ManageEngine

Katalog Produktů

POWERING IT AHEAD

Klíčové vlastnosti ManageEngine

Správa mobilních zařízení.

STR. 7

Mobile Device Manager Plus

SPRÁVA AD

Správa a řízení Active Directory.

STR. 16

ADManager Plus

ITSM

Inventář a správa aktiv.

STR. 9

AssetExplorer

Správa identit a hesel a uživatelská samoobsluha.

STR. 18

ADSelfService Plus

Zpracování požadavků a zákaznická podpora.

STR. 8

SupportCenter Plus

Nástroj na zálohu a obnovení Active Directory.

STR. 20

Recovery Manager Plus

Audit a reporting pro Exchange server.

STR. 19

Exchange Reporter Plus

Integrovaná správa Active Directory a Exchange.

STR. 23

AD360

Pohodlná správa vícero prohlížečů v jednom rozhraní.

STR. 13

Browser Security Plus

Správa a reporting pro platformu Office365.

STR. 21

O365 Manager Plus

Audit změn v Active Directory.

STR. 17

ADAudit Plus

Správa aktualizací/patchů aplikací.

STR. 14

Patch Manager Plus

Správa a reporting pro Sharepoint.

STR. 22

SharePoint Manager Plus

Nástroje podporující vzdálené ovládání pracovních stanic

STR. 15

Remote Access Plus

Integrované spravování logů a audit Active Directory.

STR. 35

LOG360

Správa SSH klíčů a SSL certifikátů.

STR. 37

Key Manager Plus

ManageEngine

POWERING IT AHEAD

Správa koncových a mobilních zařízení.

STR. 6

Desktop Central

Deployment operačních systémů.

STR. 11

OS Deployer

Správa aktualizací aplikací.

STR. 12

Patch Connect Plus

Helpdesk se správou aktiv založený na metodice ITIL.

STR. 4

ServiceDesk Plus

MONITORING IT

Analytický systém pro Business Intelligence.

STR. 5

Analytics Plus

Monitoring webových stránek a aplikací z globální perspektivy (Cloud).

STR. 27

Site24x7

Integrovaný monitoring IT infrastruktury z pohledu poskytovaných služeb. Analýza IT komponent orientovaná na poskytované služby.

STR. 28

Applications Manager

Centrální úložiště hesel a správa privilegovaných účtů.

STR. 36

Password Manager Pro

Komplexní správa a monitoring IT infrastruktury.

STR. 25

OpManager

Správa IP adres a nástroj na mapování portů v přepínači v jednotném pohledu.

STR. 30

OpUtils

Zabezpečení cloudu a správa logů.

STR. 38

Cloud Security Plus

Spravování citlivých údajů.

STR. 39

Data Security Plus

Správa konfigurace FW & Správa logů.

STR. 31

Firewall Analyzer

Správa periferních zařízení a ochrana před únikem dat.

STR. 40

Device Control Plus

Detekce zranitelností a hrozeb.

STR. 41

Vulnerability Manager Plus

Monitoring propustnosti sítě & Analýza síťového provozu.

STR. 32

NetFlow Analyzer

BEZPEČNOST IT

Správa konfigurace sítě.

STR. 34

Network Configuration Manager

+ ITSM

Helpdesk se správou aktiv založený na metodice ITIL

ServiceDesk Plus

ServiceDesk Plus je kompletní systém Helpdesk založený na knihovně ITIL. Aplikace funguje na bázi webového prohlížeče. Díky tomu umožňuje registraci hlášení pomocí prohlížeče, ale také e-mailem, telefonicky nebo osobně.

Aplikace automatizuje činnosti spojené s obsluhou hlášení, včetně předávání hlášení příslušným skupinám podpory a servisním pracovníkům, odesílání oznámení servisním pracovníkům a uživatelům a ověření shody smluv SLA. V jednom balíčku jsou integrovány takové moduly, jako registrace a správa incidentů - včetně tvorby katalogu hlášení, registrace a správy žádostí o služby - v tom možnost tvorby katalogu služeb pro vybrané uživatele, modul správy problémů (s možností propojení mnoha incidentů do jednoho problému), rozsáhlé správy změn. ServiceDesk umožňuje evidenci IT i ne-IT aktiv. Evidence aktiv a softwaru je spojena s modulem nákupů IT, se správou servisních smluv, a také modulem správy licencí pro software.

ServiceDesk nabízí velmi přehledný a uživatelsky přívětivý samoobslužný portál pro koncové uživatele, pro které je navíc připravena dedikovaná databáze. ServiceDesk Plus zefektivňuje práci servisních pracovníků, kterým nabízí možnost přípravy příslušných rolí, v souladu s oprávněním daného technika.

