Vodafone Business CyberWall

Uživatelská příručka pro PC

Together we can
vodafone
business

Obsah

Vodafone Business CyberWall pro PC je nezávislé bezpečnostní řešení pro ochranu koncových bodů. Je k dispozici pro PC a obsahuje řešení pro tři oblasti ochrany:

1. AntiVirus
2. Anti-Ransomware
3. Rozšíření pro Google Chrome (včetně ochrany před phishingovými útoky nultého dne (Zero-day Phishing Protection) a odstraňování hrozeb (Threat Extraction))

Celá technologie je napojena na Threat Cloud společnosti Check Point, jednu z největších světových sítí pro analýzu hrozeb, ze které získáváme data v reálném čase.

1. Instalace a aktivace

a. Aktivace CyberWall aktivačním kódem

Stáhněte si náš produkt a aktivujte ho.

Stáhněte si CyberWall do svého PC

Pokud jste již obdrželi v SMS odkaz na aktivaci CyberWallu, otevřete tento odkaz přímo v PC, na kterém ho chcete instalovat – tím se zahájí stahování souboru včetně licenčního klíče.

Pro bezpečné prohlížení internetových stránek pomocí rozšíření CyberWall Web Secure musíte mít nainstalovaný prohlížeč Google Chrome.

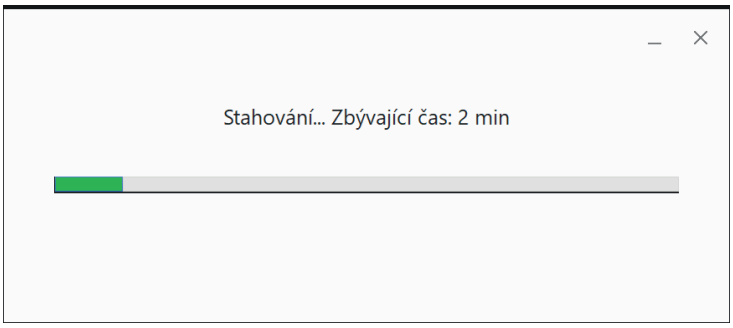
Chcete-li si nainstalovat prohlížeč Google Chrome, klikněte na následující odkaz: https://www.google.com/chrome/

Instalace

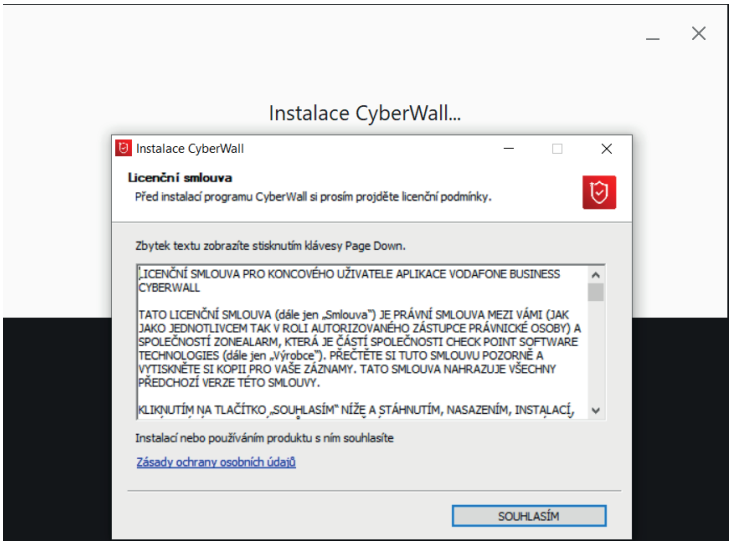
Instalaci provedete v následujících krocích:

1. Otevřete stažený soubor, a když vás systém Windows vyzve k povolení spuštění programu, klikněte na možnost **Ano** (Yes).
   CyberWall_Setup_CS

2. CyberWall začne stahovat aplikaci.



3. Na obrazovce obsahující Licenční smlouvu s koncovým uživatelem CyberWall (EULA) klikněte na možnost **Přijmout a nainstalovat** (Accept and Install).



4. Instalace bude pokračovat.

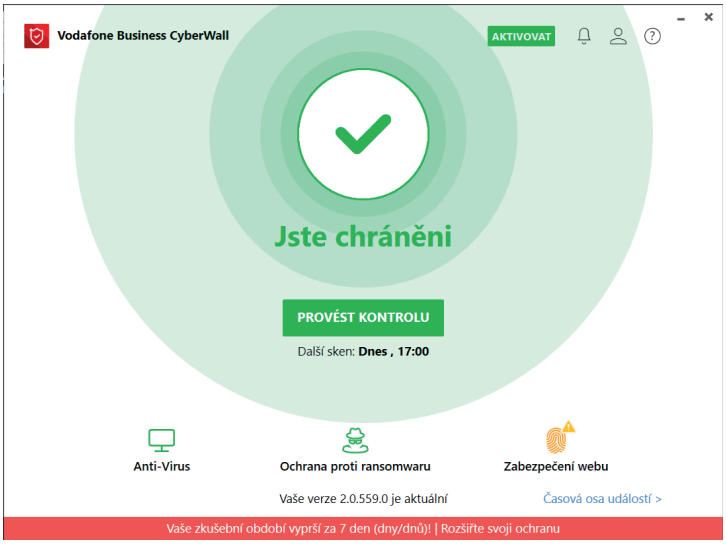
b. Aktivace CyberWall přímým odkazem

Pokud jste aplikaci instalovali přímo z námi dodaného odkazu, služba se aktivuje automaticky.

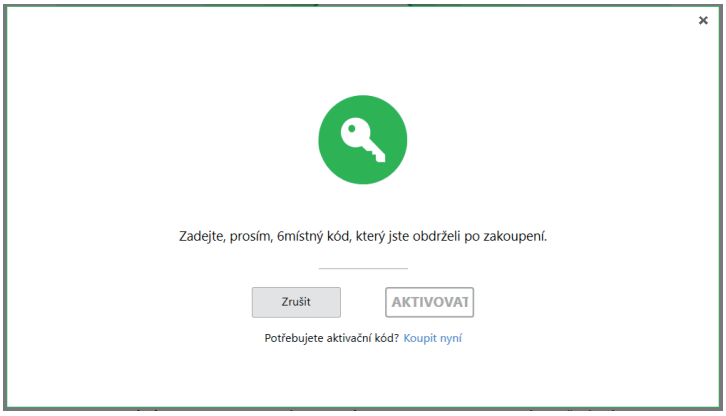
Pokud jste aplikaci stáhli bez našeho odkazu, je možné, že budete chráněni **7denní zkušební verzí**, nebo vám již platnost zkušební verze mohla vypršet. Ochrana Anti-Ransomware je ve výchozím nastavení automaticky **zapnutá**.

Pokud chcete používat funkce Safe Browsing a Web Secure, je třeba v prohlížeči Chrome nainstalovat a zapnout rozšíření CyberWall Web Secure.

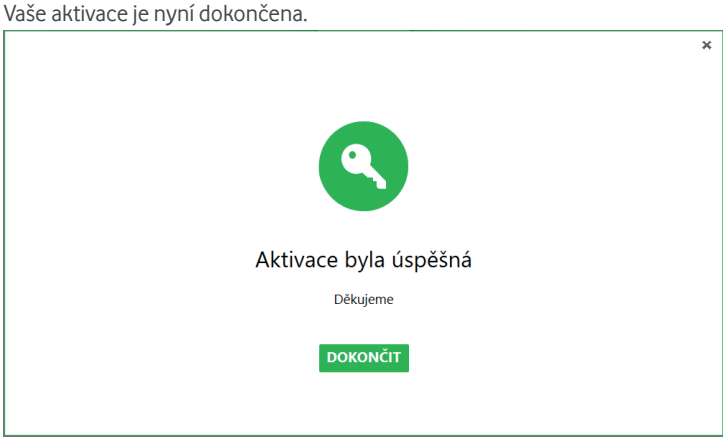
1. Chcete-li aktivovat předplatné, klikněte na možnost **Aktivovat** (Activate).



2. Zadejte šestimístný aktivační kód a klikněte na možnost **Aktivovat** (Activate). Pokud nemáte aktivační kód, kontaktujte naši Péči o zákazníky na tel.: 800 77 00 77 a my vám ho znovu zašleme.



