OCHRANA KANCELÁŘE

McAfee PROTECTED

COPIER MFP LINE OF THE YEAR 2018 BLI BUYERS LAB LINE OF THE YEAR

BLI BUYERS LAB 2019 PICK
Canon uniFLOW Online
Outstanding Cloud Output-Management Solution

COPIER MFP LINE OF THE YEAR 2020 BLI BUYERS LAB LINE OF THE YEAR

Canon

JAK ZABEZPEČENÉ JSOU INFORMACE, KTERÉ MÁTE V KANCELÁŘI?

Dnešní firmy do velké míry spoléhají na informace, vytvářejí složité sítě propojených technologií, procesů, lidí a organizací, které přesahují národní hranice. V éře digitální transformace vznikají nové agilní pracovní postupy, které mění podobu kanceláří a toho, jak lidé vytvářejí, sdílejí a spotřebovávají informace. Zabezpečení dat v tomto spletitém prostředí je mnohem náročnější než kdy předtím a většina firem investuje do propracovaných technologií, jako jsou robustní firewally, aktuální antivirová ochrana, zabezpečený software a mnohé další. Často se jim však nedaří rozpoznat nutnost rozšířit tuto ochranu na své kancelářské tiskárny, které tím vystavují většímu ohrožení, než si vůbec uvědomují.

UVAŽUJTE O TISKÁRNÁCH

Moderní multifunkční tiskárny (MFP) se vyvinuly do výkonných nástrojů, které mají stejně jako servery operační systémy, obrovské pevné disky, připojení k síti a internetu a které uživatelé je sdílejí, aby mohli denně zpracovávat velké počty dokumentů zásadních pro jejich práci.

JAKÁ JSOU RIZIKA?

- Neautorizovaní uživatelé si mohou prohlížet citlivé informace uložené na nechráněných MFP.
- Kvůli nesprávnému provozu je narušena dostupnost vaší tiskové infrastruktury.
- Externí strany se škodlivými úmysly získají přístup do vaší sítě prostřednictvím tiskárny a zneužijí ho k dalším útokům.
- Důvěrné dokumenty zapomenuté ve výstupním zásobníku po vytištění jsou ohroženy.
- Potištěný materiál, který patří různým uživatelům, se smíchá.
- Dokumenty mohou být odeslány faxem nebo v e-mailu nesprávným příjemcům, například v důsledku překlepu.
- Hackeři se zmocní přenášených tiskových nebo skenerových dat.
- Dochází ke ztrátám dat v důsledku nedbalého nakládání s tiskárnami na konci období pronájmu.

„Přijetí základních standardů zabezpečení informací se vyplatí v kancelářích, kde potenciálně pracujete s velkým množstvím dat. Dnešní tiskárny již nejsou němými stroji, jsou to servery, které jen tak mimochodem tisknou na papír.“

(CISO, Publicis Groupe)

BEZPEČNÁ TISKOVÁ ŘEŠENÍ PRO VAŠI FIRMU

Bezpečnost a ochrana soukromí od počátku

Když navrhujeme nebo vybíráme technologie, produkty nebo služby pro naše zákazníky, uvažujeme o pravděpodobném dopadu zabezpečení informací na jejich prostředí. Proto jsou naše kancelářské multifunkční tiskárny vybaveny celou řadou bezpečnostních funkcí, standardních i volitelných, které firmám všech velikostí umožňují dosahovat požadované úrovně ochrany:

ZAŘÍZENÍ | SÍTĚ | DOKUMENTŮ | VAŠÍ SPOLEČNOSTI

MEZINÁRODNĚ UZNÁVANÉ STANDARDY A CERTIFIKACE

Naše multifunkční tiskárny imageRUNNER ADVANCE pravidelně procházejí hodnocením a certifikací pomocí metodologie společných kritérií a v souladu s požadavky norem IEEE2600 pro zabezpečení zařízení generujících tištěné dokumenty.

TESTOVÁNÍ ZABEZPEČENÍ

Společnost Canon využívá jeden z nejpřísnějších postupů testování bezpečnosti v odvětví kancelářského vybavení. Technologie přijímané v našem portfoliu produktů procházejí stejně náročným testováním, jaké očekáváme v oblasti našeho vlastního předmětu podnikání.