K NEJDŮLEŽITĚJŠÍM FUNKCÍM SERVICEDESK PLUS PATŘÍ:

- Obsluha aplikace prostřednictvím internetového prohlížeče s využitím elektronické pošty
- Oddělená instalace na serveru, bez nutnosti instalace jakéhokoliv softwaru na počítačích uživatelů
- Krátká implementace, nevyžadující změny nebo přerušení provozu firmy
- Integrovaný nástroj vzdálené plochy, usnadňující obsluhu servisních hlášení
- Automatická inventarizace aktiv
- Automatická synchronizace údajů o uživatelích z ActiveDirectory
- Podpora mobilních servisních pracovníků - obsluhujících hlášení pomocí mobilních zařízení
- Možnost integrace s monitorovacími zařízeními (OpManager, Applications Manager)
- Možnost integrace s vyspělým nástrojem pro správu pracovních stanic (Desktop Central)
- Software je dostupný v českém jazyce.

Analytický systém pro Business Intelligence

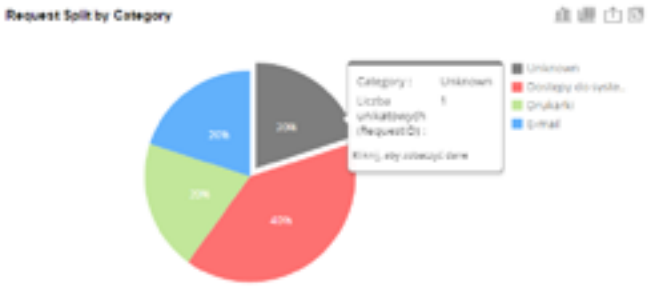
Analytics Plus

Analytics Plus je robustní analytický nástroj, založený na internetovém prohlížeči, který umožňuje převod IT dat do přehledných výkazů a tabulek ukazatelů. Díky Analytics Plus se mohou správci rozhodovat rychle a jistě. Analytics Plus je také dostupný v modelu v cloudu, kde se jmenuje Zoho Reports

Analytický systém má hotovou integraci se ServiceDesk Plus, díky tomu pomáhá zvýšit efektivitu IT při poskytování služeb a zvyšuje přehlednost dat s ITSM. Systém obsahuje přes 100 předdefinovaných výkazů a přes 80 hotových ukazatelů KPI. Analytics Plus umožňuje konfiguraci vlastních výkazů a tabulek ukazatelů, které lze následně poskytnout vybraným osobám, skupinám osob nebo zobrazovat na internetových stránkách a multimediálních tabulích.

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:

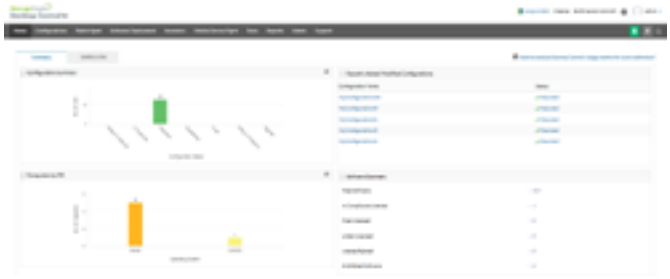
- Okamžité a upravitelné výkazy díky funkci drag&drop, s jejíž pomocí snadno sestavíte a uzpůsobíte výkazy a tabulky ukazatelů
- Možnost firemního označení tabulek ukazatelů a výkazů
- Analytics Plus automaticky stahuje údaje z integrovaných databází a aktualizuje tabulky ukazatelů a výkazy
- Zpřístupnění výkazů podle harmonogramu, jejich včasné a bezpracné odesílání e-mailem
- Možnost konfigurace náhledu aplikací, výkazů a tabulek ukazatelů
- Sdílení tabulek a výkazů při kolektivní práci



Správa koncových a mobilních zařízení

Desktop Central

Desktop Central je integrovaný software pro správu počítačů a přenosných zařízení, který umožňuje správu serverů, laptopů, pracovních stanic, smartfonů a tabletů z jednoho centrálního místa.



Desktop Central kompletně automatizuje správu IT aktiv, počínaje od snadné konfigurace operačních systémů Windows, komplikovanou distribucí softwaru konče. Obsluhuje operační systémy Windows, Linux a Mac. Desktop Central automatizuje pravidelné úkoly, jako instalace softwaru, oprav a service packů, standardizuje pracovní stanice nastavením takových konfigurací, jako tapety, zástupci, tiskárny, atd., chrání pracovní stanice blokováním USB nebo aplikací politiky bezpečnosti, umožňuje audit shody licencí, detekuje použití zakázaného softwaru. Navíc Desktop Central pomáhá správcům při automatizaci, standardizaci, ochraně a auditu jejich sítě.

