SOPHOS

Cybersecurity made simple.

Sophos Endpoint for Windows

Nápověda

Obsah

1 O řešení Sophos Endpoint for Windows

Tento soubor nápovědy poskytuje informace o řešení Sophos Endpoint for Windows a vysvětluje jednotlivé postupy krok za krokem.

2 Sophos Endpoint

Nástroj Sophos Endpoint je možné chránit na počítačích a serverech.

Omezení
Nemusíte mít k dispozici všechny funkce, které jsou zde popsané. Závisí to na dostupné licenci.

Nástroj Sophos Endpoint je nakonfigurován a spravován centrálně z Sophos Central Admin.

Na počítači nebo serveru však můžete provádět některé úlohy:

- Zkontrolujte stav počítače.
- Prohledejte počítač nebo server, zda nejsou ohroženy.
- Viz podrobnosti o událostech na počítači nebo serveru, například zjištěné hrozby.
- Vyčistěte hrozbu.
- Změna nastavení zabezpečení. Můžete například vypnout některé funkce, abyste mohli řešit problémy.
- Aktualizujte.
- Odstraňování poruch.

Poznámka
Pro vyčištění hrozeb nebo změnu nastavení je nutné použít možnost **Přihlášení správce** a zadat heslo ochrany proti neoprávněné manipulaci.

Související koncepty

Stav (strana 3)
Můžete zkontrolovat stav zabezpečení a prohledat počítač nebo server.

Události (strana 5)
Na stránce **Události** se zobrazují události v počítači nebo serveru, například zjištěné hrozby.

Související úkoly

Prohledání souboru (strana 9)
Můžete prohledávat jednotlivé soubory.

Prohledání počítače nebo serveru (strana 9)
Při prohledávání počítače nebo serveru postupujte podle těchto pokynů.

Vyčistěte hrozbu (strana 9)
Postupujte podle následujících pokynů a odstraňte zjištěné hrozby.

Změna nastavení zabezpečení (strana 9)
Při změně nastavení zabezpečení postupujte podle těchto pokynů.

Aktualizovat nyní (strana 10)
Při aktualizaci virových definic postupujte podle těchto pokynů.

Odstraňování poruch (strana 10)
Při odstraňování problémů postupujte podle těchto pokynů.

3 Stav

Můžete zkontrolovat stav zabezpečení a prohledat počítač nebo server.

Omezení
Nemusíte mít k dispozici všechny funkce, které jsou zde popsané. Závisí to na dostupné licenci.

Na stránce **Stav** můžete:

- Podívejte se na stav zabezpečení počítače nebo serveru.
- Prohledejte počítač nebo server, zda nejsou ohroženy.
- Další informace naleznete v části věnované zobrazení nainstalovaných funkcí a jejich stavu zabezpečení.

Poznámka
Odkaz **O aplikaci** v pravé dolní části stránky umožňuje aktualizovat definice virů nebo odstraňovat problémy s produktem.

Stav zabezpečení

Stav je zobrazen pomocí ikony v horní části stránky.

Nastavení	Popis
 Zelená.	Nejsou k dispozici žádná upozornění nebo pouze upozornění s nízkou prioritou.
 Červená.	Existují upozornění s vysokou prioritou.
 Žlutá.	Existují upozornění se střední prioritou.
 Šedá.	Stav je neznámý.

Níže jsou zobrazeny všechny nainstalované funkce s individuálním stavem zabezpečení.

Prohledání počítače

Kliknutím na tlačítko **Prohledat** můžete vyhledat hrozby ve všech souborech v počítači nebo na serveru.

Po dokončení prohledávání se zobrazí souhrn výsledků. Pokud jsou zjištěny hrozby, můžete přejít na stránku **Události** a zobrazit podrobnosti.

4 Události

Na stránce **Události** se zobrazují události v počítači nebo serveru, například zjištěné hrozby.

Omezení
Nemusíte mít k dispozici všechny funkce, které jsou zde popsané. Závisí to na dostupné licenci.

Události můžete filtrovat, například tak, aby se zobrazovaly pouze ty, které vyžadují provedení akce, nebo můžete vyhledávat konkrétní typy událostí.