Jako lídr odvětví v oblasti vývoje inovativních řešení pro tisk a správu informací určených kancelářím a firmám spolupracuje společnost Canon se zákazníky, aby jim pomáhala osvojit si všezahrnující přístup k zabezpečení informací, přístup, který zohledňuje bezpečnostní dopad naší kancelářské technologie jako součást širšího informačního ekosystému zákazníků.

OCHRANA ZAŘÍZENÍ

Komplexní ochrana vašeho fyzického majetku

ŘEŠENÍ PRO OVĚŘOVÁNÍ UŽIVATELŮ

Chraňte své zařízení před neautorizovaným používáním prostřednictvím implementace řízení přístupu uživatelů na základě ověřování. Patří sem také přidaná výhoda zajištění rychlejšího přístupu uživatelů k jejich preferovanému nastavení a tiskovým úlohám za současného zvýšení zodpovědnosti a kontroly. Naše tiskárny pro firemní oddělení jsou vybaveny flexibilním přihlašovacím řešením uniFLOW Online Express, které umožňuje ověřování uživatelů oproti databázi uživatelů vytvořené na zařízení, ověřování domény prostřednictvím služby Active Directory nebo serveru uniFLOW. Firmy tak získávají možnost řídit přístup k zařízením a současně zajistit rovnováhu mezi pohodlím uživatelů a bezpečností.

OCHRANA DAT NA JEDNOTCE PEVNÉHO DISKU

Multifunkční tiskárna obsahuje v jakémkoli časovém okamžiku velké množství dat, která by měla být chráněna – od tiskových úloh čekajících na vytištění, až k přijatým faxům, naskenovaným datům, adresářům, protokolům aktivity a historii úloh. Zařízení Canon nabízejí řadu opatření na ochranu vašich údajů v každé fázi životnosti zařízení a zajišťují důvěrnost, integritu a dostupnost dat.

SYSTÉM ŘÍZENÍ PŘÍSTUPU

Tato funkce poskytuje granulární řízení přístupu k funkcím zařízení. Správci mohou používat standardní dostupné role nebo vytvářet role šité na míru s požadovanou úrovní přístupových oprávnění. Někteří uživatelé mohou mít například zakázáno kopírovat dokumenty nebo používat funkci odesílání.

NASTAVENÍ ZÁSAD ZABEZPEČENÍ

Nejnovější zařízení imageRUNNER ADVANCE DX jsou vybavena také funkcí nastavení zabezpečení, která správcům umožňuje přejít ke všem nastavením souvisejícím se zabezpečením v jedné nabídce a před vynucením na zařízení je upravit. Po vynucení musí používání zařízení a změny nastavení odpovídat zásadám. Zásady zabezpečení je možné chránit samostatným heslem, takže je přístup do této oblasti omezen na zodpovědné pracovníky IT pověřené zabezpečením. To dodává další úroveň kontroly a zabezpečení.

ŘÍZENÍ SPRÁVY ZAŘÍZENÍ

Konfigurace zařízení, jako je nastavení sítě a další možnosti řízení, jsou k dispozici pouze těm uživatelům, kteří mají oprávnění ke správě. To zabraňuje záměrným nebo náhodným změnám.

PREVENTIVNÍ ZABEZPEČENÍ

Produkty imageRUNNER ADVANCE DX nabízejí řadu bezpečnostních nastavení, která umožňují ochranu tiskáren před útoky. Ověřovací systém při spuštění poskytuje integritu zařízení ihned po zapnutí systému, zatímco software McAfee Embedded Control integritu po celou dobu životnosti zařízení, a to tak, že zabraňuje manipulaci s programy nebo brání spuštění neautorizovaných programů během provozu. Údaje Syslog navíc poskytují informace o stavu zařízení v reálném čase a také možnosti sledování (údaje jsou přístupné příslušnému systému SIEM třetích stran).

JAK BEZPEČNÁ JSOU VAŠE ZAŘÍZENÍ?