Distribuce softwaru na jednotlivé pracovní stanice a skupiny pracovních stanic. Systém umožňuje instalaci balíků MSI, EXE, ISS, u kterých nabízí možnost přiřazení argumentů a přidání vybraných skriptů, spouštěných ve vybrané fázi instalace.
Správa oprav pro systémy Microsoft, Apple a mnoho jiných. Systém také nabízí možnost průzkumu kondice systémů, měřitelné z hlediska nezbytných záplat.
Správa aktiv, včetně aktiv, které nesouvisejí s IT. Systém umožňuje inventarizaci a dálkovou správu aktiv. Mechanismus detekce změn v aktivech, včetně detekce zakázaného softwaru, má poplachový modul a také mechanismus automatizace proaktivních a nápravných opatření. Navíc systém umožňuje správu licencí softwaru a SLA pro aktiva.
Vzdálená konfigurace všech pracovních stanic a mobilních zařízení fungujících na systémech Android a iOS.
Sdílení plochy a vzdálená kontrola plochy umožňuje podporu uživatelů v nestandardních případech. Modul může informovat uživatele o vzdáleném připojení, odeslat požadavek na souhlas. Umožňuje také úplné převzetí kontroly nad stanicí - bez možnosti zásahu ze strany koncového uživatele.

Správa úspory energie v organizaci, včetně správy plánu napájení pracovních stanic.
Správa portů USB, počínaje úplnou blokací portů, po blokaci pro vybraná zařízení.
Systémové nástroje Windows zajišťují příslušný výkon pracovních stanic uživatelů.
Široké možnosti výkazů, včetně výkazů z Active Directory. Systém má také generátor výkazů a dotazů pro náročnější uživatele.
Stejně, jako DesktopCentral provádí automatizaci konfigurace pracovních stanic, obsluhuje také mobilní zařízení. Aplikace umožňuje konfiguraci profilů pro dedikované skupiny zařízení a uživatelů, konfiguraci ochrany, systémů a funkcí, včetně nastavení: Wifi, Mail, Internet, atd. Aplikace podporuje přístupy BYOD a BYOA.

Správa mobilních zařízení

Mobile Device Manager Plus

Neustále rostoucí počet uživatelů mobilních zařízení vytváří větší možnost ohrožení podniků, neboť citlivé firemní údaje se nacházejí „v kapse“ pracovníků a zcizení takového zařízení může způsobit citelnou ztrátu dat organizace. Proto by MDM (Mobile Device Management) neměl být volbou, ale povinností. Mobile Device Manager Plus zdokonaluje realizaci úkolů spojených se správou mobilních zařízení (MDM). Systém umožňuje konfiguraci tabletů a smartfonů z centrální lokace. Software je dostupný ve verzích On-premise a Cloud.

JAKÉ NABÍZÍ FUNKCE?

- Registrace zařízení jednotlivě, hromadně nebo umožnění registrace zařízení uživatelů s dvoustupňovým ověřením.
- Distribuce vlastních i komerčních aplikací. Odstranění a vyřazení aplikace ze zakázaného seznamu.
- Tvorba a konfigurace politik a profilů pro různé pobočky a role v organizaci.
- Skenování a ukládání informací o instalovaných aplikacích, omezeních, certifikátech a hardwarových parametrech mobilních zařízení.
- Konfigurace restriktivní politiky bezpečnosti - přístupový kód, blokace zařízení - to vše za účelem zajištění ochrany dat organizace proti vnějším hrozbám.
- Audit mobilních zařízení díky standardně dostupným výkazům.

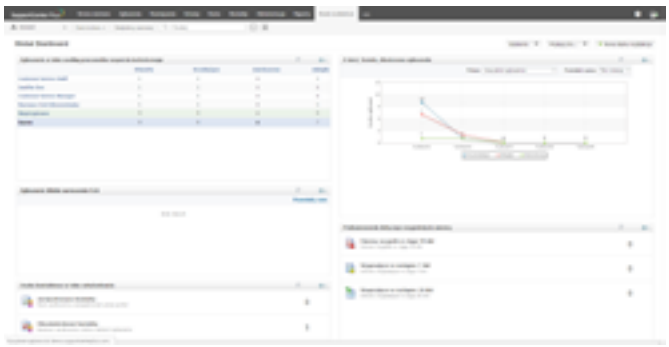
Centrální systém správy mobilních zařízení je především účinnou metodou pro zavádění tabletů a smartphonů do organizační struktury, garancí bezpečnosti dat organizace a přehledný systém distribuce aplikací nezbytných pro realizaci úkolů pracovníků.

Systém zajišťuje snadné a přehledné rozdělení struktury dat na soukromá a firemní. Díky MDM Plus uživatelé získávají jednoduchý mechanismus stahování aplikací zpřístupněných organizací a mají zajištěnu bezpečnost dat v případě zcizení zařízení.

Zpracování požadavků a zákaznická podpora

SupportCenter Plus

SupportCenter Plus je aplikace podporující obsluhu uživatele, založená na internetovém prohlížeči. Nabízí registraci hlášení, správu účtů a kontaktů, správu smluv SLA a databázi, to vše za velmi přijatelnou cenu. Tento software podporuje sledování a řešení problémů, které se vyskytují u uživatelů, a současně zvyšuje spokojenost a kvalitu servisu firmy. Aplikace je dostupná v českém jazyce.



Web Portálu Podpory umožňuje značnou redukci počtu telefonátů uživatelů do oddělení podpory. Uživatel může samostatně prohledat databázi, přidávat nová hlášení nebo ověřovat statusy dříve přidaných hlášení.