Seznam událostí

Seznam zobrazuje:

- Závažnost. Ikona v levé části seznamu ukazuje, zda má událost vysokou nebo střední prioritu, nebo se jedná o upozornění.
- Zdroj. Ikona v levé části seznamu označuje funkci Sophos, která událost ohlásila.
- Datum a čas, kdy k události došlo.
- Popis události.
- Odkaz, který vám umožní provést akci (pokud je potřeba nějakou akci provést). Zobrazí se pouze v případě, že jste se přihlásili jako správce.

Chcete-li zobrazit podrobnosti každé události, kliknutím na šipku vpravo ji rozbalte.

Akce, které můžete provést, jsou stejné jako ty, které jsou k dispozici v části Sophos Central Admin. Viz také seznam na stránce **Upozornění** v části Sophos Central Admin nápověda.

Události můžete filtrovat podle následujících typů:

Typ události	Popis
Malware a potenciálně nežádoucí aplikace	Malware je obecný pojem pro škodlivý software. Zahrnuje viry, červy, trojské koně a spyware. Potenciálně nežádoucí aplikace (PUA) jsou programy, které nejsou škodlivé, jako například program měnící nastavení vytáčení (dialery), nástroje pro vzdálenou správu a nástroje pro hacking, ale jsou obecně považovány za nevhodné pro většinu firemních sítí.
Webové hrozby	Webové hrozby zahrnují škodlivé webové stránky, nezařazené webové stránky a riskantní stahování. Některé webové stránky jsou také obecně považovány za nevhodné pro firemní sítě, například pro stránky dospělé nebo pro sociální sítě. Ty mohou být také blokovány.

Typ události	Popis
Škodlivé chování	Škodlivé chování je podezřelé chování softwaru, který je již spuštěn v počítači nebo serveru. Ransomware je škodlivý software, který vám odepírá přístup k vašim souborům, dokud nezaplatíte výkupné.
Řízené položky	Tato kategorie zahrnuje: • Aplikace, které nejsou bezpečnostní hrozbou, ale které jsou podle vás nevhodné pro použití v běžné kancelářské práci. • Periferní zařízení a vyjímatelná média. • Riskantní stahování nebo webové stránky, které nejsou vhodné pro práci v kanceláři. • Soubory obsahující citlivé informace (například osobní nebo finanční údaje), které nechcete nechat uniknout.
Škodlivý provoz	Škodlivý provoz je provoz mezi počítači, který indikuje možný pokus o převzetí kontroly nad počítačem nebo serverem (útok typu „příkaz a kontrola“).
Exploity	Exploity, kterým může společnost Sophos zabránit, zahrnují ovládnutí aplikací a zneužití, které využívají zranitelných míst v prohlížečích, zásuvných modulech prohlížeče, aplikacích Java, multimediálních aplikacích a aplikacích sady Microsoft Office.

5 Nastavení

Dočasně můžete změnit nastavení zabezpečení v tomto počítači nebo serveru.

Možná bude nutné provést tento postup při odstraňování problémů. Můžete například vypnout funkci a zjistit, zda způsobuje problémy v počítači.

Omezení
Nemusíte mít k dispozici všechny funkce, které jsou zde popsané. Závisí to na dostupné licenci.

Omezení
Stránka **Nastavení** je k dispozici pouze v případě, že jste zadali heslo ochrany proti neoprávněné manipulaci (je k dispozici u správce systému Sophos Central).

Postup při změně nastavení

Zaškrtněte pole **Potlačit zásady systému Sophos Central na dobu až 4 hodin, abyste mohli odstranit potíže**.

Nyní můžete provést změny na této stránce. Změny dočasně potlačí zásady, které jste vy (nebo jiný správce) aplikovali z Sophos Central Admin.

Po čtyřech hodinách se nastavení automaticky změní zpět na centrálně vynucená nastavení zásad.

Pokud chcete, můžete nastavení vrátit zpět dříve. K tomu nelze použít posuvníky pro jednotlivé funkce. Místo toho vypněte možnost **Potlačit zásady systému Sophos Central na dobu až 4 hodin, abyste mohli odstranit potíže**.