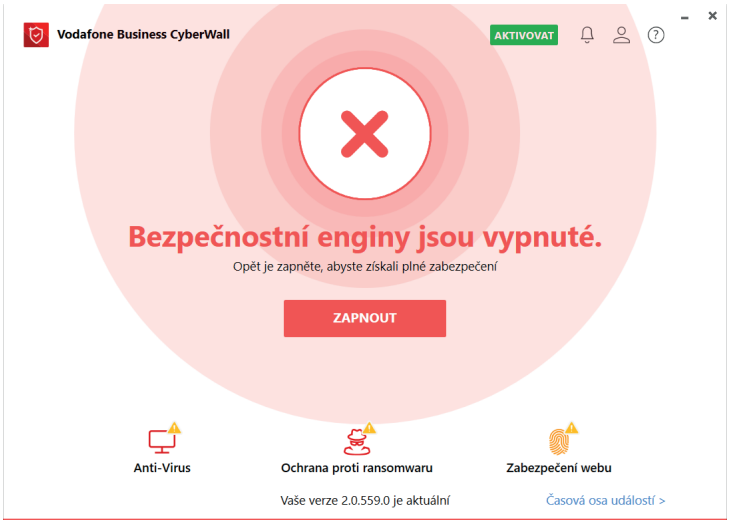
3. Vaše aktivace je nyní dokončena.



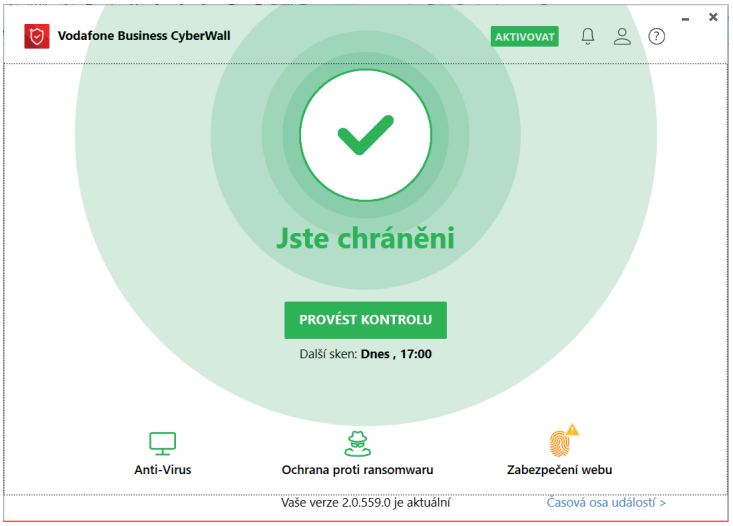
2. Hlavní panel

Při spuštění programu CyberWall se zobrazí hlavní panel. Na hlavním panelu se zobrazuje stav vašeho systému a aktuální úroveň zabezpečení. Kroky k zabezpečení vašeho systému jsou následující:

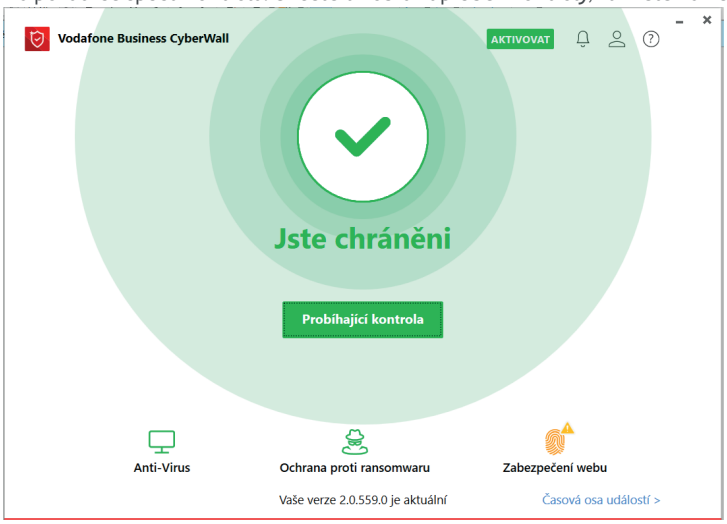
1. Pokud se vám zobrazí upozornění z programu CyberWall, klikněte na tlačítko **ZAPNOUT** (TURN ON).



2. Zobrazí se zpráva „Jste chráněni“ (You Are Protected). Na hlavním panelu můžete spustit kontrolu svého zařízení. Klikněte na možnost **Spustit kontrolu** (Scan).



3. Na pozadí se spustí kontrola. Chcete-li zobrazit průběh kontroly, klikněte na **Zobrazit spuštěnou kontrolu** (View Running Scan).

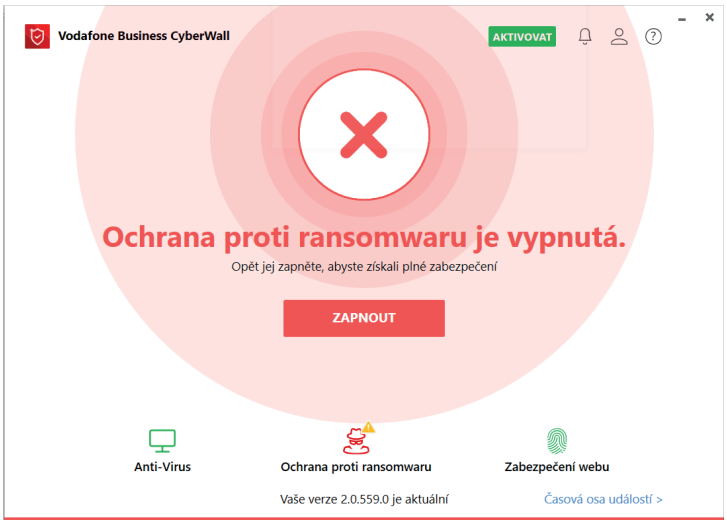


3. Anti-Ransomware

Anti-Ransomware odhaluje bloky, odstraňuje útoky ransomwaru a navíc obnovuje všechny šifrované soubory pomocí technologií založených na chování, které se nespoléhají na aktualizace virových signatur.

Jak funguje CyberWall Anti-Ransomware

CyberWall Anti-Ransomware využívá víceúrovňovou bezpečnostní architekturu a poskytuje komplexní řešení.



Úroveň 1: Analýza chování ransomwaru

Přizpůsobená analýza chování v reálném čase, která identifikuje většinu ransomwaru ještě dříve, než začne šifrovat data. Účelově vytvořené pokročilé algoritmy průběžně provádí behaviorální analýzu všech aktivit v operačním systému se zvláštním důrazem na detekci konkrétního chování ransomwaru.

Úroveň 2: Identifikace neoprávněného šifrování dat

Identifikuje ransomware, který se dokázal vyhnout počáteční analýze chování a začal šifrovat data.

» Nezávislý modul pro sledování souborů hledá důkazy o tom, že datové soubory, jako např. dokumenty a obrázky, jsou neoprávněně a systematicky šifrovány.

» Modul pro sledování souborů pečlivě sleduje všechny změny souborů a kontroluje, které procesy modifikují datové soubory a jakým způsobem. Je navržen tak, aby rozlišoval mezi oprávněnými a neoprávněnými aktivitami.

» Pokud ransomware aktivně šifruje data, algoritmy modulu tuto aktivitu rychle odhalí.

Úroveň 3: Automatizovaná forenzní analýza a umístění škodlivého softwaru (malwaru) do karantény

Odhalený ransomware je automaticky analyzován a umístěn do karantény.

» Když výše popsané moduly (úroveň 1 a 2) odhalí ransomware (nebo jiný malware), automaticky se spustí forenzní analýza.

» Analýza začíná odhalením indikátoru kompromitace (IOC), od kterého se analýza odvíjí.

Forenzní analýza využívá špičkové schopnosti nástroje Anti-Ransomware automaticky sledovat aktivitu související s útokem a analyzovat všechny její prvky za účelem identifikace celého modelu útoku.

» Vygenerovaný model útoku zahrnuje identifikaci škodlivých prvků a aktivit Ransomwaru.

» Díky programu CyberWall Anti-Ransomware a jeho schopnosti odstraňovat škodlivý software budou všechny škodlivé součásti malwaru identifikované vygenerovaným forenzním modelem útoku ukončeny a umístěny do karantény.

Úroveň 4: Obnova dat

Data se automaticky zálohují a obnovují v případě, že šifrování začne před identifikací ransomwaru.

» Před tím, než mohou být datové soubory modifikovány, se automaticky pořizují jejich snapshoty.

» Následující pravidla pomáhají minimalizovat kapacitu úložiště vyžadovanou pro ukládání těchto snapshotů:

  a. Snapshot souboru se pořizuje pouze v případě podezření, že došlo k neoprávněnému pokusu o jeho modifikaci. Snapshoty souborů mohou být uchovávány pouze do doby, než bude rozhodnuto o povaze modifikace. Pokud se nejedná o ransomware, mohou být snapshoty smazány.

  b. Uživatelé obvykle modifikují datové soubory jen velmi málo.

