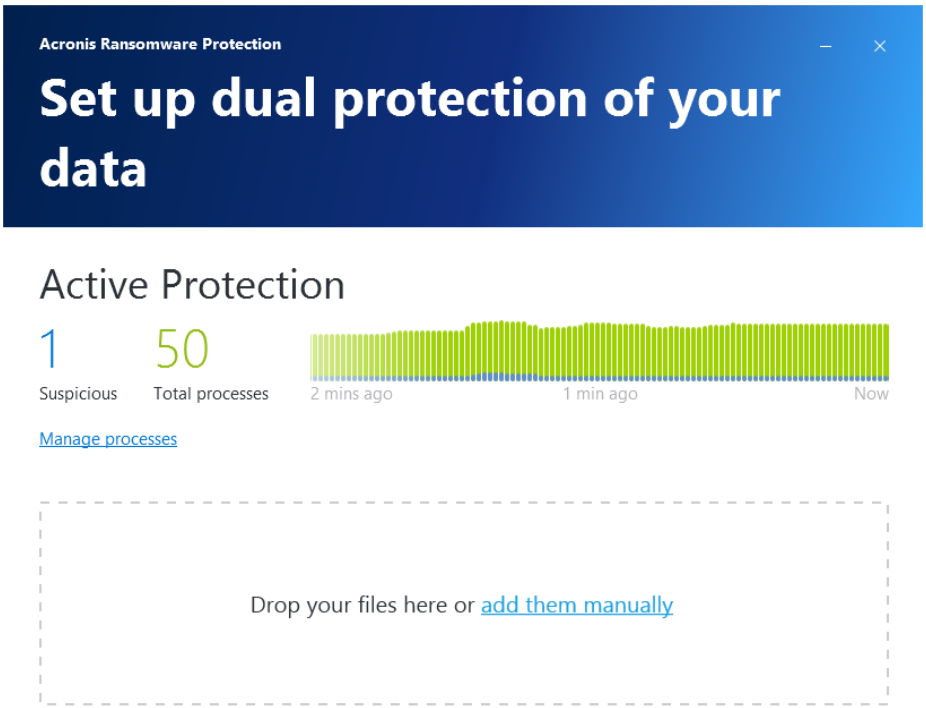
È possibile configurare le impostazioni di Acronis Active Protection e controllare il processo di protezione da più posizioni:

- Sezione su Acronis Active Protection
- Area di notifica nella barra delle applicazioni di Windows

Copyright © Acronis International GmbH, 2003-2018

Sezione su Acronis Active Protection

Questa sezione tratta le statistiche relative al processo di protezione e permette di configurare l'elenco di permessi di Acronis Active Protection.



È possibile:

- Verificare nella modalità in tempo reale il numero di processi monitorati e sicuri.
- Gestire l'elenco di autorizzazioni per consentire o bloccare le applicazioni.

Area di notifica nella barra delle applicazioni di Windows

Facendo clic con il pulsante destro del mouse sull'icona dell'area di notifica, si aprono i seguenti elementi del menu:

- **Disattivare Active Protection** (**Attivare Active Protection**): fare clic su questa opzione per attivare o disattivare la protezione dal ransomware.
- **Apri**: fare clic per aprire la finestra principale dell'applicazione.

Copyright © Acronis International GmbH, 2003-2018

6 Acronis Mobile

Acronis Cloud potrebbe non essere disponibile nella propria area geografica. Per maggiori informazioni, fare clic qui: https://kb.acronis.com/content/4541 https://kb.acronis.com/content/4541

Acronis Mobile consente di eseguire il backup dei dati in Acronis Cloud e di ripristinarli in caso di perdita o danneggiamento.

Quali periferiche sono supportate dall'applicazione mobile?

Acronis Mobile può essere installato su qualsiasi dispositivo mobile dotato dei seguenti sistemi operativi:

- iOS 8.0 e versioni successive (iPhone, iPad, iPod)
- Android 4.1 e versioni successive (telefoni cellulari e tablet)

Funzionalità principali

Acronis Mobile consente di:

- Backup dei dati personali, inclusi:
  - Foto
  - Video
  - Foto e video presenti in iCloud (solo iOS)
  - Contatti
  - Calendari
  - Messaggi (solo su Android)
  - Promemoria (solo su iOS)
- Crittografare i backup con l'algoritmo crittografico AES-256
- Eseguire automaticamente il backup dei dati nuovi e di quelli modificati
- Accedere ai backup cloud da tutti i dispositivi mobili e ripristinare i dati da questi backup

Dove posso trovare queste app?