1
Jsou zařízení sdílena a umístěna ve veřejných oblastech?

2
Mohou uživatelé získat nezabezpečený přístup k zařízením?

3
Máte nasazená opatření na ochranu informací na pevném disku zařízení?

4
Mohou neautorizovaní uživatelé měnit nastavení zařízení?

5
Vzali jste v úvahu životnost zařízení a jeho bezpečnou likvidaci?

ŠIFROVÁNÍ PEVNÉHO DISKU

Naše zařízení imageRUNNER ADVANCE DX šifrují všechna data na jednotce pevného disku, což ještě posiluje zabezpečení. Bezpečnostní čip zodpovídající za šifrování dat vyhovuje standardu zabezpečení FIPS 140-2 úrovně 2 stanovenému americkou vládou a má certifikaci v rámci programu Cryptographic Module Validation Program (CMVP) zavedeného v USA a Kanadě, a programu Japan Cryptographic Module Validation Program (JCMVP).

MAZÁNÍ PEVNÉHO DISKU

Stejná data, jako jsou kopírovaná nebo skenovaná data snímku, i data dokumentů vytištěná z počítače, jsou pouze dočasně uložena na jednotce pevného disku a po dokončení operace se smažou. Aby bylo zajištěno, že nezůstanou zachována žádná zbývající data, jsou naše zařízení vybavena pevným diskem, který nabízí možnost rutinního mazání zbývajících dat v rámci zpracování úlohy.

INICIALIZACE VŠECH DAT A NASTAVENÍ

Aby se zabránilo ztrátě dat při výměně nebo likvidaci pevného disku, můžete přepsat všechny dokumenty a data na pevném disku a obnovit výchozí nastavení přístroje.

ZRCADLENÍ PEVNÉHO DISKU*

Firmy mají možnost zálohovat data na jednotce pevného disku zařízení pomocí dalšího přídavného pevného disku. Při zrcadlení jsou data na obou jednotkách pevného disku plně šifrovaná.

*Volitelné u vybraných modelů. Podrobné informace o dostupnosti funkcí a možností v rámci kancelářského tiskového portfolia vám poskytne zástupce společnosti Canon.

ZABEZPEČENÍ SÍTĚ

MŮŽE TISKÁRNA OHROZIT VAŠI SÍŤ?

- Necháváte síťové porty otevřené útoku?
- Mohou hosté tisknout a skenovat, aniž by to ohrozilo vaši síť?
- Jsou zásady vaší firmy týkající se používá vlastních zařízení bezpečné a mají zajištěnou podporu?
- Jsou datové toky tisku z počítače do výstupního zařízení zašifrovány?
- Jsou tisková a skenerová data při přepravě zabezpečena?

Společnost Canon nabízí řadu řešení zabezpečení, která zajistí bezpečnost vaší sítě a dat před interními a externími útoky.

FILTROVÁNÍ IP A MAC ADRES

Chraňte svou síť před neoprávněným přístupem třetích stran tím, že umožníte pouze komunikaci se zařízeními s konkrétní IP nebo MAC adresou pro odchozí i příchozí komunikaci.

KONFIGURACE PROXY SERVERU

Nastavte proxy server tak, aby zvládal komunikaci místo vašeho přístroje, a používejte tuto funkci při připojování zařízení mimo síť.

OVĚŘOVÁNÍ IEEE 802.1X

Neautorizovaný síťový přístup je zablokován přepínačem LAN, který uděluje přístupová oprávnění pouze těm klientským zařízením, která mají oprávnění ze serveru pro ověřování.

KOMUNIKACE IPSEC

Komunikace IPSec brání třetím stranám v příjmu nebo falšování IP paketů přenášených přes síť IP.

Používejte šifrovanou komunikaci TLS k prevenci falšování, zkreslování a neoprávněného zasahování do dat, která jsou vyměňována mezi přístrojem a ostatními zařízeními, jako jsou počítače.

KONTROLA PORTU

V rámci nastavení zásad zabezpečení nakonfigurujte porty.

CERTIFIKACE AUTOMATICKÉ REGISTRACE

Díky této funkci se značně snižuje zátěž spojená s uchováváním certifikátů zabezpečení. Pomocí technologie uznávané v odvětví může správce systému automaticky aktualizovat a vydávat certifikáty a přitom zajistit, že je celou dobu vyhověno zásadám zabezpečení.

