



---

# TeamViewer 10 Handbuch

---

**ITbrain**

Rev 10.2-201503



# Inhaltsverzeichnis

<b>1</b>	<b>Allgemein</b>	<b>4</b>
1.1	Über ITbrain™	4
1.2	Über das Handbuch	5
<b>2</b>	<b>Voraussetzungen</b>	<b>6</b>
2.1	Lizenzierung	6
2.2	Systemvoraussetzungen	7
<b>3</b>	<b>ITbrain einrichten</b>	<b>8</b>
3.1	Lizenz aktivieren	8
3.2	ITbrain für Endpunkte aktivieren	9
3.3	ITbrain-Richtlinie einem Endpunkt zuweisen	11
<b>4</b>	<b>Monitoring</b>	<b>17</b>
4.1	Alarmprotokoll	17
4.2	Alarmmeldungen bearbeiten	18
4.3	Alarmmeldungen erneut prüfen	19
<b>5</b>	<b>Inventarisierung</b>	<b>20</b>
5.1	Berichte	20
<b>6</b>	<b>Anti-Malware</b>	<b>23</b>
6.1	Manuelle Scans	23
6.2	Status der Geräte	24
6.3	Alarmprotokoll	25
6.4	Bedrohung bestätigen	27



6.5	Details zur Bedrohung .....	28
-----	-----------------------------	----



# 1 Allgemein

## 1.1 Über ITbrain™

ITbrain™ ist eine einfache und professionelle IT Management Plattform, die in TeamViewer integriert ist. Folgende Dienste sind für ITbrain™ verfügbar:

- ITbrain™ Monitoring und Inventarisierung
- ITbrain™ Anti-Malware

Mit ITbrain™, TeamViewer und der TeamViewer Management Console haben Sie alle wichtigen Daten und Funktionen Ihrer Systeme stets im Blick.

- Mit dem Dienst **ITbrain™ Monitoring und Inventarisierung** richten Sie individuelle Checks ein, die Sie gezielt z. B. über Festplattenzustand, Antivirus-Software, Online-Status, Arbeitsspeicher-Auslastung oder laufende Prozesse eines Computers informieren. Mit der integrierten Inventarisierung erstellen Sie zudem Berichte über IT-Bestände in Ihrem Netzwerk. Komfortabel überwachen Sie all Ihre Geräte in der TeamViewer Management Console oder über Ihren TeamViewer Client und erhalten Alarmmeldungen zusätzlich direkt per E-Mail.
- Mit dem Dienst **ITbrain™ Anti-Malware** schützen Sie Ihre Geräte vor Schadsoftware. ITbrain™ scannt Ihre Geräte regelmäßig. Entdecken Sie potentielle Bedrohungen frühzeitig und schützen Sie Ihre Geräte zuverlässig. Gefundene Schadsoftware wird umgehend unschädlich gemacht und kann später auch komplett gelöscht werden. Mit der TeamViewer Management Console haben Sie jederzeit und überall alle Bedrohungen und Scans im Blick.

**Hinweis:** Mit ITbrain™ können Sie Computer ab Windows XP SP2 und Server ab Windows Server 2003 überwachen.

**Hinweis:** ITbrain™ ist nicht Teil der TeamViewer-Lizenz. Falls Sie ITbrain™ in vollem Umfang nutzen möchten, sind separate Lizenzen erforderlich.



## 1.2 Über das Handbuch

Dieses Handbuch beschreibt die Arbeit mit ITbrain™ von TeamViewer.

Sofern keine anderweitigen Angaben gemacht werden, bezieht sich die beschriebene Funktionalität stets auf die im Titel angegebene Funktion der TeamViewer Vollversion unter Microsoft Windows. „ITbrain™“ wird im Folgenden vereinfacht als „ITbrain“ bezeichnet.

Mac OS, iPhone und iPad sind Handelsmarken der Apple Inc. Linux® ist eine eingetragene Marke von Linus Torvalds in den USA und anderen Ländern. Android ist eine Handelsmarke der Google Inc. Windows und Microsoft sind eingetragene Marken der Microsoft Corporation in den USA und anderen Ländern. In diesem Handbuch werden die Betriebssysteme, Microsoft® Windows® XP, Microsoft® Windows® Vista, Microsoft® Windows® 7 und Microsoft® Windows® 8 im Folgenden vereinfacht als „Windows“ bezeichnet. Alle unterstützten Betriebssysteme finden Sie auf unserer Website unter <http://www.teamviewer.com/de/kb/38-Which-operating-systems-are-supported.aspx>.



## 2 Voraussetzungen

Im Folgenden finden Sie die Voraussetzungen, die erfüllt sein müssen, um ITbrain in vollem Umfang nutzen zu können.

### 2.1 Lizenzierung

ITbrain ist ein eigenständiges Produkt und ist nicht im TeamViewer-Lizenzmodell enthalten. Das bedeutet:

- ITbrain ist nicht Teil der TeamViewer Corporate-, Premium-, oder Business-Lizenz.
- ITbrain kann auch ohne eine TeamViewer Corporate-, Premium-, oder Business-Lizenz genutzt werden.
- Um den vollen Funktionsumfang von ITbrain nutzen zu können, benötigen Sie eine ITbrain-Lizenz.

ITbrain ist im Monats- oder Jahresabonnement erhältlich. Das Lizenzmodell ist so aufgebaut, dass Sie für jeden Computer, für den Sie ITbrain nutzen möchten, einen so genannten Endpunkt erwerben. Das bedeutet, wenn Sie mit ITbrain beispielsweise fünf Computer überwachen wollen, benötigen Sie eine ITbrain-Lizenz mit fünf Endpunkten.

Weitere Informationen zum Lizenzmodell finden Sie in unserem **ITbrain-Shop** unter <https://www.itbrain.com/pricing/>.

**Hinweis:** Sie können die Funktionen von ITbrain auch ohne Lizenz unverbindlich 14 Tage testen.

**Hinweis:** Sie benötigen für jeden ITbrain-Dienst separate Endpunkte. Die verschiedenen Dienste können unabhängig voneinander genutzt werden.



## 2.2 Systemvoraussetzungen

Um Alarmmeldungen von ITbrain zu sehen benötigen Sie die TeamViewer Management Console.

Diese ist browserbasiert und somit unabhängig vom Betriebssystem.