È possibile visualizzare informazioni aggiuntive e scaricare Acronis Mobile dall'App Store di Apple o da Google Play:

- Acronis Mobile per i dispositivi iOS:
  https://itunes.apple.com/us/app/acronis-true-image-cloud/id978342143
- Acronis Mobile per i dispositivi Android:
  https://play.google.com/store/apps/details?id=com.acronis.acronistrueimage

In questa sezione

Installazione di Acronis Mobile 16
Backup del dispositivo mobile su Acronis Cloud 16
Ripristino dei dati mobili 16
Ripristino di dati su un nuovo smartphone 17
Impostazioni dell'app mobile 17

Copyright © Acronis International GmbH, 2003-2018

6.1 Installazione di Acronis Mobile

A seconda del dispositivo mobile, visitare l'App Store di Apple o Google Play e cercare l'app Acronis Acronis Mobile.

Ad esempio, per trovare e installare Acronis Mobile per iOS:

1. Su iPhone, aprire **App Store**.
2. Toccare l'icona Cerca.
3. Immettere **acronis** nel campo di ricerca.
4. Selezionare **acronis mobile** nei risultati della ricerca per passare alla pagina dell'app.
5. Seguire la procedura di installazione standard.

La procedura per cercare e installare l'app Android è simile.

6.2 Backup del dispositivo mobile su Acronis Cloud

Un backup mobile è la garanzia che i dati sui dispositivi mobili sono sicuri e possono essere ripristinati in caso di danneggiamento o perdita. È anche possibile usare il backup per trasferire i dati e le impostazioni personali dal vecchio smartphone a uno nuovo. Per ulteriori dettagli, fare riferimento ad Acronis Mobile (p. 15).

Per eseguire il backup del dispositivo mobile su Acronis Cloud:

1. Avviare Acronis Mobile.
2. Selezionare Acronis Cloud come destinazione per il backup.
3. Effettuare l'accesso all'account Acronis.
4. Toccare l'icona dell'ingranaggio e selezionare le categorie di dati dei quali si desidera effettuare il backup o toccare **Esegui backup** se si desidera eseguire il backup di tutti i dati.
5. [passaggio facoltativo] Toccare **Utilizza crittografia** per crittografare il backup e proteggerlo con una password. Altrimenti, toccare **Ignora**.
6. Toccare **Esegui backup**.
7. Consentire a Acronis Mobile di accedere ai dati personali.

Quando il backup è stato completato, i dati vengono caricati sul Acronis Cloud protetto. Se si desidera che il backup delle modifiche ai dati, per esempio nuove foto, venga eseguito automaticamente, accertarsi che l'impostazione **Backup continui** sia attivata. Se questa impostazione non è attivata, viene eseguito il backup dei nuovi dati solo quando si seleziona **Backup**. Per i dettagli, vedere Impostazioni app mobile (p. 17).

6.3 Ripristino dei dati mobili

Recuperare i dati mobili con un dispositivo mobile

Con smartphone o tablet, è possibile accedere a qualsiasi backup mobile archiviato in Acronis Cloud. Generalmente, è possibile aprire, visualizzare, ripristinare ed eseguire altre operazioni con una categoria di file o dati. Notare che a causa delle limitazioni del sistema operativo, alcune operazioni possono non essere disponibili per tipi di file specifici.

Per accedere ai dati mobili usando un backup mobile:

1. Installare e avviare Acronis Mobile.
2. Per accedere a un backup cloud, effettuare l'accesso all'account Acronis, se richiesto.

Copyright © Acronis International GmbH, 2003-2018

3. Per aprire il menu laterale, scorrere dal bordo sinistro dello schermo a quello destro, quindi selezionare **Accesso e ripristino**.
4. Selezionare il backup che contiene le categorie di file o dati desiderati. È possibile selezionare il backup tramite il nome o tramite il dispositivo che contiene i dati desiderati. Per esempio, per accedere ai dati dal dispositivo mobile corrente, selezionare questo dispositivo dall'elenco.
5. Individuare la categoria di file o dati desiderati.
6. In base al tipo di dati, possono essere effettuate le seguenti operazioni:
   - **Apri**
   - **Ripristina**
   - **Ripristina tutto**

6.4 Ripristino di dati su un nuovo smartphone

Con un backup mobile dello smartphone, è possibile trasferire facilmente i dati personali su un altro dispositivo mobile. Ad esempio, questo è utile quando si acquista un nuovo smartphone. Basta ripristinare i dati da Acronis Cloud sul nuovo dispositivo.