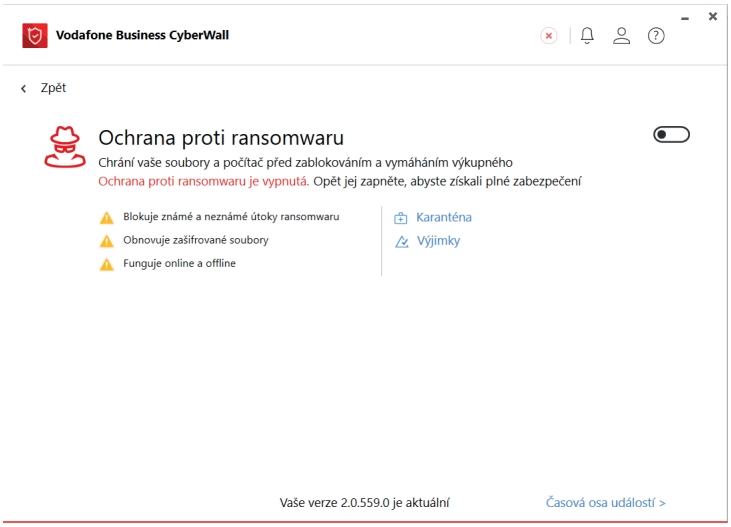
  c. Uchovávání záznamů o úpravách souborů pouze po krátkou dobu je dostačující.

» Anti-Ransomware nepřidělí pro snapshoty souborů na disku větší kapacitu než 2 GB. Ve většině případů je potřeba mnohem méně místa.

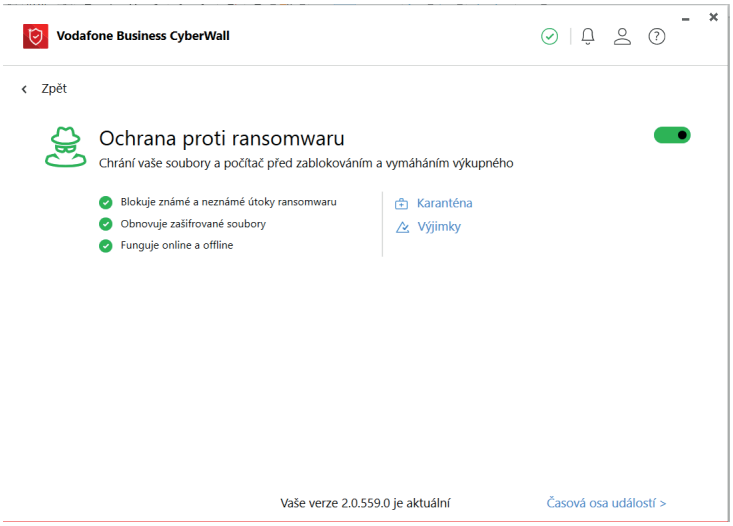
» Snapshoty datových souborů jsou uloženy v systému souborů koncového bodu a chráněny před nedovolenou manipulací pomocí zabezpečení koncových bodů Check Point Endpoint obsahujícího ovladače jádra s vnitřní ochranou.

» Poté co výše popsaná úroveň zabezpečení 3 umístí malware do karantény, dojde k automatické obnově datových souborů ze snapshotů.

Klikněte na ikonu **Anti-Ransomware**.



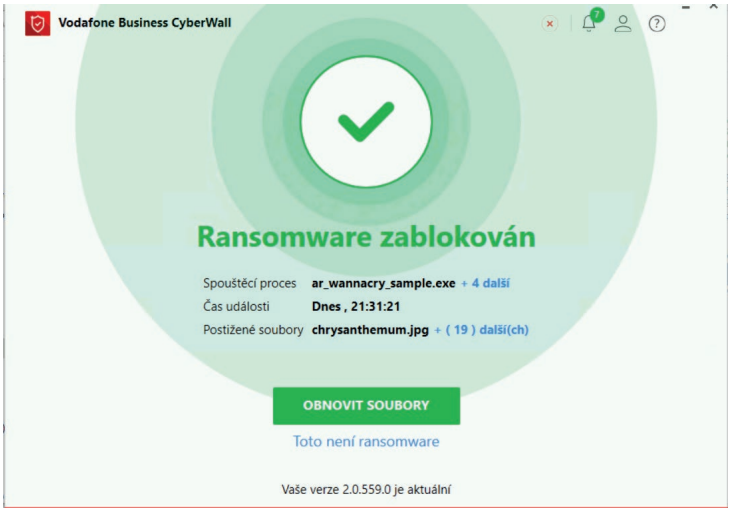
Kliknutím na **přepínací** tlačítko povolíte nebo zakážete Anti-Ransomware ve svém zařízení.



Anti-Ransomware je nyní aktivní.

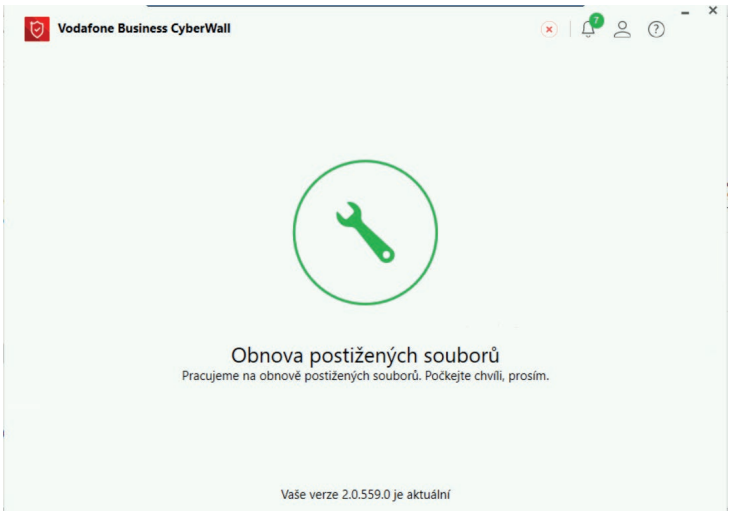
a. Detekce výskytu ransomwaru (Anti-Ransomware)

Když je Anti-Ransomware aktivní, CyberWall odhalí přítomnost ransomwaru a upozorní vás na ni, kdykoli se nějaký ransomware pokusí na vaše zařízení zaútočit.

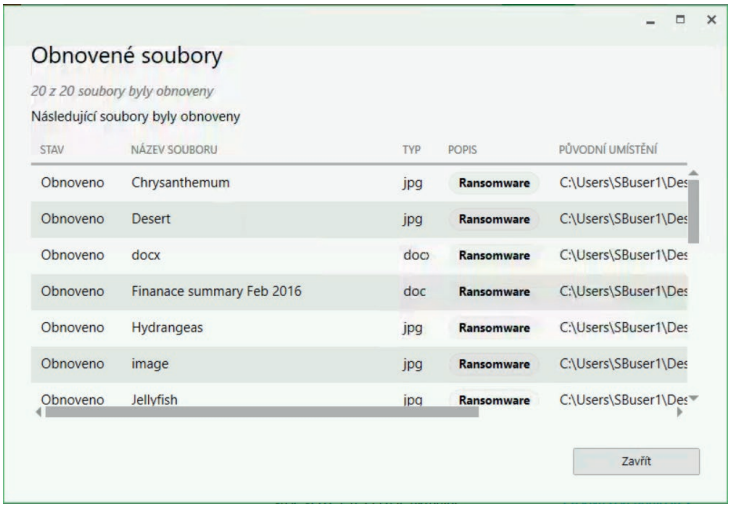


CyberWall ransomware automaticky zablokuje. Pomáhá také obnovit soubory šifrované/blokované ransomwarem. Klikněte na možnost **Obnovit postižené soubory** (Recover Affected Files).

Proces obnovy souborů se spustí na pozadí a zobrazí se následující zpráva.

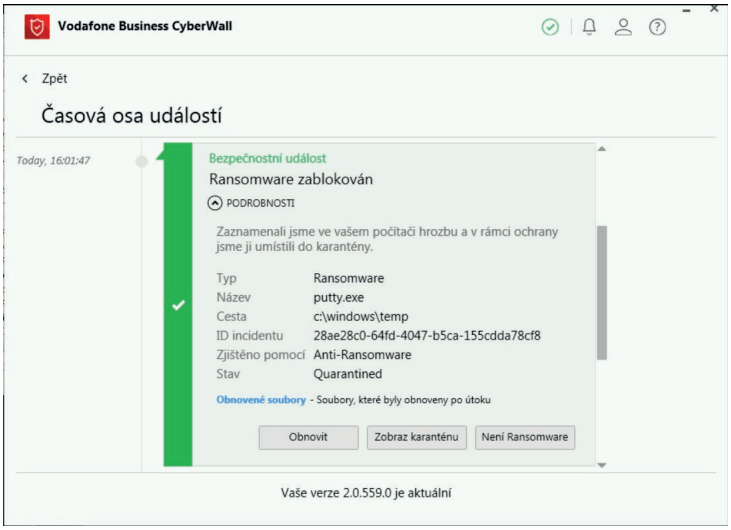


Poté se zobrazí tabulka se seznamem **Obnovených souborů** (Recovered Files).



b. Scénář – útok ransomwaru

Nyní se podívejme na možný scénář útoku ransomwaru a na to, jak ho nástroj CyberWall Next Generation pomůže zablokovat a obnovit soubory.