Alternativ können Sie auch die TeamViewer 9 Vollversion (oder neuer) unter folgenden Betriebssystemen nutzen:

- Windows
- Linux
- iOS
- Windows Phone 8

### 2.2.1 ITbrain Monitoring und Inventarisierung

Um ITbrain Monitoring und Inventarisierung nutzen zu können, muss auf den Geräten, die Sie überwachen wollen (Endpunkte), eines der folgenden Betriebssysteme ausgeführt werden:

- Windows 8 / 7 / Vista / XP SP3
- Windows Server 2012 R2 / 2012 / 2008 R2 / 2008 / 2003 R2  
Der Antivirus-Software Check wird für Server-Betriebssysteme nicht unterstützt.

und TeamViewer 8 Vollversion oder Host (oder neuer) installiert sein.

### 2.2.2 ITbrain Anti-Malware

Um ITbrain nutzen zu können, muss auf den Geräten, die Sie mit ITbrain schützen wollen (Endpunkte), eines der folgenden Betriebssysteme ausgeführt werden:

- Windows 8 / 7 / Vista / XP SP3
- Windows Server 2012 R2 / 2012 / 2008 R2 / 2008 / 2003 R2

und TeamViewer 9 Vollversion oder Host (oder neuer) installiert sein.



## 3 ITbrain einrichten

In der TeamViewer Management Console richten Sie ITbrain für die Nutzung ein. Öffnen Sie dazu die TeamViewer Management Console unter <https://login.teamviewer.com> und melden Sie sich mit Ihrem TeamViewer-Konto an.

Alle weiteren Schritte zur Konfiguration von ITbrain werden im Folgenden beschrieben.

**Hinweis:** Je nach Berechtigung können auch TeamViewer-Konten Ihres Firmen-Profiles die im Folgenden beschriebenen Funktionen nutzen.

### 3.1 Lizenz aktivieren

Wie unter *Abschnitt 2.1 "Lizenzierung", Seite 6* beschrieben, wird für die Nutzung aller ITbrain-Funktionen eine ITbrain-Lizenz benötigt. Nach dem Erwerb einer Lizenz erhalten Sie eine Bestätigung-E-Mail.



Klicken Sie auf den Aktivierungs-Link, um die Lizenz für Ihr TeamViewer-Konto zu aktivieren.

Nachdem Sie die Lizenz für Ihr Konto aktiviert haben, ist diese mit Ihrem TeamViewer-Konto verknüpft und kann genutzt werden.

ITbrain-Lizenz für Ihr TeamViewer-Konto aktivieren.





**Hinweis:** Falls Sie mit Ihrem TeamViewer-Konto einem Firmen-Profil beigetreten sind, kann die ITbrain-Lizenz auf Firmenebene genutzt werden.

**Hinweis:** Die Aktivierung der ITbrain-Lizenz kann nur in Ausnahmefällen rückgängig gemacht werden.

## 3.2 ITbrain für Endpunkte aktivieren

Alle Computer, auf denen Sie ITbrain nutzen möchten, werden Endpunkte genannt. Auf jedem Endpunkt muss ITbrain aktiviert und konfiguriert werden. Nutzen Sie dazu die Bulk-Aktivierung, um ITbrain auf mehreren Geräten gleichzeitig zu aktivieren oder aktivieren Sie ITbrain für jeden Endpunkt separat.

Nachdem Sie ITbrain Anti-Malware für die Endpunkte aktiviert haben, werden auf dem Endpunkt folgende Schritte automatisch ausgeführt:

- Der ITbrain-Dienst wird heruntergeladen und auf dem Gerät installiert.
- Die neuesten ITbrain-Virendefinitionen werden heruntergeladen.
- Ein schneller Scan wird gestartet.
- Die Standard-Anti-Malware-Richtlinie wird dem Gerät zugewiesen.

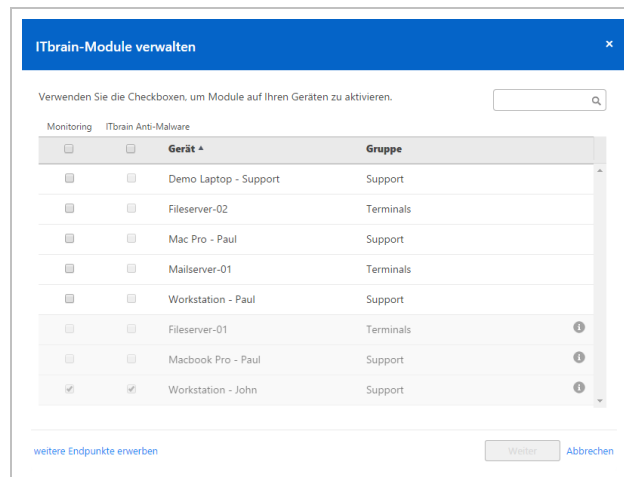
### 3.2.1 Bulk-Aktivierung

Um nicht jeden Endpunkt einzeln Ihrem TeamViewer-Konto zuweisen zu müssen und auf diesem ITbrain zu aktivieren, besteht die Möglichkeit einer Bulk-Aktivierung. Dabei werden in einem Schritt alle Endpunkte automatisiert mit Hilfe ihrer persönlichen Kennwörter Ihrem Konto zugewiesen und ITbrain für die Endpunkte aktiviert.

Um die Bulk-Aktivierung aufzurufen, wählen Sie eine der Methoden:

- ➡ Klicken Sie unter **ITbrain | Alarmprotokoll** auf die Schaltfläche **Geräte hinzufügen**.
- ➡ Klicken Sie in einer Gruppe Ihrer Computer & Kontakte-Liste auf **Extras | Geräte mit ITbrain überwachen**.

Wählen Sie im Dialog die ITbrain-Dienste, die Sie für die jeweiligen Geräte nutzen möchten. Folgen Sie anschließend den Anweisungen im Dialog.

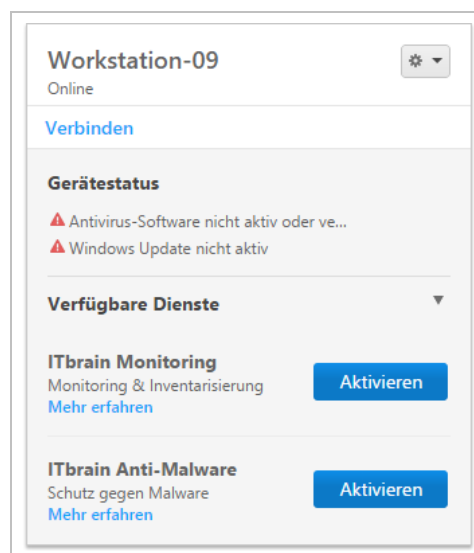


Bulk-Aktivierung für alle ITbrain-Endpunkte.

### 3.2.2 Endpunkte separat aktivieren

Sie können ITbrain auch für einzelne Geräte in Ihrer Computer & Kontakte-Liste aktivieren. Dabei wird das Gerät erst Ihrem TeamViewer-Konto zugewiesen und anschließend der ITbrain-Service eingerichtet.

