vmware

# VMware Carbon Black: udělejte první krok

## Buďte připraveni na důmyslnější kybernetické útoky a poražte hackery v jejich vlastní hře

V dnešním digitálním světě čím dál častěji společnosti využívají práci z domova, což posouvá samotné hranice organizace práce za její možnosti. Ony Hranice představují právě koncová zařízení, která mohou být zároveň I slabým místem vhodným pro kybernetickým útok.

Primárním způsobem práce ve společnosti je nyní práce z domova, což pachatelé kybernetických útoků využívají jako příležitost, jak zlepšit metody útoků. Většina dnešních útoků způsobujících škody, mezi něž patří taktiky jako lateral movement, island hopping aj., se zaměřují právě na legitimní pracovní nástroje.

Pro zabezpečení práce na dálku musí organizace přehodnotit svou stávající infrastrukturu a také svůj postoj k zabezpečení a celistvosti provozních postupů v novém pracovním uspořádání.

### Roste frekvence a důmyslnost kybernetických útoků

V průzkumu, kterého se zúčastnilo přes 3 000 bezpečnostních profesionálů, 91 % z nich uvedlo, že zaznamenalo v důsledku zavedení práce z domova nárůst kybernetických útoků[1].

V březnu hackeři pandemii využili k phishingovým útokům a rozšíření falešných mobilních aplikací, trojských koňů a ransomwaru. Jelikož bylo nutné pokračovat v práci z domova, zdokonalily se i způsoby vydírání, narušování a infiltrace organizací – 80 % bezpečnostních profesionálů uvedlo, že jsou nyní útoky mnohem důmyslnější[1].

Chyby v zabezpečení OS jsou v současnosti nejčastějšími příčinami útoků. Představují až 18 % všech útoků. Technika island hopping, která v říjnu 2019 stála za 4,5 % incidentů, je nyní na druhém místě a představuje 13 % všech systémových útoků[1].

Co dělají organizace pro zesílení svého zabezpečení, když sofistikované útoky rychle nahrazují útoky skryté, jejichž cílem je dosáhnout dlouhodobého prolomení systému?

### 96 % bezpečnostních odborníků zvyšuje investice[1]

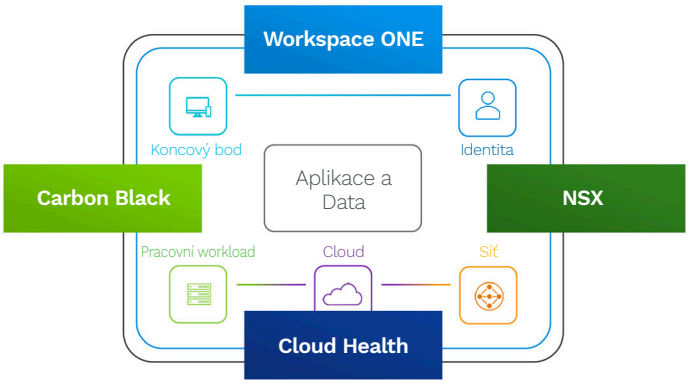
Stále více bezpečnostních odborníků, ve snaze posílit svou ochranu, navyšuje své rozpočty a investuje do nových technologií, aby získali následující výhody:

- analýza prostředí za účelem pochopení toho, co je „normální“ chování a určete oblasti zájmu,
- znemožnění útočníkům ve zneužívání legitimních nástrojů,
- automatizace vyšetřovacích postupů, aby reakce na útok byly rychlejší a efektivnější,
- zjednodušení a centralizace celkového zabezpečení.

# VMware pro implicitní zabezpečení: Carbon Black

Společnost VMware využila příležitosti k transformaci portfolia a sjednotila a dodala kontextově zaměřená bezpečnostní opatření ve všech částech svého portfolia – od zabezpečení koncových bodů a pracovních workloadů až po zabezpečení sítě, pracovního prostředí a cloudu.