Databáze založená na internetovém prohlížeči umožňuje pracovníkům podpory rychlejší řešení problémů. Vyspělý systém prohledávání údajů umožňuje rychlejší nalezení vhodných řešení. S jeho pomocí získávají uživatelé často již během prvního rozhovoru odpovědi na hlášené problémy, což zvyšuje jejich spokojenost.

Tento modul umožňuje registraci a správu všech účtů a kontaktů uživatelé firmy, to má pozitivní vliv na úroveň jejich spokojenosti.

Help desk, který se snadno obsluhuje, pomáhá firmě automatizovat proces obsluhy hlášení, aby mohla svým uživatelům dodávat konstantní a profesionální služby v nejvyšší kvalitě.

Správně definovaná úroveň kvality zvyšuje úroveň spokojenosti uživatelů. V SupportCenter Plus lze definovat podmínky smluv SLA, monitorovat jejich shodu a tvořit varianty eskalace v případě nedodržení sjednaných podmínek smlouvy SLA.

Pracovníci oddělení podpory mají přístup k seznamu všech produktů, které uživatel zakoupil, což zlepšuje a zrychluje obsluhu hlášení. Sami uživatelé mohou také sledovat a spravovat jednotlivé informace o zakoupeném produktu.

Inventář a správa aktiv

AssetExplorer

AssetExplorer je kompletní řešení pro správu IT aktiv. Nabízí kontrolu a přehled celé infrastruktury podniku, jak IT, tak aktiv nesouvisejících s informatikou. Pomocí AssetExplorer může správce z jednoho místa sledovat a spravovat předávání vlastnictví všech aktiv. AssetExplorer skenuje a audituje všechny pracovní stanice v síti LAN, WAN a VPN.

AssetExplorer se připojuje do Active Directory a skenuje všechny nalezené pracovní stanice. Za použití síťového skenování AssetExplorer dokáže najít pracovní stanice založené na systému Linux, síťové tiskárny, routery a switche. Podrobný výkaz skenování umožňuje náhled do detailů vybavení instalovaného na pracovních stanicích a instalovaného softwaru. Osoby, které spravují firemní aktiva, mohou pomocí výkazů získat detailní informace o vybavení a softwaru instalovaném na pracovních stanicích.

SPRÁVA LICENCÍ

AssetExplorer skenuje, automatizuje a detekuje všechny dostupné softwary na každém počítači v síti. Osoby, které jsou ve firmě odpovědné za software, mohou snadno získat informace o množství instalovaného softwaru v rozlišení na licencovaný a nelicencovaný.

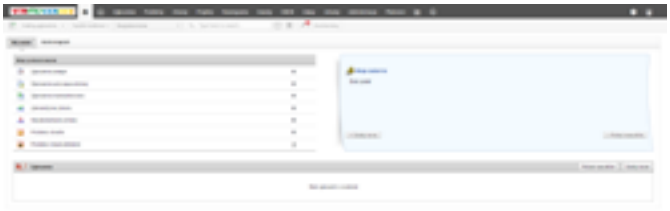
SPRÁVA SERVISNÍCH SMLUV

AssetExplorer podporuje efektivní správu servisních smluv s různými dodavateli. Informuje a připomíná blížící se konec platnosti smlouvy za účelem jejího případného prodloužení. Detailní výkazy, s rozlišením např. na maximální výdaje nebo z hlediska dodavatelů, umožňují efektivnější rozhodování.

Systém helpdesk se správou aktiv založený na metodice ITIL pro MSPs

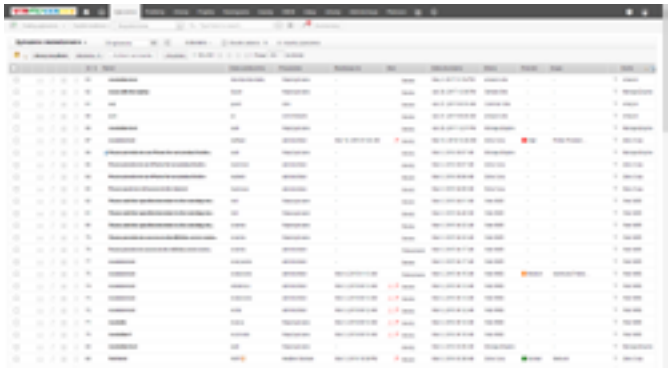
ServiceDesk Plus MSP

ServiceDesk Plus je kompletní systém Helpdesk, založený na knihovně ITIL. Aplikace funguje na bázi webového prohlížeče. Díky tomu umožňuje registraci hlášení pomocí prohlížeče, ale také e-mailem, telefonicky nebo osobně.