Hloubkové učení

Hloubkové učení využívá principy pokročilého strojového učení k detekci hrozeb. Dokáže identifikovat malware a potenciálně nežádoucí aplikace bez použití signatur.

Prohledání v reálném čase

Prohledání v reálném čase prověřuje jednotlivé položky v okamžiku, kdy se k nim uživatel pokusí získat přístup. Přístup odepře, pokud představují hrozbu. Můžete vybrat následující možnosti:

- **Soubory**: Tato možnost prohledá místní soubory a sdílené síťové složky (je-li tato možnost vybrána v zásadách).
- **Internet**: Tím prohledává také zdroje na Internetu. Může prohledávat probíhající stahování, blokovat přístup ke škodlivým webům a zjišťovat webové stránky s nízkou pověstí.

Kontroly uživatelů

- **Ovládání periferních zařízení** umožňuje řídit přístup k periferním zařízením a vyjímatelným médiím.

- **Ovládání aplikací** umožňuje zjišťovat a blokovat aplikace, které nejsou bezpečnostní hrozbou, ale které jsou podle vás nevhodné pro použití v běžné kancelářské práci.
- Možnost **Správa webu** vám umožňuje zajistit ochranu před riskantním stahováním, řídit weby, které mohou uživatelé navštívit, a zabránit ztrátě dat.
- Možnost **Prevence ztráty dat** umožňuje sledovat a omezit přenos souborů obsahujících citlivá data.
- **Ochrana proti neoprávněné manipulaci** umožňuje omezit změny. Pokud je tato funkce zapnutá, místní správce potřebuje heslo nezbytné pro změnu nastavení zabezpečení nebo odinstalaci nástroje Sophos Endpoint.

Ochrana chodu programu

Ochrana chodu programu chrání před hrozbami zjišťováním podezřelého nebo škodlivého chování nebo provozu na počítačích koncových bodů. Můžete vybrat následující možnosti:

- **Zjišťování ransomwaru**: Tato možnost chrání před malwarem, který omezuje přístup k souborům, a poté vyžaduje poplatek za jejich uvolnění.
- **Bezpečné procházení**: Tato možnost chrání webové prohlížeče před zneužitím malwarem.
- **Zmírnění následků exploitů**: Tato možnost chrání aplikace, které jsou nejvíce náchylné ke zneužití malwarem, jako jsou například aplikace Java.
- **Ochrana sítě před hrozbami**: Tato funkce detekuje provoz mezi koncovým počítačem a serverem, který indikuje možný pokus o převzetí kontroly nad koncovým počítačem. Zahrnuje kontrolu paketů, která prohledává síťovou komunikaci, identifikuje a blokuje hrozby dříve, než mohou poškodit operační systém nebo aplikace.

  Poznámka
  Pokud vypnete možnost **Ochrana sítě před hrozbami:**, funkce EDR, izolace a blokování komunikace budou také vypnuty.

- **Detekce škodlivého chování**: To se provádí zjišťováním a blokováním chování, o kterém je známo, že je škodlivé nebo podezřelé.

Ovládací prvky počítače

V počítačích a serverech můžete sledovat bránu Windows Firewall (a další registrované brány firewall).

6 Jak na...

6.1 Prohledání souboru

Můžete prohledávat jednotlivé soubory.

Chcete-li prohledat soubor, postupujte takto:

- V Průzkumníku klepněte pravým tlačítkem na soubor a vyberte příkaz **Prohledat**.

6.2 Prohledání počítače nebo serveru

Při prohledávání počítače nebo serveru postupujte podle těchto pokynů.

Prohledání všech souborů v počítači nebo na serveru:

1. Přejděte na stránku **Stav** nebo stránku **Detekce**.
2. Klepněte na tlačítko **Skenovat**.
   Po dokončení prohledávání se zobrazí souhrn výsledků.
3. Pokud jsou zjištěny hrozby, můžete přejít na stránku **Události** a zobrazit podrobnosti.

6.3 Vyčistěte hrozbu

Postupujte podle následujících pokynů a odstraňte zjištěné hrozby.