SLEDOVÁNÍ PROTOKOLŮ

Různé protokoly umožňují sledovat aktivitu týkající se vašeho zařízení, včetně blokovaných žádostí o komunikaci.

WI-FI DIRECT

Povolte vzájemné propojení pro mobilní tisk, aniž by mobilní zařízení potřebovalo přístup do vaší sítě.

ŠIFROVÁNÍ DAT PŘEPRAVOVANÝCH DO ZAŘÍZENÍ A MIMO NĚ

Tato možnost šifruje tiskové úlohy přenášené z počítače uživatele do multifunkční tiskárny. Díky povolení univerzální sady funkcí zabezpečení mohou být šifrována také naskenovaná data ve formátu PDF.

MOŽNOSTI MOBILNÍHO TISKU PRO HOSTY

Náš software pro zabezpečený tisk v síti a správu skenování řeší běžná rizika zabezpečení pro mobilní tisk a tisk pro hosty tak, že poskytuje externí cesty k odesílání tiskových úloh přes e-mail, web a mobilní aplikaci. Tím se minimalizují vektory útoku díky uzamknutí MDF na zabezpečený zdroj.

DUÁLNÍ SÍŤ

Nejnovější technologie již umožňují připojení k duální síti: Zatímco primární síť bude vždy kabelová, sekundární linka může teď být buď bezdrátová, nebo kabelová, což zajistí přesnější a bezpečnější oddělení sítí.

OCHRANA DOKUMENTŮ

Všechny firmy pracují s citlivými dokumenty, jako jsou smlouvy, informace o platech zaměstnanců, údaje o zákaznících, plány výzkumu a vývoje a další. V případě, že dokumenty padnou do špatných rukou, důsledky se pohybují od poškození dobré pověsti až k siným pokutám nebo trestnímu řízení.

Společnost Canon nabízí řadu řešení zabezpečení na ochranu vašich citlivých dokumentů po celou dobu jejich životnosti.

DŮVĚRNOST TIŠTĚNÉHO DOKUMENTU

Zabezpečený tisk
Uživatel může nastavit kód PIN pro tisk, aby tisk dokumentu mohl proběhnout až po zadání správného kódu PIN do zařízení. Díky tomu mohou zabezpečit ty dokumenty, které považují za důvěrné.

Blokování všech tiskových úloh
Na zařízení imageRUNNER ADVANCE DX může správce vynutit zablokování všech odeslaných tiskových úloh, aby se uživatelé museli nejprve přihlásit a teprve potom bylo možné tisknout úlohy. Důvodem je ochrana důvěrnosti všech tištěných materiálů.

Poštovní schránky
Tiskové úlohy nebo skenované dokumenty je možné uchovávat ve schránce pro pozdější přístup. Poštovní schránky lze chránit PIN kódem, aby se zajistilo, že uložený obsah může zobrazit pouze přidělený vlastník. Tento bezpečný prostor na zařízení je vhodný k uchovávání dokumentů, které se tisknou často (například formuláře), ale vyžadují pečlivou manipulaci.

Zabezpečený tisk uniFLOW*
Díky zabezpečenému tisku uniFLOW MyPrintAnywhere uživatelé odesílají tiskové úlohy prostřednictvím univerzálního ovladače a vyzvedávají si je na libovolné tiskárně v síti.

ODRAZENÍ NEBO PREVENCE DUPLIKOVÁNÍ DOKUMENTŮ

Tisk s viditelnými vodoznaky
Ovladače mohou zajistit tisk viditelných značek na stránce, překrytých nad nebo pod obsahem dokumentu. To odrazuje od kopírování, protože si uživatelé jsou vědomi důvěrné povahy dokumentu.

Tisk/kopírování s neviditelnými vodoznaky
Když je tato možnost povolená, dokumenty lze tisknout nebo kopírovat s vloženým skrytým textem na pozadí, takže se v případě duplikování text na dokumentu objeví a funguje jako odrazující prostředek.

Prevence ztráty dat na korporátní úrovni
Upgradujte základní schopnosti prevence ztráty dat na iW SAM Express v kombinaci s uniFLOW. Toto serverové řešení umožňuje zachycovat a archivovat dokumenty zasílané na tiskárnu a z tiskárny, analyzovat a interpretovat pomocí textu nebo atributů s jednoznačným cílem zabránit hrozbám zabezpečení.