- ➡ Klicken sie dazu auf deren Namen in der Computer & Kontakte-Übersicht und anschließend für das jeweilige Paket auf **Aktivieren**.



ITbrain-Dienste für einzelnen Endpunkt aktivieren.

- ➡ Falls Sie das persönliche Kennwort für das Gerät nicht in der Computer & Kontakte-Liste hinterlegt haben, geben Sie dieses im Dialog ein.



Gerät mit dem persönlichen Kennwort Ihrem Konto zuweisen.

Falls Sie für den Endpunkt kein persönliches Kennwort festgelegt haben, können Sie den Endpunkt auch über die Einstellungen in der TeamViewer Vollversion Ihrem Konto zuweisen.

➡ Dazu müssen Sie die Einstellungen unter **Extras | Optionen | Allgemein | Kontozugehörigkeit** lokal auf diesem Computer aufrufen.

### 3.3 ITbrain-Richtlinie einem Endpunkt zuweisen

Definieren Sie Richtlinien, die festlegen, in welchem Umfang und wann die Computer auf Schadsoftware und Fehler überprüft werden.

Standardmäßig ist für jeden Dienst eine vordefinierte Richtlinie vorhanden.

Richtlinien können auch einer Gruppe zugewiesen werden. Alle Endpunkte innerhalb dieser Gruppe erben dann die Richtlinie von der Gruppe. Dazu muss für jeden Endpunkt innerhalb der Gruppe als Richtlinie **Von Gruppe erben** ausgewählt sein.

ITbrain-Richtlinie einem Endpunkt zuweisen.



Im letzten Schritt der Konfiguration weisen Sie den Endpunkten eine der verfügbaren Richtlinien zu.

- ➡ Klicken Sie dazu auf den Namen des Endpunkts in der Computer & Kontakte-Übersicht und anschließend auf **Eigenschaften**. In den Eigenschaften des Endpunktes können sie unter **ITbrain Monitoring Richtlinie** und **Anti-Malware-Richtlinie** eine der konfigurierten Richtlinien auswählen.
- ➡ Wählen Sie alternativ eine Richtlinie bei der Bulk-Aktivierung aus oder weisen Sie eine Richtlinie einer Gruppe zu.

Standardmäßig ist für alle Endpunkte die Richtlinie **Von Gruppe erben** ausgewählt und für alle Gruppen die **Standard-Richtlinie** definiert. Wie Sie eigene Richtlinien konfigurieren lesen Sie unter [Abschnitt 3.3.1 "Richtlinien konfigurieren", Seite 12](#).

Die **Standard-Monitoringrichtlinie** enthält folgende unter [Abschnitt 3.3.1 "Richtlinien konfigurieren", Seite 12](#) beschriebenen Monitoring-Checks:

- Ist eine **Antivirus**-Software installiert und aktiv?
- Sind mehr als 500 MB **Arbeitsspeicher** verfügbar?
- Ist die **CPU-Auslastung** höher als 75%?
- Wie ist der **Festplattenzustand**?
- Ist die freie **Speicherkapazität** geringer als 10%?
- Ist das **Windows-Update** aktiv?
- Ist die **Windows-Firewall** aktiviert?

Die **Standard-Anti-Malware-Richtlinie** enthält folgende unter [Abschnitt 3.3.1 "Richtlinien konfigurieren", Seite 12](#) beschriebenen Scans:

- Schneller Scan, täglich 09:00Uhr
- Vollständiger Scan, täglich 12:00Uhr

### 3.3.1 Richtlinien konfigurieren

Legen Sie für jeden ITbrain-Dienst Richtlinien fest. Abhängig vom Dienst beinhalten diese folgende Informationen:

- **Anti-Malware Richtlinien:** Definieren, wann und in welchem Umfang Ihre Geräte durch ITbrain Anti-Malware auf Schadsoftware geprüft werden.
- **Monitoring-Richtlinien:** Definieren, anhand welcher Kriterien (Arbeitsspeicherauslastung, CPU-Auslastung, Festplattenzustand, etc.) Ihre Geräte durch ITbrain Monitoring und Inventarisierung geprüft werden.

Alle Richtlinien finden Sie unter **ITbrain | Richtlinien**. Dort können Sie ebenfalls neue Richtlinien erstellen.

- ➡ Klicken Sie dazu auf die Schaltfläche **Richtlinie hinzufügen**.



Zur Verdeutlichung der Nutzung unterschiedlicher Richtlinien im Folgenden ein kurzes Anwendungsbeispiel.

**Beispiel:** Definieren Sie je nach verwendeter Hardware unterschiedliche Richtlinien. Für Ihre Server ist es beispielsweise wichtig, dass ein bestimmter Dienst immer läuft. Bekommen Sie eine Nachricht, sobald der Dienst nicht mehr läuft. Auf den überwachten Desktop-Computern ist es wiederum wichtig, dass das Windows-Update aktiviert ist. Erhalten Sie also eine Benachrichtigung, falls das Windows-Update deaktiviert wird.

### 3.3.2 Eine neue Richtlinie hinzufügen

In diesem Dialog können Sie neben einem **Namen** für die Richtlinie auch die relevanten Optionen für die jeweiligen Richtlinie definieren. Im Folgenden finden Sie eine Beschreibung der verfügbaren Optionen je Richtlinie.

**Brand new Anti-Malware policy that rocks**

Name  
Brand new Anti-Malware policy th

Geplante Scans

Scantyp	Zeitplan	Details
Vollständiger Scan	Wöchentlich, Sonntag, ...	
Schneller Scan	Täglich, 23:30 Uhr	
Benutzerdefinierte...	Alle 3 Tage, 20:00 Uhr	C:\Windows

+ Scan hinzufügen

☒ Echtzeitschutz

E-Mail-Benachrichtigung  
example-en@example.com

ITbrain Anti-Malware-Richtlinie konfigurieren.

**Policy for "Wayne Enterprises"**

Allgemein

Name  
Policy for "Wayne Enterprises"

Checks

Typ	Einstellungen	E-Mail-Benachrichtigung
Antivirus		
Arbeitsspeicherauslastung	2000 MB	
Online Status		Michael Smith
Prozess	IEXPLORER.EXE, wird ...	
Windows Update		
Windows-Dienst	airbackup Service Con...	

Bitte wählen Sie einen Check aus...

Hinzufügen

Richtlinie löschen

Speichern Abbrechen

ITbrain Monitoring Richtlinie konfigurieren.