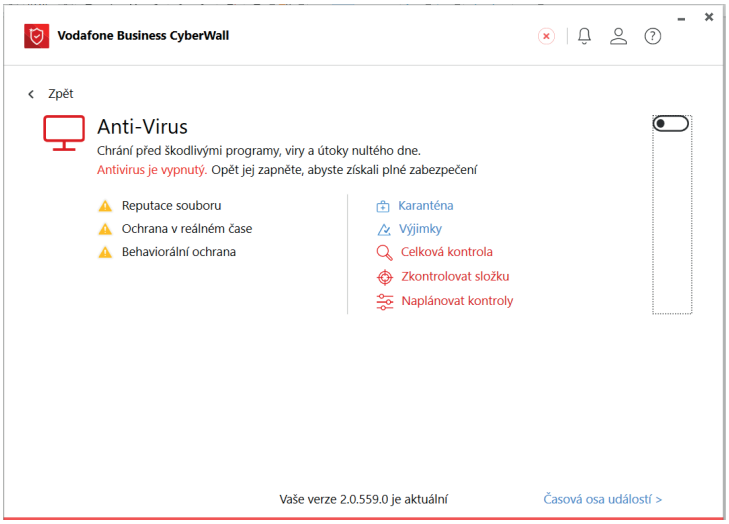
4. AntiVirus

CyberWall je komplexní víceúrovňová sada zabezpečení, která zastaví i nejsofistikovanější viry a hackery. Jedná se o konečné řešení pro vaše digitální zabezpečení, které vám zajistí 100% ochranu.

Jak CyberWall AntiVirus funguje

Klikněte na ikonu **AntiVirus**.

Chcete-li AntiVirus zapnout, po zobrazení okna klikněte na **přepínací** tlačítko.

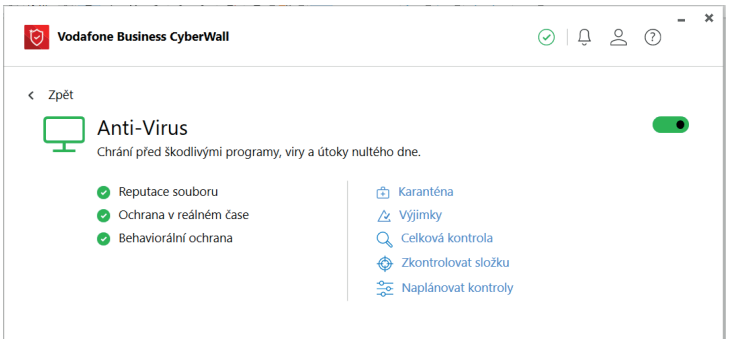


CyberWall AntiVirus je povolen.

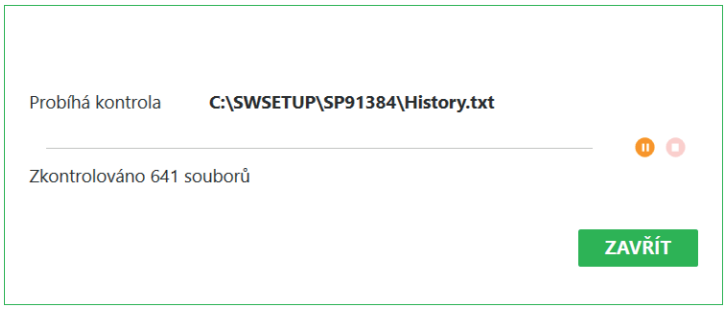
a. Celková kontrola

Celková kontrola prověří všechny soubory a složky ve vašem systému. Kroky k provedení celkové kontroly jsou následující:

1. Klikněte na možnost **AntiVirus** a poté vyberte možnost **Celková kontrola** (Full Scan).



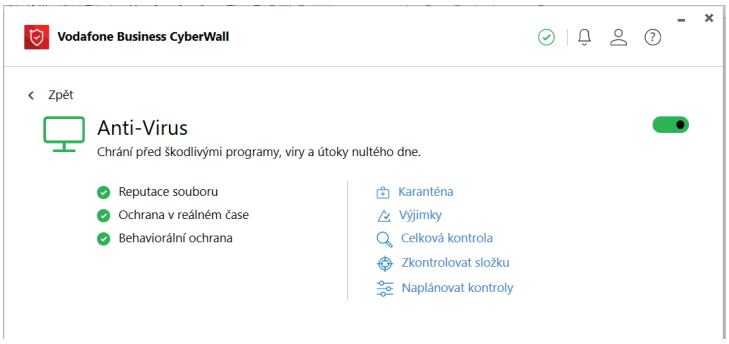
2. Na obrazovce se zobrazí průběh kontroly včetně všech prověřovaných souborů a složek. Doporučujeme nepřerušovat ani neukončovat probíhající kontrolu.



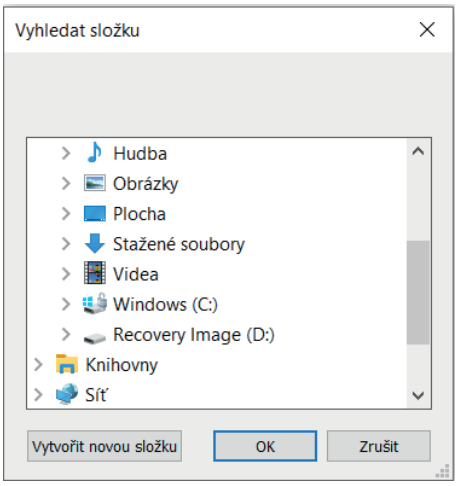
3. Po dokončení kontroly se zobrazí upozornění **Kontrola byla úspěšně dokončena** (Scan Completed Successfully).

b. Kontrola složky

CyberWall umožňuje spustit kontrolu konkrétní složky/složek dle vašich požadavků. Klikněte na možnost **AntiVirus** a poté vyberte možnost **Kontrola složky** (Scan a Folder).

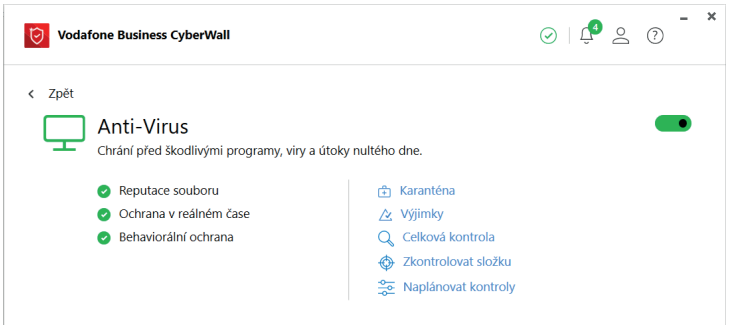


Složky, které chcete zkontrolovat, vyberte ve vyskakovacím okně a spusťte kontrolu stejným způsobem, jaký je uveden výše.

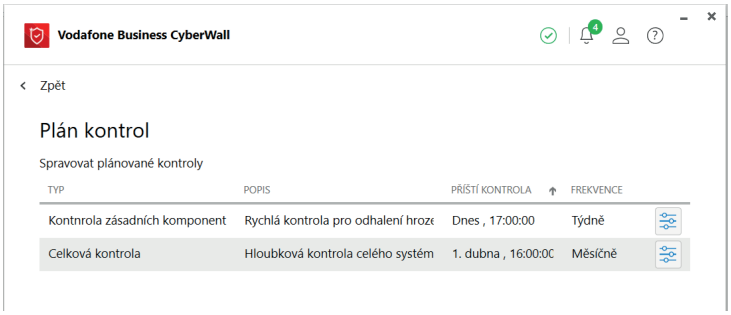


c. Naplánované kontroly

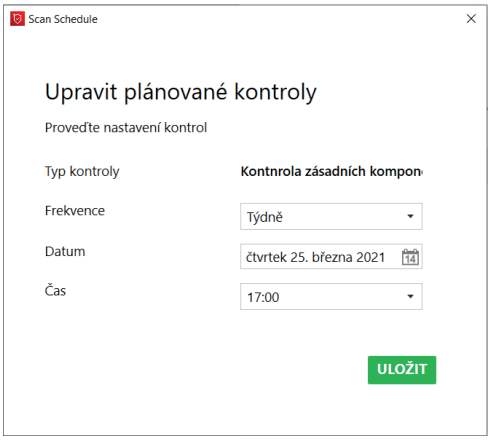
Kontroly lze naplánovat požadovanou četnost kontrol a jejich opakování. Chcete-li zobrazit naplánované kontroly, klikněte na možnost **Naplánované kontroly** (Schedule Scans).



Zobrazí se seznam naplánovaných kontrol. V seznamu **Naplánované kontroly** (Scan Schedule) se zobrazuje typ kontroly, její popis a další naplánovaná kontrola spolu s její četností.



Chcete-li naplánované kontroly upravit, klikněte na ikonu **Upravit**.