Aplikace automatizuje činnosti spojené s obsluhou hlášení, včetně předávání hlášení příslušným skupinám podpory a servisním pracovníkům, odesílání oznámení servisním pracovníkům a uživatelům a ověření shody se smlouvami SLA. V jednom balíčku jsou integrovány takové moduly, jako registrace a správa incidentů - včetně tvorby katalogu hlášení, registrace a správy žádostí o služby - v tom možnost tvorby katalogu služeb pro vybrané uživatele, modul správy problémů (s možností propojení mnoha incidentů do jednoho problému), rozsáhlé správy změn. ServiceDesk umožňuje evidenci IT i ne-IT aktiv. Evidence zásob a softwaru je spojena s modulem nákupů IT, se správou servisních smluv, a také modulem správy licencí pro software. ServiceDesk nabízí velmi přehledný a uživatelsky přívětivý samoobslužný portál pro koncové uživatele, pro které je navíc připravena dedikovaná databáze.

ServiceDesk Plus zefektivňuje práci servisních pracovníků, kterým nabízí možnost přípravy příslušných rolí, v souladu s oprávněním daného technika.



Software je kromě verze dostupné pro interní oddělení IT dostupný také ve verzích pro firmy MSP (Managed Service Provider). Největší rozdíl mezi ServiceDesk Plus a ServiceDesk Plus MSP je možnost obsluhy mnoha klientských účtů.

Deployment operačních systémů

OS Deployer

OS Deployer je komplexní nástroj pro distribuci operačních systémů, který umožňuje tvorbu obrazů systémů a aplikací a následně rychlou a snadnou instalaci na podnikových počítačích.

Díky možnosti tvorby a distribuce obrazů operačních systémů OS Deployer pomáhá tvořit a rychle implementovat standardní operační systém pro celou organizaci. Zkracuje tak dobu nezbytnou pro podporu, trénink a správu. OS Deployer vytváří přesnou kopii hard disku, obsahující standardní konfiguraci, operační systém a všechny aplikace, která může být instalována na mnoha počítačích současně. Systém je integrován se softwarem pro správu pracovních stanic - Desktop Central. To umožňuje rychlé a účinné přidání počítače do organizace, od nahrání operačního systému po komplexní správu pracovní stanice.

JAKÉ NABÍZÍ FUNKCE?

- Uchovávání image a jeho distribuce
- Šablony distribuce
- Pružné možnosti distribuce
- Nastavitelné možnosti tvorby image
- Bootování z nosičů image
- Lokální distribuce image
- Doladění po procesu distribuce
- Univerzální distribuce
- Implementace naplánované ve Wake-on-LAN

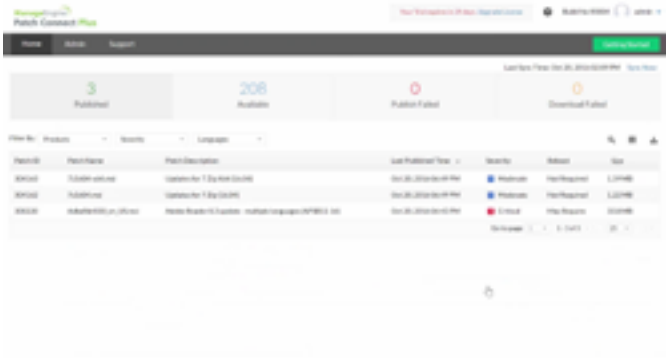
Správa aktualizací aplikace

Patch Connect Plus

Microsoft SCCM je skvěle vybaven pro správu pracovních stanic Windows a jejich aplikací. Hlavním omezením SCCM je však neschopnost nahrávat aktualizace pro programy ostatních výrobců SW. Toto je hlavní zdroj obtíží pro IT administrátory, protože musí udržovat konzistentní a aktualizovanou IT infrastrukturu s použitím více nástrojů pro správu.

ManageEngine Patch Connect Plus je nástroj, který pomáhá implementovat opravy pro více než 250 aplikací třetích stran, jako Adobe, Java nebo WinRAR a dalších, pomocí stávajícího Microsoft System Center Configuration Manageru. Díky tomu je problém patchováním aplikací od jiných výrobců než je Microsoft, vyřešen integrací Patch Connect Plus s SCCM.

Kombinace Patch Connector Plus se současnými možnostmi SCCM umožňuje nahrávání aktualizací téměř pro každou aplikaci. Umožňuje pravidelné skenování patchů za účelem zefektivnění workflow, které Vám umožňuje rozhodnout se a zvolit, kdy se mají aktualizace nahrávat. Instalace softwaru je jednoduchá a díky integraci se službami SMTP je možné zasílat administrátorům oznámení o nově vydaných aktualizacích.



Pohodlná správa vícero prohlížečů v jednom rozhraní

Browser Security Plus

Browser Security Plus je SW řešení , které pomáhá správcům IT kontrolovat a zabezpečovat webové prohlížeče v interních sítích. Umožňuje jim uplatňovat zásady zabezpečení, mít pod kontrolou rozšíření prohlížečů, pluginy a případně je i zablokovat. Také umožňuje zajistit soulad s korporátnímipravidly týkajícími se prohlížečů a chránit tak síť před hrozbami s nimi souvisejícími.