## Anti-Malware-Richtlinie hinzufügen

### Geplante Scans

**Scans** Definieren Sie eine beliebige Anzahl an Scans. Abhängig vom Scantyp und Zeitplan werden alle Geräte regelmäßig auf Schadsoftware überprüft.

➡ Klicken Sie auf die Schaltfläche **Scan hinzufügen** und definieren Sie einen Scan.

Wählen Sie zwischen folgenden Optionen:

- **Schneller Scan:** ITbrain Anti-Malware scannt nur bestimmte Daten, laufende Prozesse und die Registry. Dadurch ist der Scan schnell abgeschlossen und die wichtigsten Daten Ihres Gerätes sind geschützt.
- **Vollständiger Scan:** ITbrain Anti-Malware scannt die gesamten Festplatten Ihres Gerätes. Dieser Scan dauert länger als ein schneller Scan. Die gesamten Daten Ihres Gerätes werden überprüft.

**Hinweis:** Bitte beachten Sie, das über die Dauer des Scans gegebenenfalls die Geschwindigkeit Ihres Systems beeinträchtigt sein kann.

- **Benutzerdefinierter Scan:** ITbrain Anti-Malware scannt ein definiertes Laufwerk, Ordner oder Datei. Geben Sie dazu den Pfad der Form `C:\Folder\Filename.fileextension` ein.

### Echtzeitschutz

**An/Aus** Wählen Sie ob, für die Richtlinie der Echtzeitschutz deaktiviert werden soll.

Falls aktiviert werden alle Dateien, auf die zugegriffen wird (geöffnet, ausgeführt, etc.), auf Malware überprüft. Falls deaktiviert, werden Probleme gegebenenfalls nur entdeckt, sobald ein Scan ausgeführt wird.

**Achtung:** Falls Sie den Echtzeitschutz deaktivieren, ist das Gerät zwischen den Scans potentiell gefährdet.

### E-Mail-Benachrichtigung

**E-Mail** Falls eine Bedrohung entdeckt wird, sendet ITbrain eine E-Mail-Benachrichtigung an die definierten E-Mail-Adressen.

➡ Geben Sie E-Mail-Adressen ein, die Benachrichtigungen zu entdeckten Bedrohungen erhalten sollen.



## Monitoringrichtlinie hinzufügen

ITbrain Monitoring Check	Beschreibung
<b>Antivirus</b>	Ein Alarm wird ausgelöst, falls keine Antivirus-Software installiert oder die installierte Antivirus-Software veraltet ist.
<b>Arbeitsspeicherauslastung</b>	<p>Ein Alarm wird ausgelöst, falls der durchschnittlich verfügbare Arbeitsspeicher über einen Zeitraum von fünf Minuten unter den definierten Schwellenwert fällt.</p> <p>Definieren Sie im Textfeld den Schwellenwert.</p>
<b>CPU-Auslastung</b>	<p>Ein Alarm wird ausgelöst, falls die Durchschnittsauslastung eines Prozessors über einen Zeitraum von fünf Minuten den gewählten Schwellenwert überschreitet.</p> <p>Wählen Sie mit dem Schieberegler einen Schwellenwert.</p>
<b>Ereignisprotokoll</b>	<p>Ein Alarm wird ausgelöst, falls bestimmte Informationen in einem Ereignisprotokoll entdeckt werden. Nur wenn alle unten beschriebenen Parameter zutreffen, wird ein Alarm ausgelöst.</p> <ul style="list-style-type: none"> <li>• <b>Name:</b> Geben Sie einen beschreibenden Namen ein.</li> <li>• <b>Ereignisprotokoll:</b> Wählen Sie, ob die Protokolle zu Anwendungen, Sicherheit oder System geprüft werden.</li> <li>• <b>Ereignis ID(s):</b> Legen Sie die Ergebnis-IDs der Protokolle fest, für die ein Alarm ausgelöst werden soll.</li> <li>• <b>Ereignisquelle:</b> Legen Sie die Ereignisquelle fest. So können Sie z. B. Alarme nach Anwendungen filtern.</li> <li>• <b>Ereignistyp:</b> Wählen Sie, welchen Ergebnistyp (Ebene) das Protokoll hat, um einen Alarm auszulösen.</li> </ul>
<b>Festplattenzustand</b>	Ein Alarm wird ausgelöst, sobald ein Datenträger physikalische Fehler meldet. Dies gilt für alle internen Festplatten.
<b>Online Status</b>	Ein Alarm wird ausgelöst, sobald das Gerät offline ist.



ITbrain Monitoring Check	Beschreibung
<b>Prozess</b>	<p>Ein Alarm wird ausgelöst, sobald ein bestimmter Prozess ausgeführt oder nicht ausgeführt wird.</p> <ul style="list-style-type: none"> <li>• <b>Prozessname:</b> Geben Sie den Namen des Prozesses ein, für den ein Alarm ausgelöst werden soll (z. B. „BackupSC.exe“). Den Namen finden Sie über den Taskmanager in den Eigenschaften des Prozesses unter <b>Details   Originalname</b>.</li> <li>• <b>Alarmbedingung:</b> Wählen Sie, ob ein Alarm ausgelöst werden soll, falls der Prozess beendet oder gestartet wird.</li> </ul>
<b>Speicherkapazität</b>	<p>Ein Alarm wird ausgelöst, sobald der Festplattenspeicher unter den definierten Wert fällt.</p> <ul style="list-style-type: none"> <li>• <b>Datenträger:</b> Wählen Sie die Partition der Festplatte, für die ein Alarm ausgelöst werden soll.</li> <li>• <b>Mindestmenge des freien Speicherplatzes:</b> Geben Sie einen Wert für den minimalen Speicherplatz an. Ist der Speicherplatz geringer als der angegebenen Wert, wird ein Alarm ausgelöst.</li> </ul>
<b>Windows Update</b>	<p>Ein Alarm wird ausgelöst, sobald das Windows-Update deaktiviert ist.</p>
<b>Windows-Dienst</b>	<p>Ein Alarm wird ausgelöst, sobald ein Windows-Dienst nicht mehr ausgeführt wird.</p> <ul style="list-style-type: none"> <li>• <b>Dienstname:</b> Geben Sie den Namen des Dienstes ein, für den ein Alarm ausgelöst werden soll (z. B. „air-backup Service Controller“). Den Namen finden Sie über den Windows Dienst-Manager in den Eigenschaften des Dienstes unter <b>Allgemein   Dienstname</b>.</li> <li>• <b>Alarm:</b> Wählen Sie, nach wie vielen fehlerhaften Überprüfungs-Intervallen ein Alarm ausgelöst wird.</li> </ul>
<b>Windows-Firewall</b>	<p>Ein Alarm wird ausgelöst, sobald die Windows-Firewall deaktiviert ist.</p>





# 4 Monitoring

Nutzen Sie den ITbrain-Dienst **ITbrain Monitoring**, um Ihre Geräte zu überwachen und für die Inventarisierung.