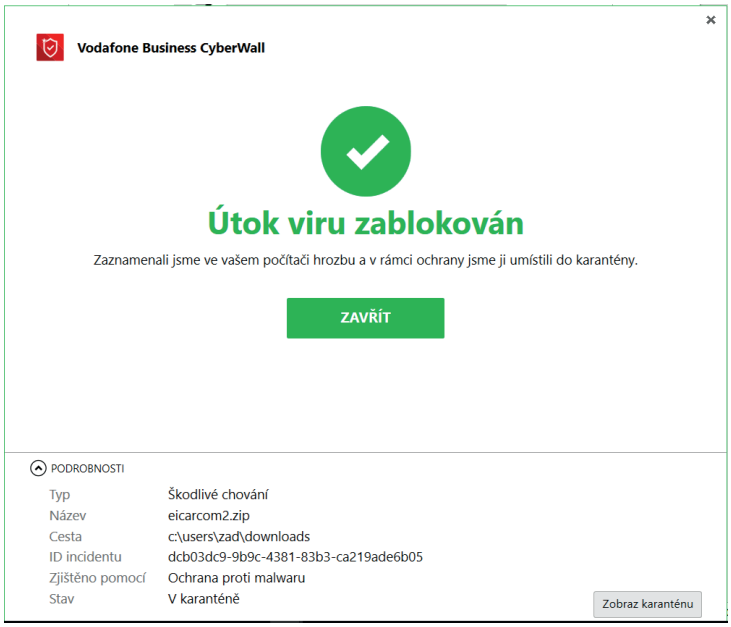
Zobrazí se **Naplánované kontroly**. Četnost kontrol (jednou za den, týden, měsíc atd.) lze nastavit v rozbalovací nabídce. Datum lze nastavit kliknutím na den ve vyskakovacím kalendáři. Čas kontroly lze nastavit obdobně po kliknutí na rozbalovací nabídku. Kliknutím na tlačítko **Uložit** (Save) změny uložíte.

d. Detekce výskytu malwaru (Anti-Malware)

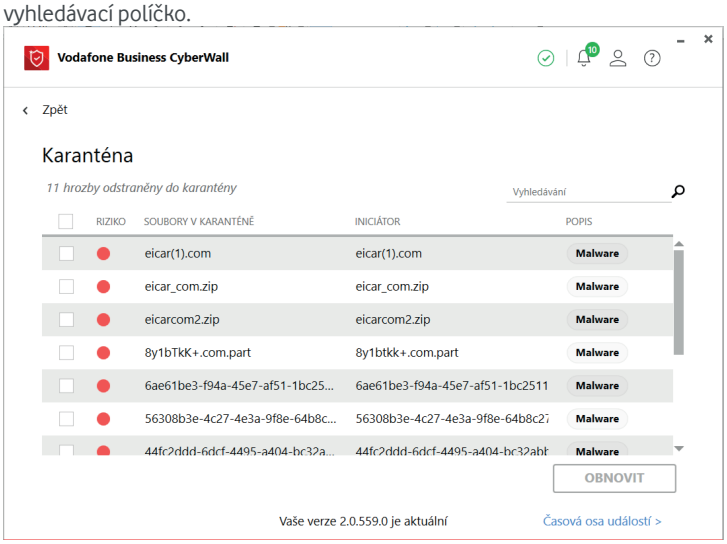
V této části jsou popsány kroky, které budou provedeny při detekci malwaru.

1. **Detekce malwaru**: Při detekci malwaru se zobrazí následující upozornění od CyberWall:

2. **Virový útok zablokován**: Dále je hrozba umístěna do karantény a po kliknutí na záložku **Podrobnosti** (Details) lze zobrazit **Typ** souboru (Type), jeho **Název** (Name), **Umístění** (Path), **Identifikační číslo výskytu** (Incident ID), **Stav** (Status) a jak byl **Odhalen** (Detected By).



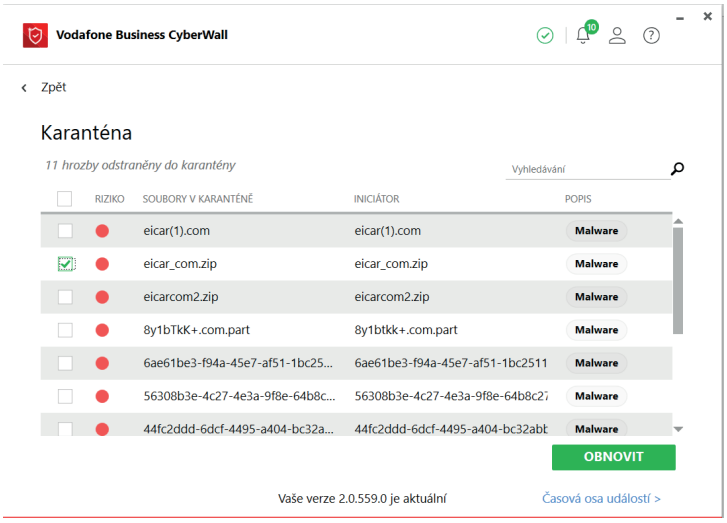
3. **Zobrazit karanténu**: Pro rychlý přístup do složky Karanténa klikněte na tlačítko **Zobrazit karanténu** (View Quarantine). Tato složka obsahuje veškerý odhalený malware. Pro výběr a další manipulaci s konkrétním souborem či několika soubory umístěnými v karanténě lze využít vyhledávací políčko.



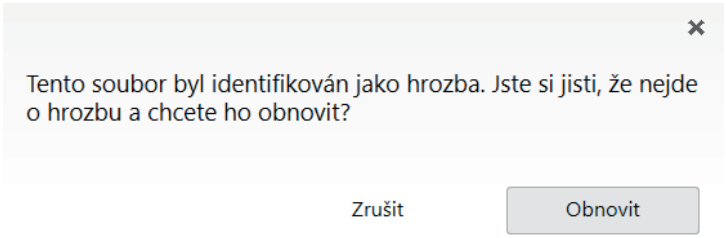
e. Chybné hlášení infikovaných souborů a jejich obnova

Když má CyberWall podezření, že je určitý soubor infikován virem, umístí ho do karantény. Soubory v karanténě lze obnovit, pokud jsou získány z důvěryhodného zdroje a byly chybně nahlášeny jako infikované.

Chcete-li z karantény obnovit soubor, o kterém se domníváte, že pochází z důvěryhodného zdroje, označte ho a klikněte na tlačítko **Obnovit** (Restore).

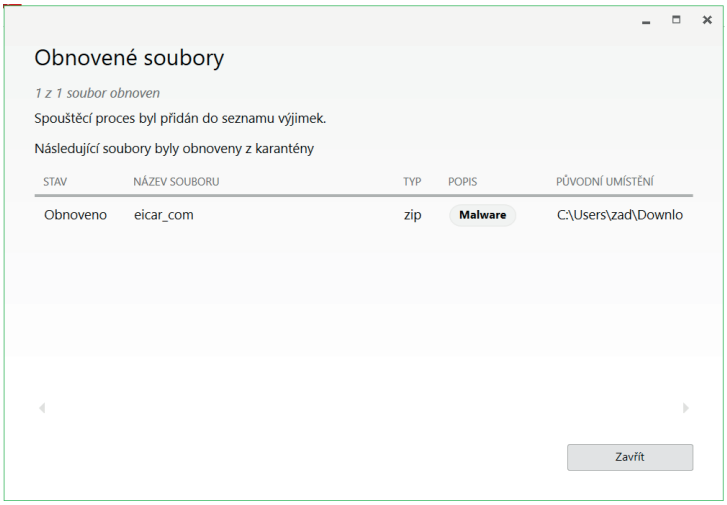


Obnovu potvrďte ve vyskakovacím okně kliknutím na tlačítko **Obnovit** (Restore).



Spustí se proces obnovení vybraného souboru.

Po dokončení se na obrazovce zobrazí potvrzovací zpráva o stavu souboru, jeho název, typ, popis a původní umístění.



CyberWall provede následující úkony:

1. Přidá spouštěcí proces tohoto souboru do Seznamu výjimek. To znamená, že signatura souboru bude uvedena na seznamu povolených signatur pro případy, kdy budou v budoucnu opět stahovány podobné soubory.
2. Skutečný soubor je obnoven z karantény do příslušné složky v počítači.

Tyto kroky provádí jak AntiVirus, tak Anti-Ransomware.