ODHALOVÁNÍ NEDOSTATKŮ A JEJICH SPRÁVA

- Získejte úplný přehled o trendech v používání prohlížečů a o jejich doplňcích ve Vaší síti.
- Zjistěte, které doplňkové komponenty mohou způsobit narušení zabezpečení.
- Spravujte a kontrolujete doplňky prohlížečů .

SPRÁVA BEZPEČNOSTNÍCH KONFIGURACÍ A JEJICH KOMPATIBILITY

- Aplikujte konfiguraci zabezpečení na počítačích, abyste zabránili hrozbám spojeným s prohlížeči.
- Vytvoření a zajištění shody s platnými konfiguracemi zabezpečení.
- Chraňte podniková data před krádeží ověřovacích údajů, phishingovými útoky a náhodnými úniky dat.

KONTROLUJTE PLUGINY, ROZŠÍŘENÍ A WEBOVÉ PROHLÍŽEČE

- Udělujte a odebírejte přístupová práva k internetovým aplikacím na základě podnikových/firemních požadavků.

- Zabezpečte podnikové prohlížeče, aby zaměstnanci mohli používat pouze důvěryhodné obchodní webové aplikace.
- Bezpečně spravujte firemní a nezávislé weby v samostatném webovém prohlížeči s odděleným od vnější sítě.

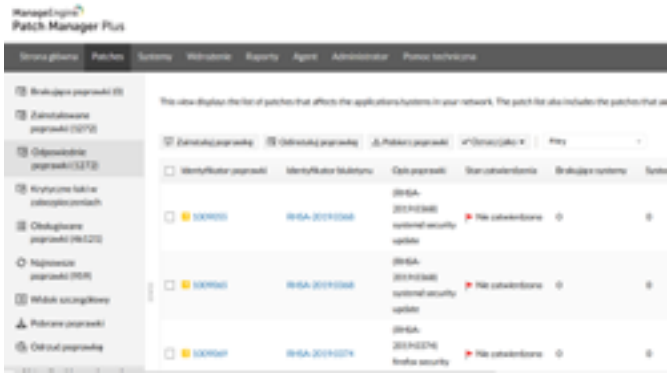
PROVÁDĚJTE KONTROLY A GENERUJTE SESTAVY

- Sledujte stav prohlížeče nainstalovaného ve vaší síti.
- Odhalujte a opravujte nové citlivé doplňky k prohlížeči,v reálném čase.
- Generujte sestavy za účelem odhalení počítačů, které neodpovídají standardním či firemním konfiguracím zabezpečení.

Správa aktualizací/patchů aplikací

Patch Manager Plus

Patch Manager Plus je nástroj nabízející automatickou instalaci oprav a aktualizací pro systémy Windows, MacOS, Linux a pro více než 300 aplikací třetích stran. To pomáhá správcům zajistit bezpečnost a snižuje náchylnost vůči hrozbám typu malware (malwarovým).



PPMP prohledává monitorované systémy a zjišťuje aktualizační nedostatky, testuje stažené opravy před jejich implementací, aby se minimalizovalo riziko selhání, a pak automaticky nainstaluje vybrané a otestované opravy.

Kromě toho získáváme přístup k auditům a zprávám, což umožňuje získat úplný obrázek o situaci v organizaci a snadnou kontrolu nad instalací oprav.

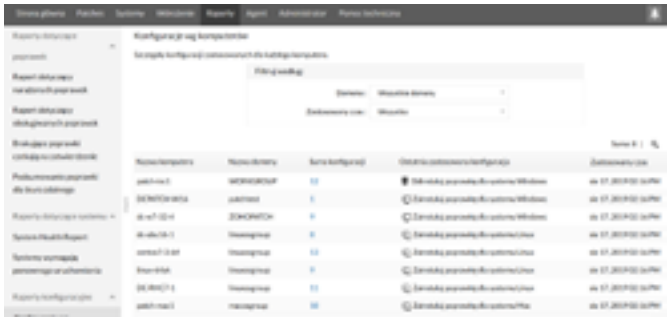
KLÍČOVÉ FUNKCE PMP:

AUTOMATICKÁ INSTALACE OPRAV

urychluje aktualizace a šetří čas díky automatizaci všech činností souvisejících s údržbou systémů v celé organizaci

PODPORA PRO MNOHO SYSTÉMŮ

PMP podporuje systémy Windows, MacOS, Linux a více než 300 aplikací třetích stran

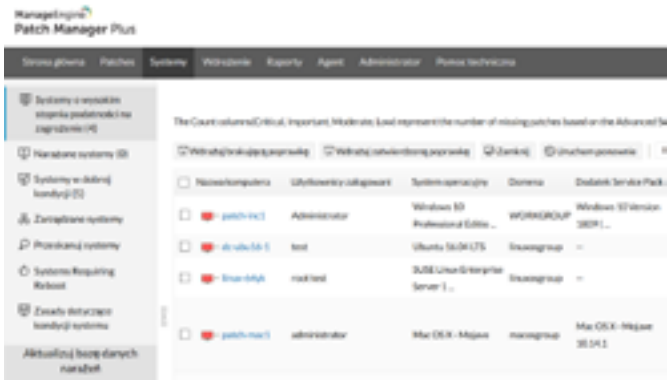


IMPLEMENTAČNÍ ZÁSADY

PMP umožňuje připravit si vlastní implementační zásady, takže můžete minimalizovat dopad změn na konečné uživatele, a tím i na fungování organizace.