Per ripristinare i dati su un nuovo smartphone:

1. Installare e avviare Acronis Mobile.
2. Toccare **Esegui backup nel Cloud** ed effettuare l'accesso al proprio account Acronis.

   Acronis Mobile rileva la presenza di backup mobili in Acronis Cloud.
3. Toccare **Ripristina dati**.
4. Selezionare il dispositivo mobile da cui ripristinare i dati, quindi toccare **Seleziona dispositivo**. Ad esempio, se si desidera trasferire i dati dal vecchio smartphone, selezionarlo.
5. Selezionare le categorie di dati che si desidera ripristinare, quindi toccare **Ripristina**.
6. Consentire a Acronis Mobile di accedere ai dati personali.

Quando il ripristino è stato completato, i dati vengono scaricati sul nuovo dispositivo.

6.5 Impostazioni dell'app mobile

Per aprire la sezione **Impostazioni**, scorrere dal bordo sinistro dello schermo a quello destro, quindi selezionare **Impostazioni**. Sono disponibili le seguenti impostazioni:

- **Backup continuo**

  Se questa impostazione è attiva, Acronis Mobile rileva automaticamente i nuovi dati e li carica in Acronis Cloud.
- **Esegui il backup solo con rete Wi-Fi** o **Esegui il backup con rete Wi-Fi e cellulare**

  È possibile selezionare un tipo di connessione Internet per caricare e scaricare i dati. Questo è utile perché a volte una connessione Wi-Fi è più economica(o gratuita) o più affidabile di altri tipi di connessione.
- **Guida in linea**

  Selezionare questa voce per aprire una guida del prodotto basata sul Web.
- **Invia feedback**

  Questo comando consente di inviare feedback su Acronis Mobile, sottoporre un problema o contattare il supporto tecnico.
- **Cancellare le password memorizzate**

Copyright © Acronis International GmbH, 2003-2018

Selezionando l'impostazione che consente all'applicazione di ricordare la password durante la crittografia un backup, l'applicazione non chiederà la password operando sul dispositivo mobile con i dati di cui ha eseguito il backup. Cancellare le password memorizzate per fare in modo che l'applicazione chieda la password a ogni accesso al backup.

Copyright © Acronis International GmbH, 2003-2018

Informazioni sul copyright

Copyright © Acronis International GmbH, 2003-2018. Tutti i diritti riservati.

"Acronis", "Acronis Compute with Confidence", "Acronis Recovery Manager", "Acronis Secure Zone", "Acronis True Image", "Acronis Try&Decide" e il logo Acronis sono marchi commerciali di Acronis International GmbH.

Linux è un marchio registrato di Linus Torvalds.

VMware e VMware Ready sono marchi e/o marchi registrati di VMware, Inc. negli Stati Uniti e/o in altre giurisdizioni.

Windows e MS-DOS sono marchi registrati di Microsoft Corporation.

Tutti gli altri marchi e copyright a cui si fa riferimento appartengono ai rispettivi proprietari.

È vietata la distribuzione di versioni con modifiche sostanziali di questo documento, a meno che non sia stata concessa in precedenza un'autorizzazione specifica da parte del detentore del copyright.

È vietata la distribuzione a fini commerciali del presente lavoro o di lavori derivati in qualsiasi formato di libro (cartaceo), a meno che non sia stata concessa in precedenza un'autorizzazione da parte del detentore del copyright.

LA PRESENTE DOCUMENTAZIONE VIENE FORNITA "ALLO STATO IN CUI SI TROVA" E QUALSIVOGLIA CONDIZIONE, DICHIARAZIONE E GARANZIA, SIA ESSA ESPRESSA O IMPLICITA, IVI INCLUSA QUALSIVOGLIA GARANZIA DI COMMERCIABILITÀ, IDONEITÀ AD UN FINE SPECIFICO O NON INFRAZIONE, SI INTENDE ESCLUSA, NELLA MISURA IN CUI LE SUDDETTE RINUNCE SIANO DA INTENDERSI LEGALMENTE CONSENTITE.