Sledování původu dokumentu*
Prostřednictvím vloženého kódu je možné vysledovat původ dokumentu až ke zdroji.

JAK BEZPEČNÉ JSOU VAŠE DOKUMENTY?

1
Je neoprávněným uživatelům zabráněno v přístupu k citlivým dokumentům v tiskárně?

2
Můžete zajistit důvěrnost všech dokumentů, které procházejí přes sdílené zařízení?

3
Dokážete vysledovat původ tištěných dokumentů?

4
Nemohl by někdo odejít od tiskárny s citlivými dokumenty?

5
Dokážete při odesílání dokumentů ze zařízení zajistit prevenci běžných chyb?

PROCVIČENÍ KONTROLY NAD ODESÍLÁNÍM A FAXOVÁNÍM DOKUMENTŮ

Omezení cílů odesílání
Aby se snížilo riziko úniku informací, mohou správci omezit dostupné destinace pro odesílání pouze na osoby v adresáři nebo na serveru LDAP, adresu přihlášeného uživatele nebo určité domény.

Zakázání automatického dokončování adres
Zabraňte zaslání dokumentů na nesprávné adresy tím, že zakážete automatické dokončování e-mailových adres.

Ochrana adresáře
Nastavte PIN kód na ochranu adresáře zařízení před neoprávněnými úpravami ze strany uživatelů.

Ověření čísla faxu
Zabraňte odesílání dokumentů nezamýšleným příjemcům tím, že budete po uživatelích požadovat dvojí zadání čísla faxu pro potvrzení před odesláním.

Důvěrnost přijímaného faxu
Nastavte přístroj tak, aby dokumenty ukládal do paměti bez tisku. Můžete také chránit důvěrnost přijímaných faxových dokumentů tím, že použijete podmínky určující místo uchovávání na důvěrnou schránku s doručenou poštou a kódy PIN.

OVĚŘTE PŮVOD A PRAVOST DOKUMENTŮ PROSTŘEDNICTVÍM DIGITÁLNÍCH PODPISŮ

Podpis zařízení
Podpisy zařízení lze použít na naskenovaných dokumentech ve formátu PDF nebo XPS pomocí klíče a mechanismu certifikátu, aby mohl příjemce ověřit původ i pravost dokumentu.

Podpis uživatele*
Tato možnost uživatelům umožňuje poslat soubor PDF nebo XPS s jedinečným digitálním podpisem uživatele získaným od certifikačního úřadu. Tímto způsobem může příjemce ověřit, který uživatel dokument podepsal.

POUŽITÍ ZÁSAD S INTEGRACÍ SPRÁVY ŽIVOTNOSTI ADOBE ES

Uživatelé mohou zabezpečit soubory PDF a použít trvalé a dynamické zásady k řízení přístupových práv a práv používání k ochraně citlivých a cenných informací před neúmyslným nebo škodlivým zpřístupněním.

Zásady zabezpečení jsou uchovávány na úrovni serveru, takže je možné po distribuci souboru změnit práva. Řadu imageRUNNER ADVANCE DX lze konfigurovat tak, aby umožňovala integraci Adobe® ES.

*Volitelné. Podrobné informace o dostupnosti funkcí a možností v rámci kancelářského tiskového portfolia vám poskytne zástupce společnosti Canon.

ZABEZPEČENÍ PODNIKOVÝCH INFORMACÍ

Společnost Canon může přispět k celkové ochraně informací ve vaší organizaci.

DOKONČENÍ ŘÍZENÍ PRO POTŘEBY KONCOVÉHO ZAZNAMENÁNÍ A VÝSTUPU

Díky našemu modulárnímu výstupnímu softwaru pro správu si firmy mohou užívat bezpečného sdílení síťových zařízení, což jim umožní bezpečný tisk úloh na libovolné tiskárně připojené k výstupnímu serveru pro správu. Uživatelé mobilních zařízení mají podporu centrálně řízené služby, zatímco interní a hostující uživatelé mají bezpečný přístup k tisku z mobilních zařízení.
Pro účely podnikového zachycování poskytuje skenovací modul zachycení, kompresi, konverzi a distribuci dokumentů z multifunkčního zařízení do různých míst určení, včetně cloudových systémů. Můžete také bezpečně přesměrovávat tiskové úlohy na nejvhodnější tiskárnu, a optimalizovat tak náklady na tisk každého dokumentu. Naše řešení zlepšuje bezpečnost dokumentů v celé vaší firmě, v kombinaci s plným účtováním dokumentů. To poskytuje kompletní přehled o aktivitě podle uživatele, zařízení a oddělení.