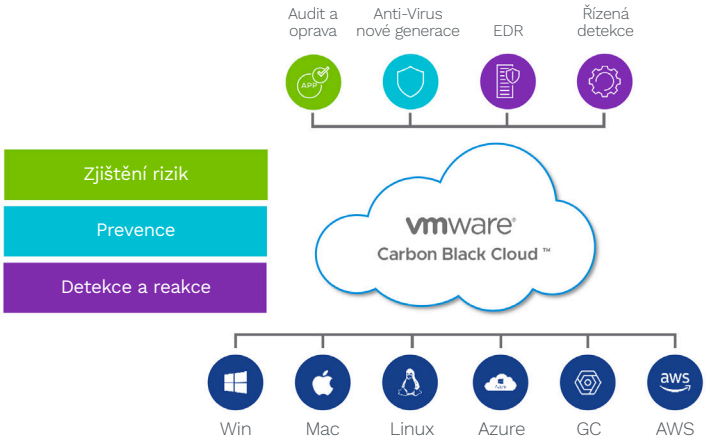
Carbon Black představuje vývoj strategie společnosti VMware pro vnitřní zabezpečení, v němž jsou bezpečnostní funkce zabudovány do infrastruktury napříč pracovními workloady, koncovými body a aplikacemi. Carbon Black zjednodušuje a posiluje zabezpečení jakékoliv aplikace, cloudu a zařízení. Interaguje tak s dalšími VMware řešeními pro vnitřní zabezpečení (Workspace ONE, Cloud Health a NSX), aby bylo dosaženo úplného přehledu o koncových zařízeních, pracovních workloadech, cloudu, síti a uživatelské identitě.




## Příležitost transformovat zabezpečení


## 5 funkcí, které VMware Carbon Black odlišují

1. **Antivirus nové generace**
2. **Behaviorální detekce koncových bodů a reakce na hrozby**
3. **Sledování výstrah a třídění**
4. **Hodnocení a oprava zařízení v reálném čase**
5. **Sledování a eliminace hrozeb**




## Cloud VMware Carbon Black

**Jedna konzole, jedna platforma, jeden agent.**

Carbon Black, který konsoliduje více funkcí zabezpečení koncových zařízení do jednoho agenta a konzole, umožňuje uživatelům pracovat rychleji a efektivněji s jedinou cloudovou nativní platformou. Pokud k útoku přeci jen dojde, je možné na něj snadno a rychle reagovat. Snadná a rychlá reakce minimalizuje prostoje a rychle obnovuje obvyklé činnosti.

**Je-li Carbon Black integrován s VMware Workspace One, dochází ke sjednocení týmů zajišťujících bezpečnost a infrastrukturu, k automatické ochraně nových a stávajících workloadů v každém koncovém zařízení a vzniká robustní obrana proti nejrůznějším hrozbám.**

**83 % uživatelů Carbon Black uvádí, že zaznamenali pokles rozporů mezi jejich bezpečnostními a IT operačními týmy.**
Forrester[2]

**Integrovaný spolu s vSphere poskytuje zabezpečení bez agentů, což snižuje náklady na instalaci a správu.**

**Sloučením do jednoho agenta a přechodem na cloudové rozhraní ušetří Carbon Black IT a bezpečnostním týmům 4 hodiny práce denně.**
Forrester[2]

**S otevřenými API a v kombinaci s více než stovkou integrovaných produktů se Carbon Black bez problémů stane součástí vašeho stávajícího bezpečnostního portfolia.**

**Carbon Black u jednoho bezpečnostního incidentu ušetří až 7,5 hodiny.**
Forrester[2]

## Přizpůsobí se jakémukoli podnikání

Každá organizace je jiná. V průměru se využívá k ochraně operací 8,91 různých bezpečnostních nástrojů1. VMware Carbon Black transformuje zabezpečení pomocí cloudové ochrany koncových zařízení, která se přizpůsobuje potřebám každého jednotlivce. Při vytváření jednotného přístupu k zabezpečení je mnohem jednodušší zaujmout proaktivní přístup k identifikaci a reakci na potenciální problémy.

## Silnější ochrana s vnitřním zabezpečením

Roste-li IT infrastruktura, "našroubuje" se nové bezpečnostní opatření na nejnovější citlivé místo – díky tomu je pro útočníky podstatně snazší proniknout do sítě. V případě Carbon Black jsou všechny bezpečnostní funkce zahrnuty v infrastruktuře a napříč cloudovými řešeními, body a aplikacemi, díky čemuž uživatelé získají úplný přehled o všech koncových zařízeních a workloadech.

## Využívá behaviorální analýzu

Podniky potřebují zabezpečení schopné odhalit drobné výkyvy, které skrývají zákeřné útoky. Proto Carbon Black každý den analyzuje více než 1 bilion bezpečnostních událostí. Zabezpečení poskytnuté na základě kontextu: Carbon Black se naučí, co je pro každé prostředí „normální", čímž dokáže porozumět chování útočníků a na základě toho určit a zastavit neznámé útoky.