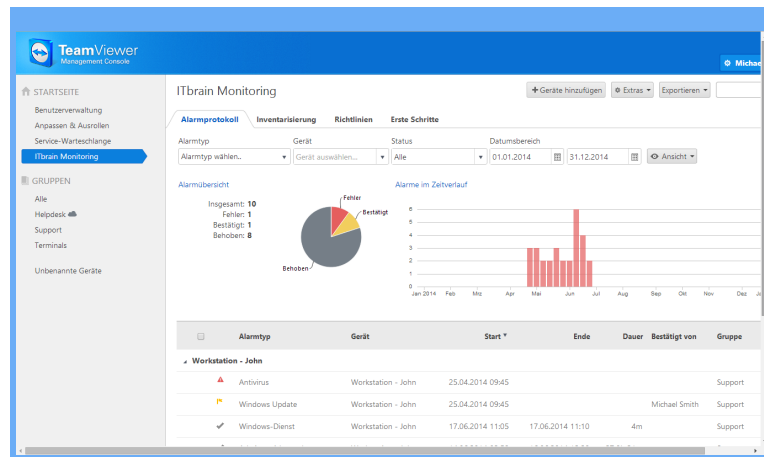
Die unter [Abschnitt 3.2 "ITbrain für Endpunkte aktivieren", Seite 9](#) eingerichteten Geräte werden mit den unter [Abschnitt 3.3.1 "Richtlinien konfigurieren", Seite 12](#) zugewiesenen Richtlinien (Liste an Monitoring-Checks) geprüft und überwacht. Sobald alle definierten Bedingungen für einen Check erfüllt sind, wird ein Alarm ausgelöst und als Alarmmeldung in der TeamViewer Management Console und der TeamViewer Vollversion angezeigt. Eine Alarmmeldung symbolisiert ein Problem, das auf einem der überwachten Geräte aufgetreten ist.

## 4.1 Alarmprotokoll

Für alle Computer, auf denen Sie ITbrain nutzen, werden im Alarmprotokoll in der TeamViewer Management Console Alarmmeldungen angezeigt. Eine Alarmmeldung wird ausgelöst, sobald auf einem der Geräte Unregelmäßigkeiten festgestellt werden. Dies ist von den definierten ITbrain-Richtlinien abhängig.

Die **Standard-Monitoringrichtlinie** enthält folgende unter [Abschnitt 3.3.1 "Richtlinien konfigurieren", Seite 12](#) beschriebenen Monitoring-Checks:

- Ist eine **Antivirus**-Software installiert und aktiv?
- Sind mehr als 500 MB **Arbeitsspeicher** verfügbar?
- Ist die **CPU-Auslastung** höher als 75%?
- Wie ist der **Festplattenzustand**?
- Ist die freie **Speicherkapazität** geringer als 10%?
- Ist das **Windows-Update** aktiv?
- Ist die **Windows-Firewall** aktiviert?



Alarmmeldungen werden im Alarmprotokoll angezeigt.

Für alle Computer, die Sie mit ITbrain Monitoring und Inventarisierung überwachen, werden im Alarmprotokoll in der TeamViewer Management Console Alarmmeldungen angezeigt, falls einer der Checks einen Alarm auslöst.

Um das Alarmprotokoll aufzurufen, wählen Sie eine der Methoden:

- ➔ Klicken Sie in der Seitenleiste auf **ITbrain** und wählen Sie den Tab **Alarmprotokoll**. Wählen Sie anschließend einen **Alarmtyp**.
- ➔ Klicken Sie in der Seitenleiste auf eine Gruppe Ihrer Computer & Kontakte-Liste und wählen Sie den Tab **Alarmprotokoll**. Wählen Sie anschließend einen **Alarmtyp**.

Die Alarmmeldungen können in der Übersicht nach **Alarmtyp**, **Gerät**, **Status** und **Datumsbereich** gefiltert werden. Wenn Sie auf einen Eintrag in der Kopfzeile der Tabelle klicken, können Sie die Alarmmeldungen nach den Spalten sortieren. Über das Menü **Ansicht** können Sie festlegen, welche Spalten in der Tabelle angezeigt werden und die grafische Darstellung der Alarmmeldungen aktivieren oder deaktivieren.

Der Zustand der Alarmmeldungen wird durch unterschiedliche Symbole gekennzeichnet.

#### Symbol Beschreibung



Einer der definierten Checks hat eine Alarmmeldung ausgelöst. Diese wurde noch nicht bestätigt.



Die Alarmmeldung wurde durch Sie oder einen Kontakt, mit dem der Computer geteilt wurde, bestätigt.




Das Problem, das die Alarmmeldung ausgelöst hat, wurde behoben.

## 4.2 Alarmmeldungen bearbeiten


Falls Sie die Ursache einer Monitoring-Alarmmeldung kennen oder verifizieren können und die Problembehebung starten möchten, bestätigen Sie einzelne oder mehrere Alarmmeldungen.



Um eine Monitoring-Alarmmeldung zu bestätigen, wählen Sie eine der Methoden:

- ➡ Klicken Sie auf das Symbol  hinter einer Alarmmeldung und wählen Sie die Option **Bestätigen**.
- ➡ Wählen Sie alle Alarmmeldungen, die Sie bestätigen können und klicken Sie auf **Extras | Ausgewählte bestätigen**.


Nachdem eine ITbrain Monitoring-Alarmmeldung bestätigt ist, können Sie das Problem beheben, indem Sie eine Verbindung zu dem Computer herstellen.

- ➡ Klicken Sie dazu auf das Symbol  hinter einer Alarmmeldung und wählen Sie die Option **Zum Computer wechseln**. Anschließend können Sie wie gewohnt eine Verbindung zu dem Computer aufbauen.

## 4.3 Alarmmeldungen erneut prüfen

Falls Sie die Ursache einer Alarmmeldung behoben haben, können Sie mit ITbrain überprüfen, ob Ihre Bemühungen erfolgreich waren, und das Problem nicht weiterhin auftritt.

Um eine Alarmmeldung erneut zu prüfen, wählen Sie eine der Methoden:

- ➡ Klicken Sie auf das Symbol  hinter einer Alarmmeldung und wählen Sie die Option **Jetzt prüfen**.
- ➡ Wählen Sie alle Alarmmeldungen, die Sie prüfen möchten und klicken Sie auf **Extras | Ausgewählte prüfen**.