Insieme al Software e/o al Servizio potrebbe essere fornito un codice di terze parti. I termini di licenza di tali terze parti sono descritti in dettaglio nel file license.txt che si trova nella directory di installazione principale. L'elenco degli ultimi aggiornamenti del codice di terze parti e i relativi termini di licenza utilizzati con il Software e/o il Servizio sono sempre disponibili all'indirizzo https://kb.acronis.com/content/7696

Tecnologie protette da brevetto Acronis

Le tecnologie utilizzate in questo prodotto sono protette e tutelate da uno o più Numeri brevetto USA: 7.047.380; 7.246.211; 7.275.139; 7.281.104; 7.318.135; 7.353.355; 7.366.859; 7.383.327; 7.475.282; 7.603.533; 7.636.824; 7.650.473; 7.721.138; 7.779.221; 7.831.789; 7.836.053; 7.886.120; 7.895.403; 7.934.064; 7.937.612; 7.941.510; 7.949.635; 7.953.948; 7.979.690; 8.005.797; 8.051.044; 8.069.320; 8.073.815; 8.074.035; 8.074.276; 8.145.607; 8.180.984; 8.225.133; 8.261.035; 8.296.264; 8.312.259; 8.347.137; 8.484.427; 8.645.748; 8.732.121; 8.850.060; 8.856.927; 8.996.830; 9.213.697; 9.400.886; 9.424.678; 9.436.558; 9.471.441; 9.501.234; e applicazioni in attesa di brevetto.

7 Glossario

A

Acronis Active Protection

Una tecnologia che protegge i dati dal ransomware, un software dannoso che blocca l'accesso ad alcuni file o all'intero sistema richiedendo un riscatto per lo sblocco. Basata su un approccio euristico, questa tecnologia esegue il monitoraggio dei processi in esecuzione sul computer con la modalità in tempo reale e informa l'utente sui tentativi di crittografare i dati sul computer. I file crittografati possono essere ripristinati dalle copie o dai backup temporanei.

B

Backup

1. Uguale all'Operazione di backup (p. 20).
2. Un set di versioni di backup create e gestite da un'attività di backup. Un backup può contenere diverse versioni del backup create usando il metodo di backup completo e incrementale (p. 20). Le versioni di backup appartenenti allo stesso backup di solito vengono archiviate nella stessa posizione.

Backup incrementale

1. Un metodo di backup utilizzato per salvare le modifiche dei dati effettuate dall'ultima versione (di qualsiasi tipo) del backup all'interno di un backup.
2. Una procedura di backup che crea una versione incrementale del backup.

Backup online

Backup online: un backup creato utilizzando Acronis Online Backup. I backup online vengono conservati in un archivio speciale chiamato Acronis Cloud, accessibile da Internet. Il vantaggio principale di un backup online è che tutti i backup vengono conservati in una posizione remota. Ciò fornisce una garanzia che tutti i dati di cui è stato eseguito il backup saranno al sicuro a prescindere dagli archivi locali dell'utente. Per iniziare a utilizzare Acronis Cloud un utente deve effettuare l'abbonamento al servizio.

O

Operazione di backup

Un'operazione che crea una copia dei dati esistenti sul disco rigido della macchina per ripristinare o riconfigurare i dati ad una data e ad un'ora specificate.

P

Processo sospetto

Acronis Active Protection (p. 20) utilizza l'euristica comportamentale e analizza la catena di azioni eseguite da un programma (ovvero un processo), che vengono poi confrontate con la catena di eventi in un database di schemi comportamentali dannosi. Se il programma manifesta comportamenti simili a quelli di un ransomware o prova a modificare i file dell'utente, viene considerato sospetto.

R

Ripristina

Il ripristino è una procedura che consiste nel riportare i dati danneggiati a uno stato normale precedente da un backup.

V

Versione del backup

Il risultato di una singola operazione di backup (p. 20). Fisicamente, si tratta di un file o di una serie di file che contengono una copia dei dati inclusi nel backup alla data e all'ora specificate. I file delle versioni del backup create da Acronis Ransomware Protection hanno estensione TIB. Anche i file TIB derivanti dal consolidamento delle versioni dei backup sono chiamati versione del backup.

Versione incrementale del backup

Una versione del backup che archivia le modifiche dei dati rispetto all'ultima versione del backup. È necessario avere accesso ad altre versioni del backup dallo stesso backup per ripristinare i dati da una versione incrementale del backup.

Copyright © Acronis International GmbH, 2003-2018