Chcete-li hrozbu odstranit, postupujte následujícím způsobem:

1. Klikněte na možnost **Přihlášení správce** a zadejte heslo ochrany proti neoprávněné manipulaci (dostupné u správce systému Sophos Central).
2. Přejděte na stránku **Události** a zobrazte podrobnosti o zjištěné hrozbě.
3. Vedle podrobností o hrozbě vyhledejte odkaz akce.

Opatření, která můžete podniknout, jsou shodná s těmi, které nabízí konzola Sophos Central Admin. Další informace naleznete v seznamu na stránce **Upozornění** v Sophos Central Admin nápověda.

6.4 Změna nastavení zabezpečení

Při změně nastavení zabezpečení postupujte podle těchto pokynů.

Změna nastavení zabezpečení:

1. Klikněte na tlačítko **Přihlášení správce** v pravém horním rohu uživatelského rozhraní.
2. Zadejte heslo ochrany proti neoprávněné manipulaci (dostupné u správce systému Sophos Central).
   V panelu nabídek je nyní odkaz **Nastavení**.
3. Přejděte na stránku **Nastavení**.
4. Zaškrtněte pole **Potlačit zásady systému Sophos Central na dobu až 4 hodin, abyste mohli odstranit potíže**.

5. Pomocí posuvníků na stránce vypněte funkce zabezpečení.

Po čtyřech hodinách se nastavení automaticky změní zpět na centrálně vynucená nastavení zásad.

Poznámka
Pokud chcete, můžete nastavení vrátit zpět dříve. K tomu nelze použít posuvníky pro jednotlivé funkce. Místo toho zrušte zaškrtnutí pole **Potlačit zásady systému Sophos Central na dobu až 4 hodin, abyste mohli odstranit potíže**.

6.5 Aktualizovat nyní

Při aktualizaci virových definic postupujte podle těchto pokynů.

Při aktualizaci postupujte následujícím způsobem:

1. Klepněte na tlačítko **O aplikaci**.
2. Klepněte na tlačítko **Aktualizovat nyní**.

6.6 Odstraňování poruch

Při odstraňování problémů postupujte podle těchto pokynů.

Při odstraňování problémů postupujte následujícím způsobem:

1. Klepněte na tlačítko **O aplikaci**.
2. Klikněte na možnost **Otevřete nástroj pro vlastní nápovědu koncového bodu** a shromážděte data o problému, nebo klikněte na odkaz na **Fórum komunity**.

6.7 Šifrování počítače

Při zašifrování počítače postupujte podle těchto pokynů.

Omezení
Šifrování zařízení je dostupné pouze na počítačích koncových bodů.

Funkce Šifrování zařízení šifruje pevný disk počítače pomocí technologie Windows BitLocker. Správce určí, zda je nutné provést ověření při každém přístupu k počítači.

Pokud není vyžadováno ověření, šifrování pevného disku se automaticky spustí, jakmile počítač restartujete poté, co jste obdrželi zásady systému Sophos Central. V tomto případě není třeba nic dělat.

Pokud potřebujete provést ověření, postupujte následovně:

1. Po zobrazení dialogového okna **Šifrování zařízení Sophos** postupujte podle pokynů v dialogovém okně. Konkrétní pokyny závisí na vašem systému a nastavení zásad definovaných správcem.
    - Pokud zásady šifrování zařízení vyžadují pro ověření kód PIN nebo heslo, postupujte podle pokynů na obrazovce a vytvořte kód PIN nebo heslo.

Poznámka
Při vytváření kódu PIN nebo hesla buďte opatrní. Prostředí před spuštěním podporuje pouze rozložení klávesnice US-English. Pokud nyní vytvoříte kód PIN nebo heslo se speciálními znaky, budete možná muset při jeho zadávání použít jiné klávesy, abyste se mohli později přihlásit.

- Pokud zásady šifrování zařízení vyžadují pro ověření klíč USB, je nutné připojit k počítači jednotku USB flash. Jednotka USB flash musí být naformátována se systémem souborů NTFS, FAT nebo FAT32.

2. Po klepnutí na tlačítko **Restartovat a šifrovat** se počítač restartuje a zašifruje pevné disky. Můžete pracovat obvyklým způsobem.

Poznámka
Dialogové okno můžete zavřít klepnutím na tlačítko **Provést později**. Zobrazí se však znovu při příštím přihlášení.