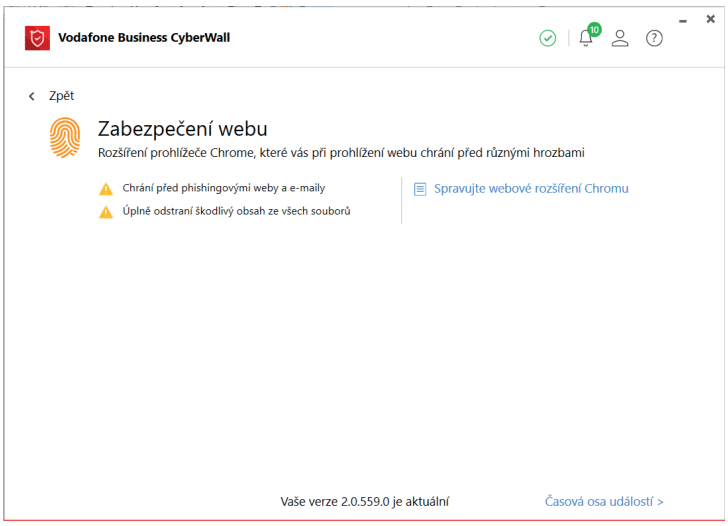
5. Rozšíření pro Chrome

Funkce Web Secure se týká pouze uživatelů, kteří používají webový prohlížeč Chrome. Poskytuje vašemu prohlížeči a aktivitám na internetu nejnovější ochranu před hrozbami Nultého dne (ZeroDay Protection). Rozšíření Web Secure Chrome Extension vás ochrání před škodlivými stránkami a phishingovými útoky. Jedná se o tzv. plugin třetí strany, společnosti ZoneAlarm.

Jak funguje Web Secure

Web Secure funguje ve dvou úrovních ochrany:

1. Ochrana před phishingovými útoky (Anti-Phishing)
2. Odstraňování hrozeb (Threat Extraction)

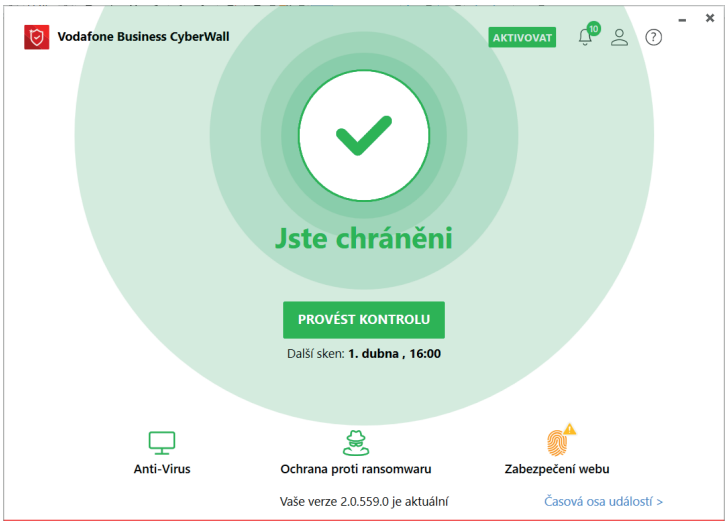


a. Web Secure

Povolení rozšíření Web Secure pro Chrome

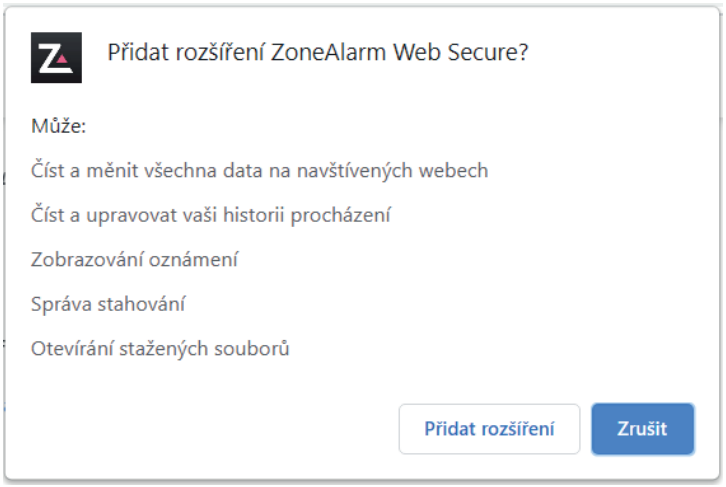
K povolení rozšíření Web Secure pro Chrome proveďte následující kroky:

1. Klikněte na ikonu **Web Secure**.



2. Pro zabezpečení svého internetového prohlížeče klikněte na odkaz **Instalovat webové rozšíření Chrome** (Install Chrome Web Extension).

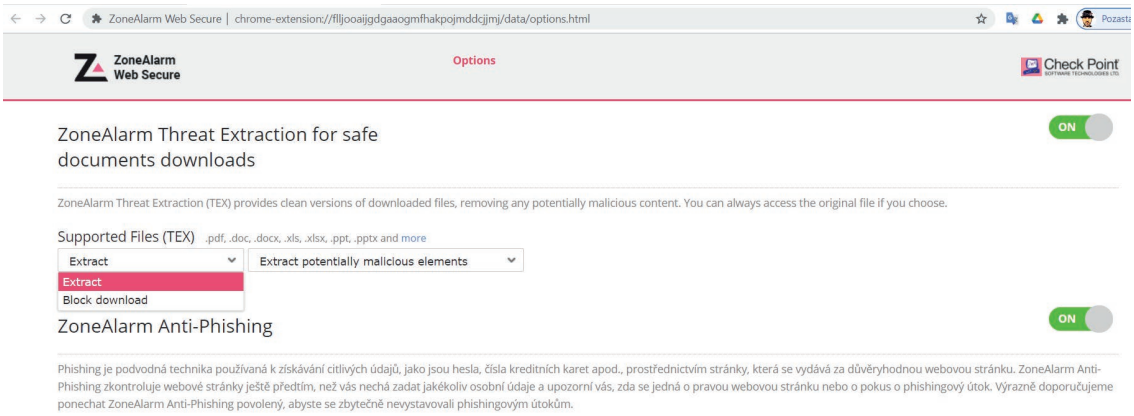
3. Spustí se prohlížeč Chrome a budete přesměrováni na rozšíření ZoneAlarm Web Secure pro Chrome v internetovém obchodě Web Store. Klikněte na možnost **Přidat do Chromu** (Add to Chrome).



4. Klikněte na možnost **Přidat rozšíření** (Add extension).

Web Secure je aktivní, když se v pravém horním rohu prohlížeče zobrazí ikona **ZoneAlarm**.

Kliknutím na tuto ikonu můžete upravit nastavení a zobrazit vaše bezpečná stahování.



b. Nastavení rozšíření pro Chrome

Ikona ZoneAlarm v prohlížeči Google Chrome vás přesměruje na stránku nastavení. Zde jsou dva typy nastavení: Stahování dokumentů a Ochrana proti phishingu.

c. Stahování dokumentů

Funkce odstraňování hrozeb při stahování dokumentů čistí soubory v různých formátech, jako jsou např. PDF, DOC, XLS, PPT atd. Přepínací tlačítko Zapnuto/Vypnuto umožňuje tuto funkci zapnout.

Všechny dokumenty jsou kontrolovány, a když jsou v souboru odhaleny škodlivé prvky, můžete se rozhodnout je ze souboru odstranit nebo zablokovat stahování.

Pomocí tlačítka **Odstranit** máte možnost odstranit ze souboru škodlivé prvky nebo soubor převést do formátu PDF.

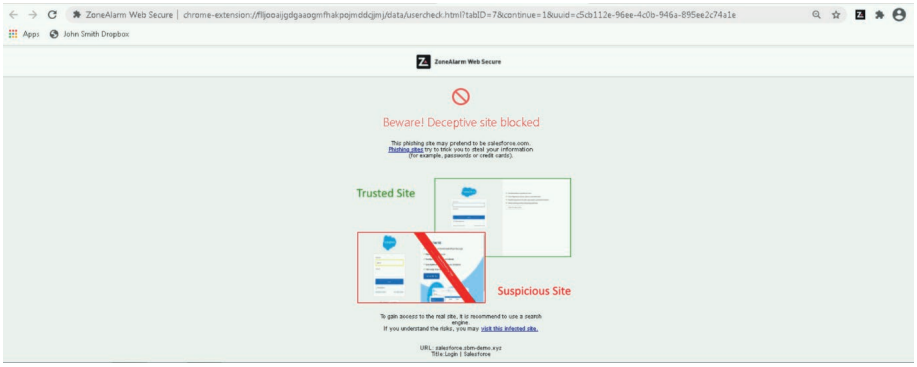
Všechny stažené soubory budou zkontrolovány a škodlivé prvky odstraněny nebo zablokovány na základě zvolených nastavení.

d. Ochrana proti phishingu

ZoneAlarm může skenovat webové stránky a detekovat jakékoli phishingové stránky, které by mohly ohrozit vás nebo váš systém. V níže uvedeném příkladu můžete vidět, že probíhá sken přihlašovací stránky webu.