CENTRALIZOVANÁ SPRÁVA TISKOVÉHO SYSTÉMU

Náš software pro správu zařízení IW MC umožňuje aktualizovat nastavení zařízení, zásady zabezpečení, hesla a certifikáty a firmware a jejich integraci do vašeho tiskového systému zařízení Canon v celé síti. To vašemu týmu IT šetří cenný čas a zajišťuje udržování aktuálního zabezpečení tiskové infrastruktury.

KOMPLEXNÍ AUDITY DOKUMENTŮ

Architektura služeb našich kancelářských dokumentů může být zdokonalena o možnosti na objednání, které zachytí úplný záznam (např. sken plus metadata úlohy) u všech dokumentů prostřednictvím zařízení imageRUNNER ADVANCE DX.

ŘÍZENÉ TISKOVÉ SLUŽBY

Canon MPS kombinuje inovativní technologii a software se správnými službami, abyste měli možnost požadovaného tiskového prostředí a prostředí pro dokumenty bez zátěže pro IT, která je s tím spojená. Díky aktivní správě a průběžné optimalizaci tiskové infrastruktury a pracovních postupů týkajících se dokumentů vám můžeme pomoci dosáhnout cílů v oblasti zabezpečení a přitom optimalizovat náklady a zvýšit produktivitu v celé vaší firmě.

VLASTNÍ VÝVOJ

Máme tým vlastních vývojářů, kteří navrhují a vyvíjejí přizpůsobená řešení vyhovující vaší konkrétní situaci nebo jedinečným požadavkům.

JAK INKLUZNÍ JE PŘÍSTUP K ZABEZPEČENÍ V RÁMCI VAŠÍ SPOLEČNOSTI?

- Jsou vaše zásady zabezpečení rozšířeny také na vaši řadu multifunkčních zařízení?
- Jak zajišťujete, že je tisková infrastruktura aktuální a vylepšení a opravy chyb jsou implementovány včas a účinně?
- Mohou hosté tisknout a skenovat, aniž by to ohrozilo vaši síť?
- Jsou zásady používání vlastních zařízení na pracovišti bezpečné a podporují je všechna vaše tisková zařízení?
- Má váš tým IT dost času na vyšetřování záležitostí ohledně zabezpečení?
- Je zajištěna správná rovnováha mezi poskytováním zabezpečení a pohodlím uživatelů?

PROČ CANON?

ODBORNÉ ZNALOSTI

Integrace hardwaru a softwaru snižuje potenciál narušení systému

PARTNERSTVÍ

Pomáháme zákazníkům lépe podnikat s vědomím, že mají **aktivně řešené hrozby zabezpečení dat.**

SLUŽBY

Stejný tým pověřený zabezpečením informací pro zákazníky spravuje naše interní zabezpečení IT.

Bereme v potaz všechny potenciální hrozby – uvnitř brány firewall vaší společnosti i mimo ni.

INOVACE

Do našich produktů a služeb **začleňujeme vylepšené způsoby,** jak minimalizovat pravděpodobnost hrozeb týkajících se zabezpečení informací.

SC 2017 awards EUROPE

„Vysoce oceňovaný“ v kategorii nejlepší tým zabezpečení v soutěži **2017 SCA Awards Europe,** v rámci níž jsou hodnoceny znalosti v oblasti počítačového zabezpečení.

Canon U.S.A. získala dvě **ocenění BLI PaceSetter 2017** (Zabezpečení snímkování dokumentů a mobilní tisk).

Canon Inc.
Canon.com

Canon Europe
Canon-europe.com

Canon CZ s.r.o.
Jankovcova 1595/14B
170 00 Prague 7 - Holešovice
Tel. +420 225 280 111
Fax +420 225 280 311
canon.cz

Czech edition

Canon

McAfee PROTECTED