## Použijte Carbon Black při...

- **Výměna podnikového antivirového programu:** rychle posílí ochranu a sníží riziko probíhajících hrozeb
- **Reakce na incident:** dokončí vyšetřování během několika minut
- **Sledování rizik:** slouží jako nástroj k identifikaci a prevenci destruktivních útoků
- **Správa citlivých míst:** přednostně hlásí citlivá místa a udržuje vaše prostředí přehledné
- **Riziko a dodržování předpisů:** zachovává kontrolu za účelem zmírnění rizika a uvádí ji do souladu s regulačními nařízeními
- **Zabezpečení pracovní zátěže** – příliš mnoho koncových zařízení? Získejte lepší ochranu, kontrolu a přehlednost tím, že sjednotíte svůj bezpečnostní systém koncových zařízení

# 16 000 organizací na celém světě důvěřuje VMware Carbon Black

Existují důvody, proč má tolik organizací (včetně třetiny společností uvedených v žebříčku Fortune 100) důvěru v to, že Carbon Black ochrání jejich prostředí před kybernetickými útoky:

## Posiluje zabezpečení koncových zařízení

Carbon Black nabízí bezpečnost vyšší úrovně. Jde mnohem dál a zajistí každé jednotlivé koncové zařízení. 94 % uživatelů ve výsledku tvrdí, že Carbon Black posílil jejich zabezpečení[2].

## Zvyšuje viditelnost koncových bodů

Kromě posílení bezpečnostního postavení Carbon Black zjednodušuje a sjednocuje, což usnadňuje správu – 75 % uživatelů uvádí, že eliminuje zbytečnou práci v IT oblasti[2].

## Bezpečná investice

Organizace, které nahradí starší řešení zabezpečení koncových zařízení řešením Carbon Black, zaznamenají až 379 % návratnost investic do 3 let a dobu návratnosti počáteční investice kratší než 3 měsíce[2].

## Cloud VMware Carbon Black se integruje do vašeho systému zabezpečení

Povolení vaší dlouhodobé bezpečnostní strategie

### Vylepšete pracovní postupy

Hodí se do vašich stávajících pracovních procesů a vylepšuje je napříč bezpečnostními a IT nástroji

### Zvyšuje viditelnost

Zvyšuje viditelnost a správu napříč koncovými zařízeními, sítěmi, úlohami a kontejnery

### Zvyšuje investice

Pomůže vám získat větší hodnotu z Carbon Black a dalších vašich investic do zabezpečení a IT

## Proč společnost Tech Data pro VMware Carbon Black

**Tech Data je dlouhodobým a zkušeným distributorem VMwaru. Navíc máme specializovaný obchodní tým zaměřený na kybernetickou bezpečnost. Tyto týmy vzájemně spolupracují a dělají vše proto, aby byla vaše zákaznická zkušenost napříč oběma technologickými disciplínami bezproblémová.**

Naši kvalifikovaní pracovníci jsou tu, aby vás provázeli na každém kroku: od výběru správných řešení, přes nasazení až po implementaci, spolu s poprodejní podporou a údržbou. Nabídneme vám nejlepší nacenění a přístup k programovým kanálům.

Tech Data poskytuje take různá školení.

Naše metoda Practice Builder partnerům pomáhá navrhovat nové obchodní modely kolem cloudu, kybernetické bezpečnosti a internetu věcí. Nejen to, nabízíme vám i bezplatná školení prodejních a marketingových týmů. Podívejte se na Tech Data Channel Academy platformu.

Technicky zaměřeným IT profesionálům nabízíme také řadu školení schválených dodavateli, která jsou zakončená certifikací v technické oblasti. Další informace najdete na webové stránce Tech Data's Academy.

Díky školení a dodaným dokumentům si udržíte přehled o základních a odborných znalostech. Kromě toho svou organizaci odlišíte od ostatních tím, že svým zákazníkům poskytnete lepší technologický zážitek.

**Chcete-li se dozvědět více, kontaktujte nás náš tým zde nebo na emailu** vmware_cz@techdata.com

[1] Zdroj: „Zpráva o globálním ohrožení", VMware, https://www.vmwarepartnerdemandcenter.com//ResourceFiles/875814a5-6aec-45ce-a13d-56e9e2eed4fc.pdf

[2] Zdroj: „Celkový dopad VMware Carbon Black Cloud na ekonomiku™", Forrester Consulting, https://www.techdatasecurity.be/topical/forrester-study-vmware-carbon-black-cloud-provides-379-roi/

vmware Carbon Black

Tech Data Advanced Solutions