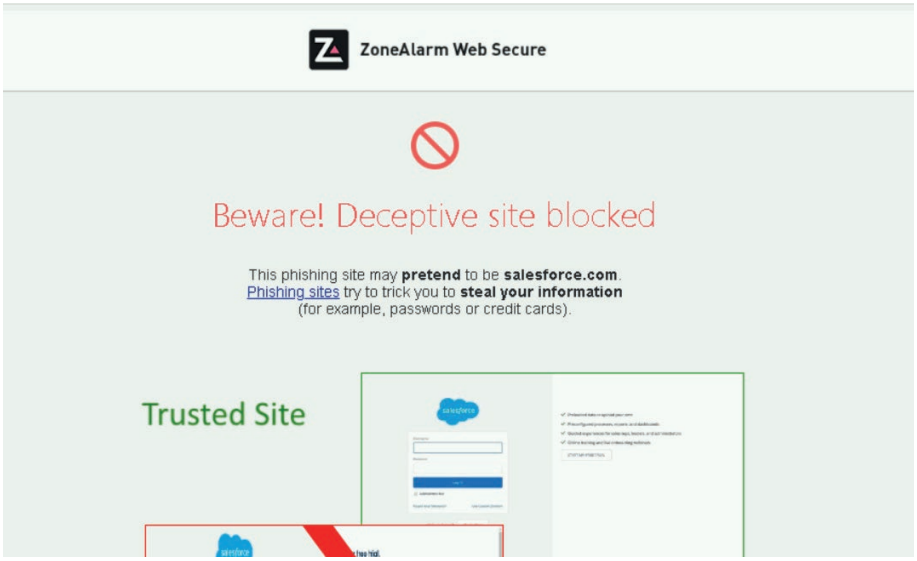
Po dokončení kontroly se zobrazí oznámení, že je kontrola dokončena a nebyla zjištěna žádná phishingová aktivita.

Nyní se podívejme na příklad, kdy došlo k identifikaci podvodného webu. ZoneAlarm skenuje níže webovou stránku v rámci aplikace Microsoft Outlook.



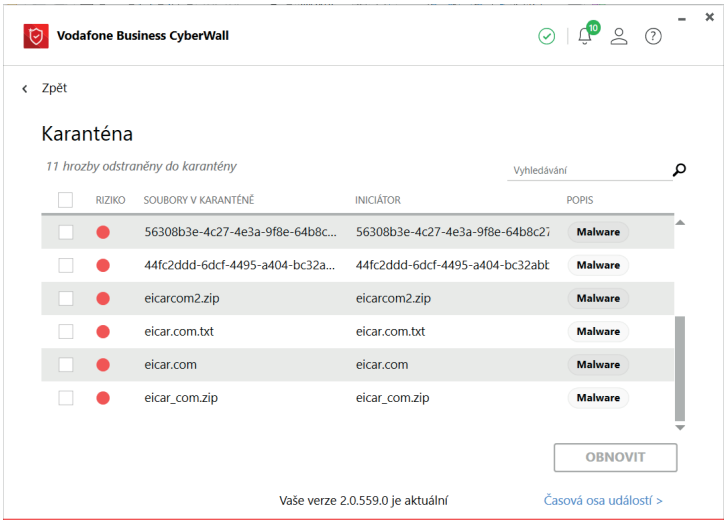
Tento web je falešný a ZoneAlarm uživatele upozorní prostřednictvím oznámení a podvodný web zablokuje.

ZoneAlarm také zobrazí srovnání mezi důvěryhodným webem a podezřelým webem.



6. Panel karantény

Pokud CyberWall nemůže infikované soubory opravit, umístí je do karantény. Soubory v karanténě nejsou odstraněny ani používány, ale nemohou vám ani uškodit. Panel **Karanténa** (Quarantine) zobrazuje škodlivé soubory, které byly detekovány a umístěny do karantény aplikací CyberWall.

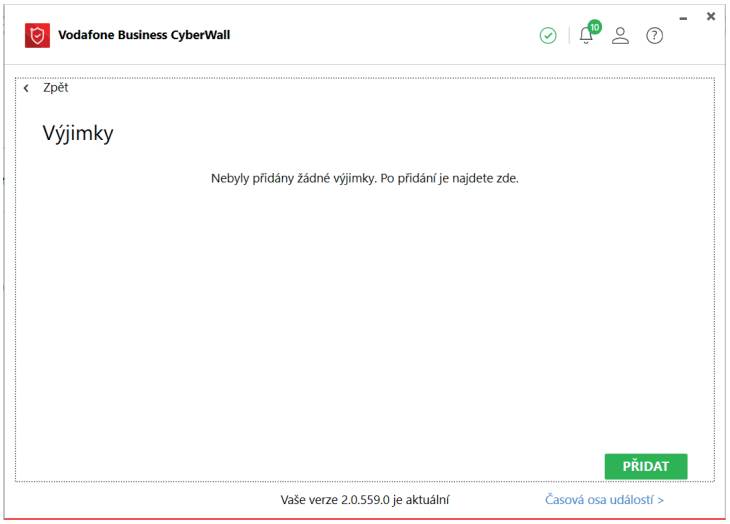


Chcete-li z karantény vyjmout zablokovaný soubor, o kterém se domníváte, že pochází z důvěryhodného zdroje, označte ho a klikněte na tlačítko **Obnovit** (Restore).

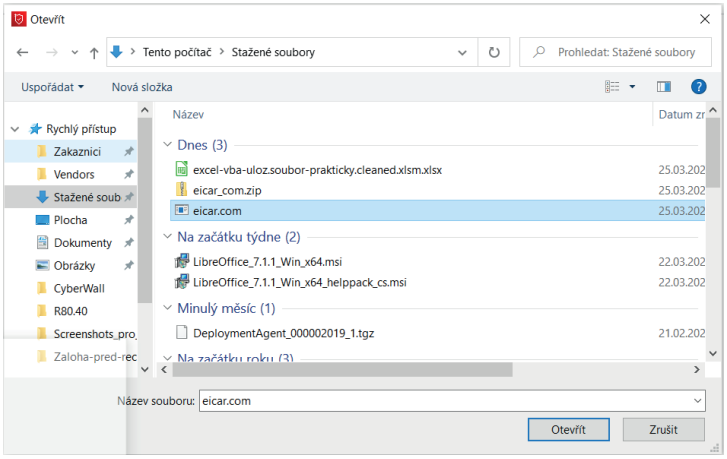
7. Panel výjimek

Panel výjimek umožňuje určit adresáře, soubory nebo programy, ve kterých si nepřejete hledat viry ani malware. To může být užitečné v případech, kdy víte, že jsou tyto adresáře, soubory a programy bezpečné, ale povede to ke snížení celkové úrovně ochrany. Výjimky můžete přidat ručně, nebo je přidat až poté, co program CyberWall soubor detekuje. Ruční přidání nebo odebrání výjimek provedete následujícím způsobem:

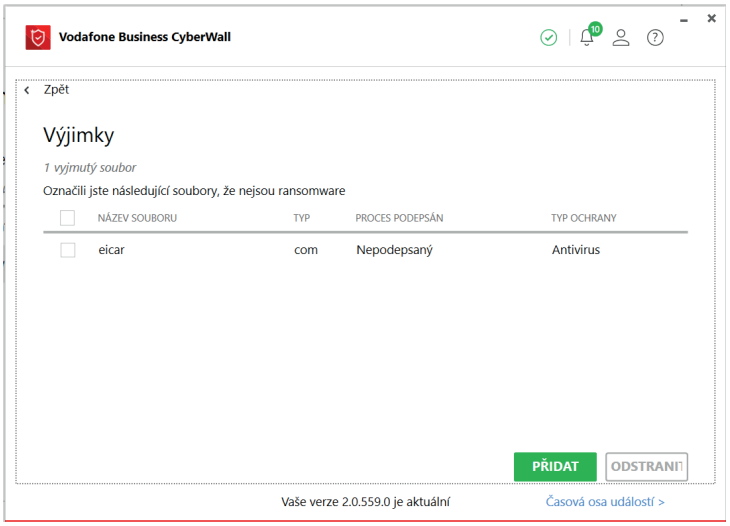
1. Klikněte na tlačítko **Přidat** (Add).



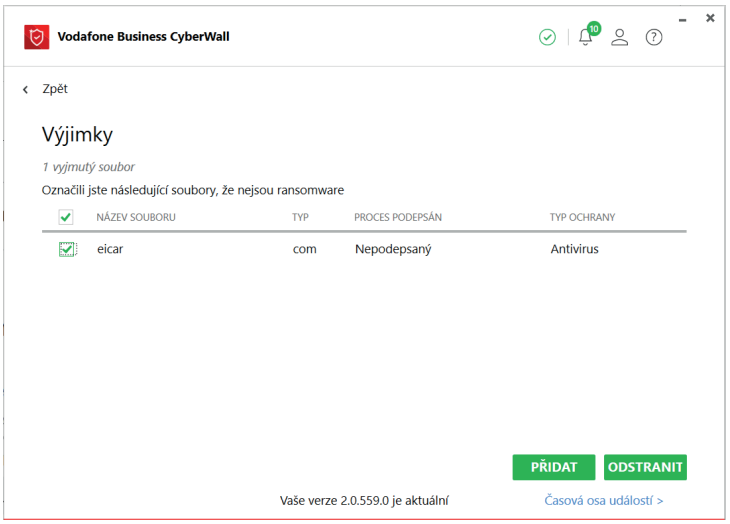
2. Vyberte soubor, který chcete přidat mezi výjimky.