PŘÍVĚTIVÉ ROZHRANÍ

Jednoduché a srozumitelné webové rozhraní, které Vás krok za krokem provede celým procesem implementace oprav



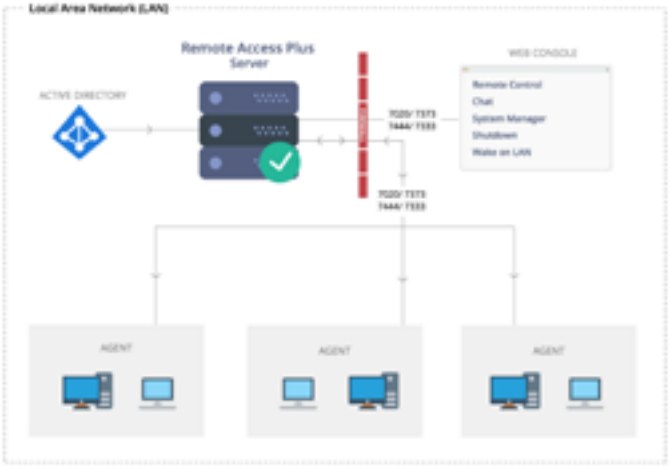
ŠKÁLOVATELNOST

Systém může podporovat až 50 000 počítačů

Nástroje podporující vzdálené ovládání pracovních stanic

Remote Access Plus

Remote Access Plus je nástroj, který umožňuje správcům a technikům HelpDesku řešit uživatelské problémy z jednoho centrálního místa. Umožňuje vzdálené připojení k pracovním stanicím, použitím Správce zařízení, Wake on LAN, dálkové vypnutí počítačů a kopírování souborů, což významně zkracuje čas potřebný k řešení problémů vznikajících na zařízeních zaměstnanců.



POKROČILÁ DÁLKOVÁ KONTROLA
Komplexní zabezpečení vzdáleného připojení pro diagnostiku problémů na počítačích se systémy Windows, Mac a Linux.

TEXTOVÝ CHAT A AUDIO A VIDEO
Vestavěný textový nebo audio / video chat usnadňuje kontakt s uživatelem a urychluje řešení problému.

DÁLKOVÉ ZASÍLÁNÍ SOUBORŮ
Vzdálené vytváření složek a kopírování souborů metodou drag & drop.

SPRÁVCE ZAŘÍZENÍ
Seznam počítačových programů umístěných na spravovaných počítačích

WAKE ON LAN
Přístup k aktuálnímu stavu napájení počítačů a možnost jejich vzdáleného zapnutí.

DÁLKOVÉ VYPNUTÍ
Možnost vzdáleného vypnutí počítačů za účelem úspory energie.

SPRÁVCE ÚLOH
Seznam všech procesů a služeb fungujících na počítačích s možností jejich spravování.

REGISTR
Možnost správy a úpravy registru.

PŘÍKAZOVÝ ŘÁDEK
Možnost přístupu k příkazovému řádku a ke spouštění systémových příkazů s příslušnými oprávněními.

KATALOG UDÁLOSTÍ
Sledování událostí na počítačích.

PODÁVÁNÍ ZPRÁV
Přístup k předdefinovaným zprávám.

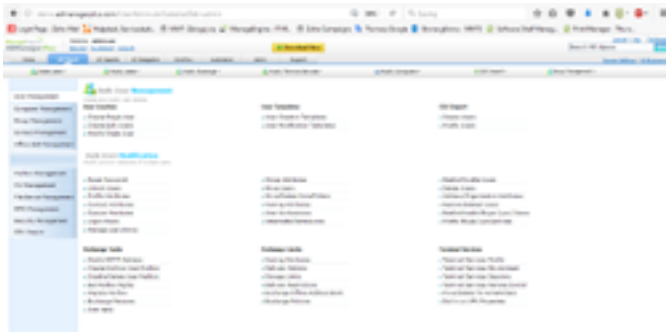
+ Správa AD

Správa a řízení Active Directory

ADManager Plus

Správa prostředí AD s rozšířenou strukturou může být pro tým IT výzvou. Takové úkoly jako: odblokování účtů, reset hesel k účtům AD, aktualizace údajů v AD, zabírají nejvíc času. Takový stav znemožňuje realizaci složitějších správcovských úkolů a brzdí rozvoj organizace.