## 5 Inventarisierung

Nutzen Sie den ITbrain-Service **ITbrain Monitoring**, um Ihre Geräte zu überwachen und für die Inventarisierung.

Die unter [Abschnitt 3.2 "ITbrain für Endpunkte aktivieren"](#), [Seite 9](#) eingerichteten Geräte werden unabhängig von den Monitoring-Funktionen ebenfalls durch ITbrain inventarisiert. Die Inventarisierung verschafft einen Überblick über die verwendeten Komponenten auf allen Computern, auf denen ITbrain eingesetzt wird. Die inventarisierten Geräte werden in der TeamViewer Management Console aufgelistet.

Um die inventarisierten Komponenten aufzurufen, wählen Sie eine der Methoden:

- ➡ Klicken Sie in der Seitenleiste auf **ITbrain** und wählen Sie den Tab **Inventarisierung**.
- ➡ Klicken Sie in der Seitenleiste auf eine Gruppe Ihrer Computer & Kontakte-Liste und wählen Sie den Tab **Inventarisierung**.

Name	Version	Geändert am	Computer	Gruppe
airbackup		2014	Demo laptop	Support
Bonjour	2.0.4.0	09.01.2014	Workstation	Support
Configuration Manager Client	5.00.7804.1000	02.10.2013	Demo laptop	Support
DataMigrationTool	1.0.6	08.01.2013	Demo laptop	Support
Dell WLAN and Bluetooth Client Installation	10.0	12.09.2012	Workstation	Support
Google Chrome	33.0.1750.117	17.12.2013	Demo laptop	Support
Google Update Helper	1.3.22.5	12.02.2014	Demo laptop	Support
Intel(R) Control Center	1.2.1.1007		Workstation	Support
Intel(R) Management Engine Components	8.0.1.1399		Workstation	Support
Intel(R) Processor Graphics	9.17.10.2849		Workstation	Support
Intel(R) Rapid Storage Technology	11.1.0.1006		Workstation	Support

Alle inventarisierten Komponenten im Überblick.

### 5.1 Berichte

Die Komponenten der inventarisierten Geräte werden kategorisiert als Berichte dargestellt. Im Folgenden finden Sie eine Beschreibung der verfügbaren Berichte.



Bericht	Beschreibung
<b>Software</b>	Übersicht der auf den Geräten installierten Anwendungen inklusive der Software-Version.
<b>Updates</b>	Übersicht der durchgeführten Windows-Updates und wann diese installiert wurden.
<b>Hardware</b>	Übersicht der verbauten Hardware-Komponenten (inkl. <b>Typ</b> , <b>Name</b> und <b>Hersteller</b> ). Diese Übersicht enthält alle im Folgenden aufgeführten Berichte.
<b>Prozessor</b>	Übersicht der in den Geräten verbauten Prozessoren (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Mainboard</b>	Übersicht der in den Geräten verbauten Mainboards (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>BIOS</b>	Übersicht der in den Geräten verbauten BIOS (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Physikalischer Speicher</b>	Übersicht der in den Geräten verbauten Arbeitsspeicher (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Cache</b>	Übersicht des in den Geräten verwendeten Cache (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Laufwerk</b>	Übersicht der in den Geräten verbauten Festplatten (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Optisches Laufwerk</b>	Übersicht der in den Geräten verbauten Laufwerke (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Logischer Datenträger</b>	Übersicht der in den Geräten verwendeten logischen Datenträger (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Diskettenlaufwerk</b>	Übersicht der in den Geräten verbauten Diskettenlaufwerken (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Bandlaufwerk</b>	Übersicht der in den Geräten verbauten Bandlaufwerke (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Videocontroller</b>	Übersicht der in den Geräten verbauten Grafikkarten (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).



Bericht	Beschreibung
<b>Aktiver Monitor</b>	Übersicht der an die Geräte angeschlossenen Monitore (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Netzwerk</b>	Übersicht der in den Geräten verbauten Netzwerkkarten (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Tastatur</b>	Übersicht der an die Geräte angeschlossenen Tastatur (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Zeigegerät</b>	Übersicht der an die Geräte angeschlossenen Eingabegeräte (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).
<b>Audiogerät</b>	Übersicht der in den Geräten verbauten Soundkarten (inkl. <b>Name</b> , <b>Details</b> und <b>Hersteller</b> ).



## 6 Anti-Malware

Nutzen Sie den ITbrain-Dienst **ITbrain Anti-Malware**, um Ihre Geräte auf Schadsoftware zu überprüfen.

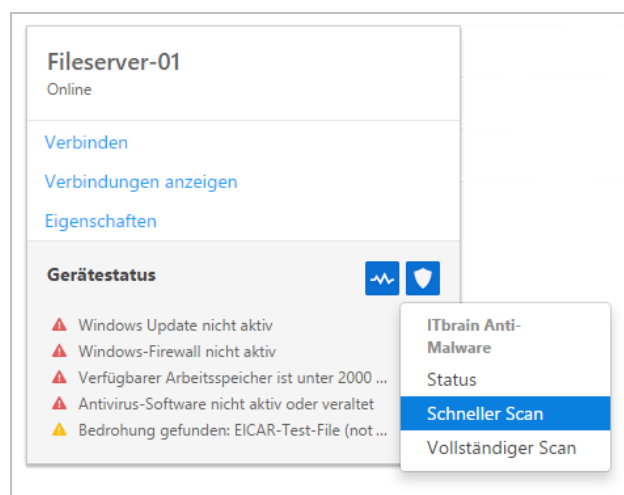
Die unter [Abschnitt 3.2 "ITbrain für Endpunkte aktivieren", Seite 9](#) eingerichteten Geräte werden mit den unter [Abschnitt 3.3.1 "Richtlinien konfigurieren", Seite 12](#) zugewiesenen Richtlinien (Liste an Scans) geprüft und geschützt.

Sobald eine Schadsoftware auf dem Gerät entdeckt wird, wird ein Alarm ausgelöst und als Alarmmeldung in der TeamViewer Management Console und der TeamViewer Vollversion angezeigt. Eine Alarmmeldung symbolisiert einen Malware-Fund auf einem Ihrer Geräte.

### 6.1 Manuelle Scans

Starten Sie für einzelne Endpunkte manuelle Scans. Unabhängig von geplanten Scans durch die Anti-Malware-Richtlinien überprüfen Sie die Endpunkte jederzeit auf Schadsoftware.

Ein manueller Scan kann, für Geräte die online sind, aus der TeamViewer Management Console oder der TeamViewer Vollversion gestartet werden.