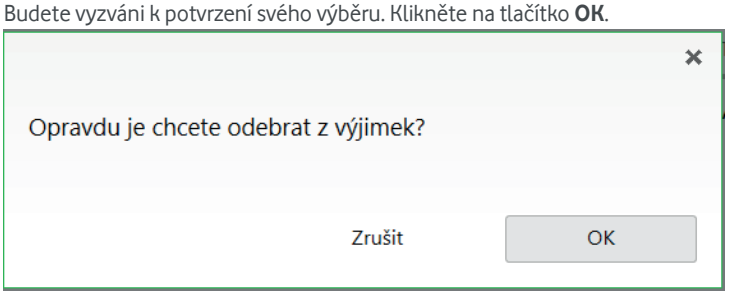
3. Soubor bude přidán do seznamu výjimek.



4. Chcete-li soubor odebrat ze seznamu výjimek, vyberte jej a klikněte na tlačítko **Odebrat** (Remove).



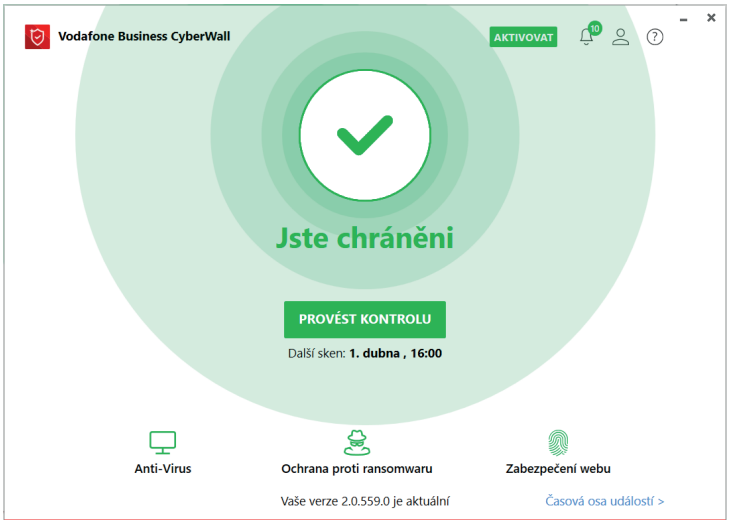
5. Budete vyzváni k potvrzení svého výběru. Klikněte na tlačítko **OK**.



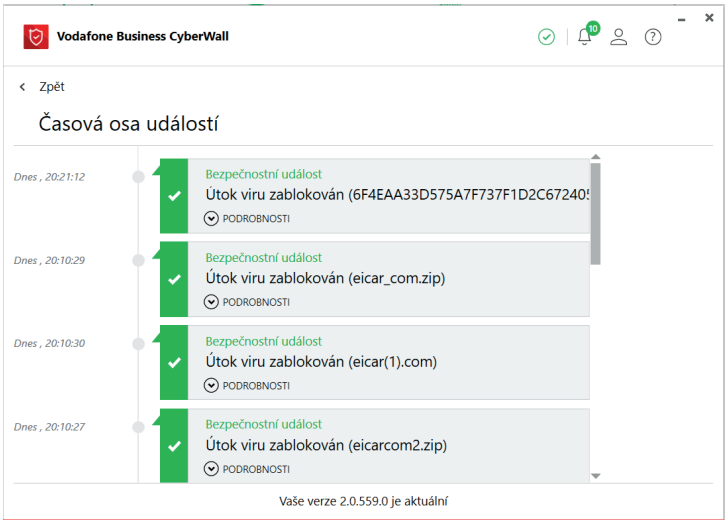
8. Časová osa událostí

CyberWall zaznamenává různé události do souboru protokolu událostí. Ve výchozím nastavení CyberWall zaznamenává do protokolu všechny kontroly, aktualizace a detekce hrozeb. Časovou osu událostí můžete zobrazit následujícím způsobem:

1. Klikněte na odkaz **Časová osa událostí** (Events Timeline) v pravém dolním rohu stránky.

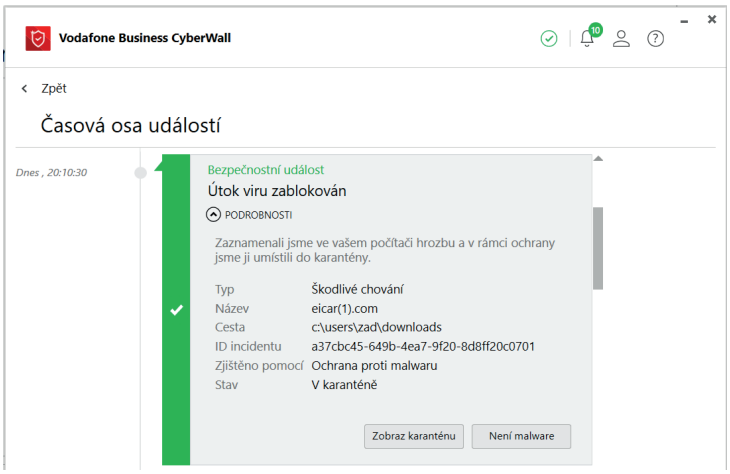


2. Zobrazí se všechny události. Kliknutím na tlačítko **Podrobnosti** (Details) zobrazíte další informace.



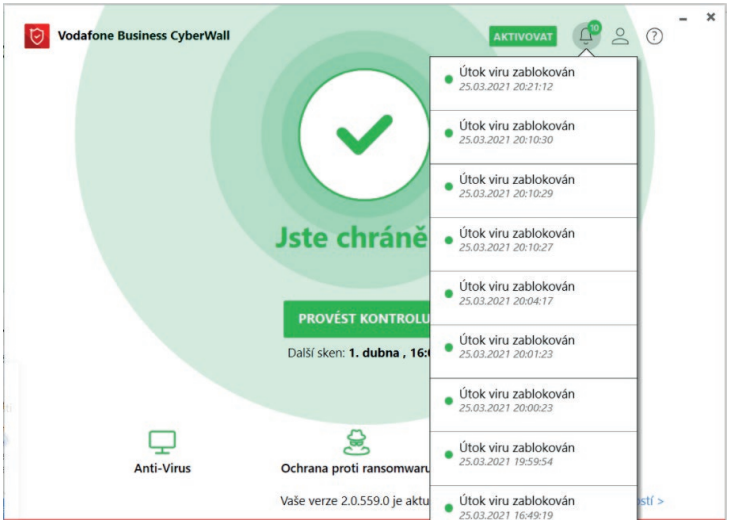
3. Zobrazí se podrobnosti události spolu se stavem. Posunutím dolů zobrazíte další události.

4. V okně **Časové osy událostí** (Events Timeline) můžete také provádět různé akce, například prohlížet panel karantény a u detekovaných hrozeb označit, že se nejedná o ransomware nebo malware.



9. Oznámení

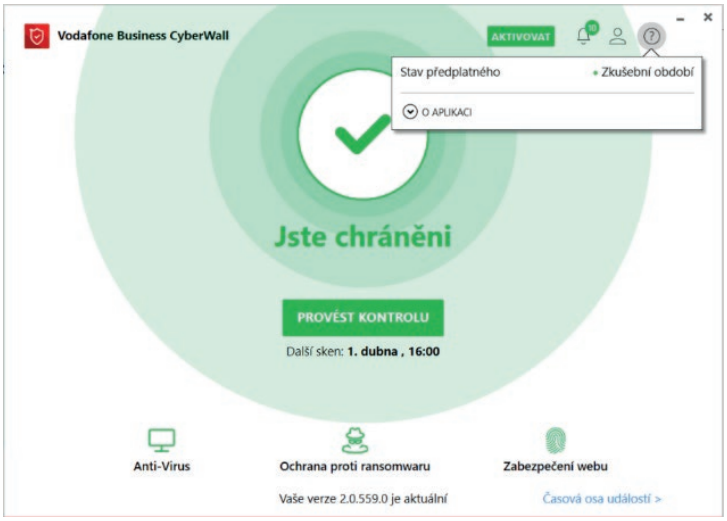
Ikona **Oznámení** umožňuje zobrazit nedávné události, ke kterým v programu CyberWall došlo. Kliknutím na možnost **Všechny události** (All events) zobrazíte všechny události na stránce **Časová osa událostí**.



10. O produktu

Kliknutím na ikonu **O produktu** (About) zobrazíte všechny podrobnosti o programu CyberWall nainstalovaném ve vašem systému. Můžete zobrazit podrobnosti, jako je stav předplatného, stav a číslo verze atd. V rámci sekce O produktu můžete provádět také následující uživatelské akce:

1. Odeslat e-mailem zpětnou vazbu týkající se produktu CyberWall
2. Zkopírovat údaje o programu do schránky
3. Ukládat protokoly a další relevantní zprávy
4. Vložit aktivační kód



PK7941