Po zašifrování systémového svazku systémem Sophos Central se spustí šifrování datových svazků. Vyměnitelné datové svazky, například jednotky USB, nejsou šifrovány.

Během přihlášení k počítači může být pro odemknutí systémového svazku nutné zadat kód PIN, heslo nebo klíč USB. Datové svazky se automaticky odemknou.

6.8 Přístup do počítače, když zapomenete heslo

Přístup k počítači získáte následujícím způsobem.

Pokud se nemůžete přihlásit k počítači, protože jste zapomněli kód PIN, heslo nebo klíč USB, potřebujete obnovovací klíč.

Používáte-li nástroj Sophos Device Encryption, obnovovací klíč se uloží v systému Sophos Central. Chcete-li získat obnovovací klíč, proveďte jeden z následujících kroků:

- Přihlaste se do samoobslužného portálu Sophos a postupujte podle pokynů v nápověda.
- Požádejte správce o poskytnutí klíče pro obnovení. Tímto způsobem postupujte, nemůžete-li použít samoobslužný portál.

Související úkoly

Použití obnovení nástrojem BitLocker (strana 11)
Podle následujících pokynů obnovte počítač.

6.8.1 Použití obnovení nástrojem BitLocker

Podle následujících pokynů obnovte počítač.

Chcete-li obnovit počítač, postupujte následujícím způsobem:

1. Restartujte počítač a stiskněte klávesu Esc na přihlašovací obrazovce nástroje **BitLocker**.
2. Na obrazovce nástroje **Obnovení BitLocker** vyhledejte možnost **ID obnovovacího klíče**. Na krátkou dobu se zobrazí **ID obnovovacího klíče**. Chcete-li jej znovu zobrazit, musíte počítač restartovat.

3. Obraťte se na správce a předejte mu **ID obnovovacího klíče**.
   Váš správce musí najít obnovovací klíč ve vašem počítači v systému Sophos Central a poskytnout vám jej.
4. Na obrazovce nástroje **Obnovení BitLocker** zadejte obnovovací klíč.
   Nyní můžete počítač spustit.
5. Podle pokynů na obrazovce vytvořte na výzvu nový kód PIN nebo heslo nástroje BitLocker.

   V počítačích se systémem Windows 7 se žádné pokyny nezobrazují. Kód PIN/heslo je nutné resetovat ručně.

Nyní můžete k počítači znovu přistupovat.

Poznámka
Obnovovací klíč lze použít pouze jednou. Pokud potřebujete počítač obnovit později, musíte získat nový obnovovací klíč.

7 Proč je přenos souborů zablokovaný?

Může se zobrazit zpráva s informací, že byl zablokován přenos souborů (například kopírování, přesouvání nebo odesílání souborů e-mailem).

K tomu dochází proto, že vaše společnost stanovila zásady, které zajistí, abyste neúmyslně neposílali citlivé informace uživatelům, kteří by je neměli mít.

Existují dva typy zpráv.

Zpráva	Popis
Přenos je zablokován	Pokud se zobrazí zpráva „Přenos souborů zablokován“, nelze soubory přenést. Váš správce mohl přidat k této zprávě nějaké rady.
Přenos může být povolen	Pokud se zobrazí zpráva „Požadavek na přenos souborů zablokován“, můžete se rozhodnout, zda soubory přenést. Váš správce mohl přidat k této zprávě nějaké rady. Pokud jste si jisti, že je bezpečné pokračovat, klikněte na tlačítko **Povolit**.

8 Podpora

Technickou podporu pro produkty společnosti Sophos můžete získat následujícími způsoby:

- Navštivte komunitu Sophos na adrese community.sophos.com/ a vyhledejte další uživatele, kteří mají stejný problém.
- Navštivte znalostní bázi podpory společnosti Sophos na adrese www.sophos.com/en-us/support.aspx.
- Stáhněte si dokumentaci k produktu na adrese www.sophos.com/en-us/support/documentation.aspx.
- Otevřete si vstupenku s naším týmem podpory na adrese https://secure2.sophos.com/support/contact-support/support-query.aspx.

9 Právní upozornění