Manueller Scan eines Endpunktes

Wählen Sie eine der folgenden Methoden, um einen manuellen Anti-Malware-Scan zu starten:

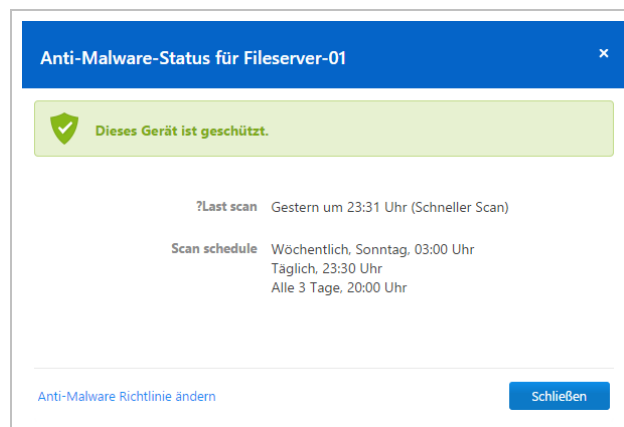


- ➔ Klicken Sie in der TeamViewer Management Console auf den Namen des Endpunktes und wählen Sie die Option | **Schneller Scan** oder | **Vollständiger Scan**.
- ➔ Klicken Sie in der TeamViewer Vollversion im Kontextmenü (rechte Maustaste) des Endpunktes auf | **Schneller Scan** oder | **Vollständiger Scan**

## 6.2 Status der Geräte

Rufen Sie für alle Endpunkte einen Status der Anti-Malware-Scans ab. Der Status enthält Informationen zum Zeitpunkt des letzten und nächsten Scans, sowie allgemeine Angaben zum Schutz des Gerätes.

- ➔ Klicken Sie auf den Namen eines Gerätes und wählen Sie im Kontextmenü die Option | **Status**.



Der Dialog **Anti-Malware-Status für <GERÄTENAME>**.

Im Dialog **Anti-Malware-Status für <GERÄTENAME>** werden folgende Informationen dargestellt:

### Beschreibung

<b>Status</b>	<p>Der Status des Gerätes ist farblich gekennzeichnet.</p> <ul style="list-style-type: none"> <li>• <b>Grün:</b> Der Endpunkt ist geschützt.</li> <li>• <b>Gelb:</b> Kleinere Probleme, beispielsweise alte Malware-Definitionen oder ein geplante Scan wurde nicht durchgeführt.</li> <li>• <b>Rot:</b> Andauerndes Problem, beispielsweise Malware wurde gefunden, jedoch nicht beseitigt.</li> </ul>
<b>Letzter Scan</b>	Datum des letzten Scans, inkl. Scantyp.
<b>Geplante Scans</b>	Alle geplanten Scans für den Endpunkt gemäß Anti-Malware-Richtlinie.





## 6.3 Alarmprotokoll

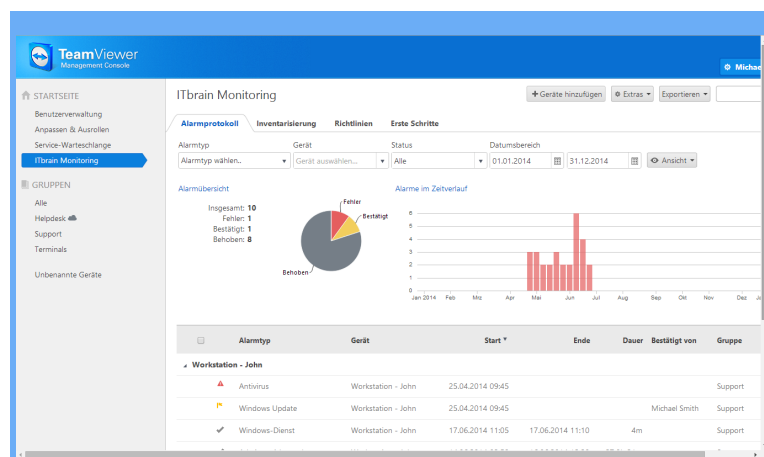
Für alle Computer, auf denen Sie ITbrain nutzen, werden im Alarmprotokoll in der TeamViewer Management Console Alarmmeldungen angezeigt. Eine Alarmmeldung wird ausgelöst, sobald auf einem der Geräte Unregelmäßigkeiten festgestellt werden. Dies ist von den definierten ITbrain-Richtlinien abhängig.

Die **Standard-Anti-Malware-Richtlinie** enthält folgende unter [Abschnitt 3.3.1 "Richtlinien konfigurieren"](#), [Seite 12](#) beschriebenen Scans:

- Schneller Scan, täglich 09:00Uhr
- Vollständiger Scan, täglich 12:00Uhr

Um das Alarmprotokoll aufzurufen, wählen Sie eine der Methoden:

- ➔ Klicken Sie in der Seitenleiste auf **ITbrain** und wählen Sie den Tab **Alarmprotokoll**. Wählen Sie anschließend einen **Alarmtyp**.
- ➔ Klicken Sie in der Seitenleiste auf eine Gruppe Ihrer Computer & Kontakte-Liste und wählen Sie den Tab **Alarmprotokoll**. Wählen Sie anschließend einen **Alarmtyp**.



Alarmmeldungen werden im Alarmprotokoll angezeigt.

Die Alarmmeldungen können in der Übersicht nach **Alarmtyp**, **Gerät**, **Status** und **Datumsbereich** gefiltert werden. Wenn Sie auf einen Eintrag in der Kopfzeile der Tabelle klicken, können Sie die Alarmmeldungen nach den Spalten sortieren. Über das Menü **Ansicht** können Sie festlegen, welche Spalten in der Tabelle angezeigt werden und die grafische Darstellung der Alarmmeldungen aktivieren oder deaktivieren.

Falls bei einem Scan eine Bedrohung entdeckt wird, wird die entdeckte Schadsoftware umgehend in einen Quarantäne-Ordner verschoben. Dort kann sie keinen weiteren Schaden anrichten. Zusätzlich wird an die E-Mail-Adressen, die für die Richtlinie definiert wurden, eine E-Mail-Benachrichtigung gesendet.

Der Zustand der Alarmmeldungen wird durch unterschiedliche Symbole gekennzeichnet.



## Symbol Beschreibung



Auf dem Gerät wurde Schadsoftware entdeckt. Die Bedrohung konnte nicht unschädlich gemacht oder in die Quarantäne verschoben werden.

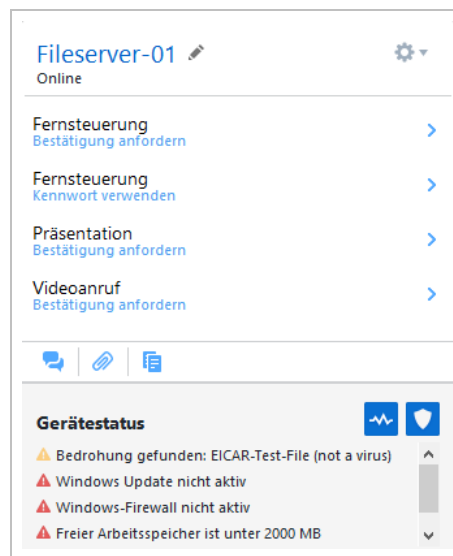
**Achtung:** Wenden Sie sich in diesem Fall an den ITbrain Support.



Auf dem Gerät wurde Schadsoftware entdeckt. Die Bedrohung wurde unschädlich gemacht und in die Quarantäne verschoben.



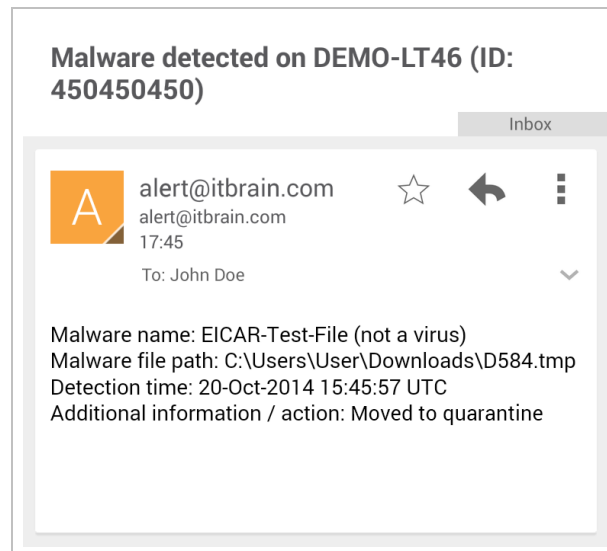
Sie haben die Bedrohung bestätigt. Die Bedrohung wird nicht mehr angezeigt.



Alarmmeldung für Schadsoftware in der Computer & Kontakte-Liste.



Alarmmeldung für Schadsoftware in der TeamViewer Management Console.



E-Mail-Benachrichtigung für Schadsoftware.

## 6.4 Bedrohung bestätigen


Bedrohungen (Schadsoftware), die während eines Scans gefunden werden, werden im Alarmprotokoll aufgelistet und können dort bestätigt werden.

Bestätigen Sie eine Alarmmeldung, wenn Sie die Bedrohung kennen oder verifizieren können und die Problembehebung starten.

Falls Sie eine Bedrohung bestätigen, wird die Bedrohung nicht mehr in den Benachrichtigungen des Gerätes angezeigt und mit einem Haken im Alarmprotokoll dargestellt.

**Beispiel:** Eine Schadsoftware wird bei einem Scan entdeckt. Sie als Administrator des Gerätes bekommen per E-Mail die entsprechende Benachrichtigung. In der TeamViewer Management Console überprüfen Sie die Benachrichtigung. Nachdem Sie nun wissen, um welche Bedrohung es sich handelt bestätigen Sie den Fund der Schadsoftware und leiten gegebenenfalls Maßnahmen ein, um solche Funde zukünftig zu vermeiden.

Um eine Bedrohung zu bestätigen, wählen Sie eine der Methoden:

- ➡ Klicken Sie auf das Symbol  hinter einer Alarmmeldung und wählen Sie die Option **Bestätigen**.
- ➡ Wählen Sie alle Alarmmeldungen, die Sie bestätigen können und klicken Sie auf **Extras | Ausgewählte bestätigen**.

**Hinweis:** Die Schadsoftware verbleibt auch nach Bestätigung weiterhin in Quarantäne. Löschen Sie die Schadsoftware nach eigenem Ermessen von dem Gerät.


**Tipp:** Es ist ebenso möglich, einen Bedrohung in der Computer & Kontakte-Liste (TeamViewer Vollversion und TeamViewer Management Console) zu bestätigen.

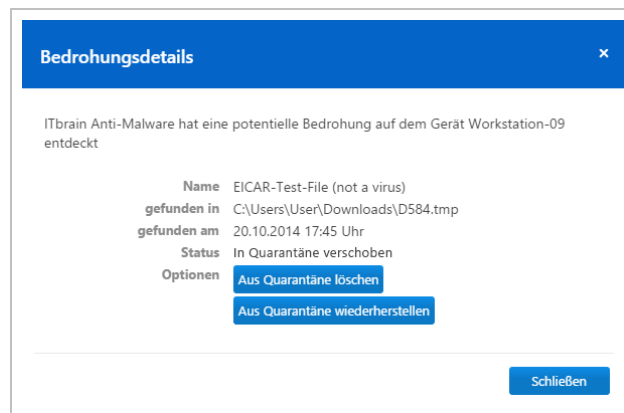


## 6.5 Details zur Bedrohung

Sie können detaillierte Informationen zu Schadsoftware anzeigen, die bei einem durchgeführten Scan gefunden wurden. Erfahren Sie, um welche Art von Schadsoftware es sich handelt und schätzen Sie das Bedrohungspotential besser ein.

Um Details zu einer Bedrohung aufzurufen, wählen Sie eine der Methoden:

- ➔ Klicken Sie auf das Symbol  hinter einer Alarmmeldung und wählen Sie die Option **Details**.
- ➔ Wählen Sie alle Alarmmeldungen, die Sie bestätigen können und klicken Sie auf **Extras | Details**.



Der Dialog **Bedrohungsdetails**.

Folgende Informationen werden im Dialog **Bedrohungsdetails** angezeigt.

Beschreibung	
<b>Gerät</b>	Name des Gerätes auf dem die Schadsoftware gefunden wurde.
<b>Name</b>	Name der Schadsoftware.
<b>Gefunden in</b>	Pfad oder Datei, in dem/der die Schadsoftware gefunden wurde.
<b>Gefunden am</b>	Zeitpunkt, an dem die Schadsoftware gefunden wurde.



## Beschreibung

---

**Optionen** Wählen Sie, wie mit der Schadsoftware weiter umgegangen wird.

- **Aus Quarantäne löschen:** Klicken Sie auf die Schaltfläche, um die Schadsoftware permanent aus der Quarantäne zu entfernen und zu löschen.
- **Aus Quarantäne wiederherstellen:** Klicken Sie auf die Schaltfläche, um die Schadsoftware wieder an ihrem ursprünglichen Ort abzulegen und aus der Quarantäne zu entfernen.

**Achtung:** Stellen Sie Schadsoftware nur wieder-her, falls Sie sich absolut sicher sind, dass die Datei keinen Schaden auf dem Gerät anrichten kann.