AADManager Plus je produkt založený na internetovém prohlížeči, který podporuje správu katalogových služeb Active Directory. Software má jednoduché a velmi intuitivní uživatelské rozhraní, které usnadňuje správu katalogových služeb a nevyžaduje použití systémových příkazových řádků a skriptů. Integrovaný modul správy a generování výkazů značně šetří čas správce. Umožňuje efektivní tvorbu účtů pro mnoho uživatelů prostřednictvím hromadného importu atributů uživatelů ze souborů *.csv, správu kontaktů, skupin a hesel. Dále umožňuje zkrácení doby práce a zjednodušení prováděných činností. ADManager Plus umožňuje pružnou, hromadnou úpravu atributů uživatele pro katalogové služby, včetně zařazení terminálových operací/služeb. Generátor výkazů nabízených v ADManager Plus umožňuje rychlé a pružné generování a export všestranných výkazů ve Vámi požadovaném formátu. Centralizovaná kontrola a efektivní správa uživatelů prostřednictvím zavedení přístupu v závislosti na roli/funkci, kterou plní uživatel systému. Omezený přístup k chráněným informacím umožňuje zajištění integrity a kontroly celého systémového prostředí.



DÍKY IMPLEMENTACI ADMANAGER PLUS LZE V ORGANIZACI DOSÁHNOUT NÁSLEDUJÍCÍCH VÝSLEDKŮ:

- Hlavní správci již nemusí věnovat tolik času rutinním úkonům, protože je mohou delegovat na jiné podnikové správce
- +20 % času navíc na typicky správcovské povinnosti
- Možnost přenosu oprávnění na osoby, které nejsou spojeny s IT
- Připravené šablony názvosloví účtů v závislosti na lokalizaci
- Automatizovaný proces tvorby uživatelských účtů pomocí náležitě připravených šablon
- Možnost definování politiky hesel v šablonách zpřístupněných podnikovým správcům
- Rychlá realizace úkolů typu „vytvoření 100 účtů pro nový projekt“ pomocí souboru csv.
- Možnost hromadného ověření atributů s využitím souborů CSV nebo mechanismů filtrování

Audit změn v Active Directory

ADAudit Plus

Active Directory je centrálním bodem všech organizačních činností, což vyžaduje bezchybnou správu změn prostřednictvím jejich sledování a ověřování. Standardní nástroje v Active Directory bohužel nemají žádné auditní funkce. Skripty nebo nástroje příkazového řádku sice dokážou vytáhnout některé údaje, ale nesplňují mnoho požadavků auditu. Vzniká tak příležitost pro důvěryhodné nástroje auditu a tvorby výkazů, které tato omezení nemají.

ADAudit Plus je nástroj pro provádění auditu změn a reporting v distribuovaném prostředí Active Directory. Splňuje nejpřísnější požadavky na bezpečnost, audity, shody definované regulačními orgány. Poskytuje správcům příslušné nástroje, které podporují správu změn. ADAudit Plus poskytuje komplexní výkazy a oznámení, srozumitelné i pro netechnické pracovníky. Výkazy odpovídají na klíčové otázky, které se týkají auditu Active Directory: „Kdo" udělal „jakou" akci, „kdy" a z „jakého" místa. Kromě auditu samotného prostředí Active Directory lze také sledovat změny na file serverech, členských serverech a také na pracovních stanicích. Nástroj ukazuje nejen údaje související se změnou, ale umožňuje také export výsledků do xls, html, pdf a csv.

Není vhodné ignorovat informace o změně sítě, neboť i malá změna může nakonec způsobit zásadní problém. V prostředí Active Directory pak mohou být následky mimořádně nákladné. Při zohlednění výše uvedeného docházíme k závěru, že potřebujeme nástroj, který bude dohlížet na prostředí, identifikovat hrozby, upozorňovat správce na nechtěné změny a pomáhat při eliminaci hrozeb. Výstrahy doručované z ADAudit Plus jsou díky mechanismu okamžitých upozornění odpovědí na tyto potřeby.

Správa identit a hesel a uživatelská samoobsluha

ADSelfService Plus

ADSelfService Plus je bezpečnostní nástroj, určený koncovým uživatelům, díky kterému lze spravovat účet v doméně. Aplikace umožňuje reset hesla, odblokování účtu a aktualizaci údajů v prostředí Active Directory.

Díky tomu lze značně omezit incidenty generované v systému Helpdesk a omezit náklady. Výhodou aplikace je především snížení nákladů incidentů Helpdesk. Díky použití ADSelfService Plus za účelem automatizace změny hesla a odblokování účtu dochází k snížení počtu nových ticketů a s tím spojených nákladů. Při použití ADSelfService Plus se zvyšuje produktivita pracovníků díky zkrácení času, který by museli věnovat registraci incidentu a čekání na reakci operátorů Helpdesk. Použitím portálu SelfService se tento proces zkracuje na jeden rychlý krok. Díky tomu se mohou pracovníci ihned vrátit ke své práci a nemusí čekat na reakci odborníků z oddělení Helpdesku.

Každá provedená akce je uložena v logu. Kritické výstrahy a potvrzení se odesílají správcům a vybraným uživatelům podle harmonogramu. Instalace nástroje je neobyčejně snadná díky intuitivnímu průvodci instalací.

Portál lze personalizovat v souladu s grafickým schématem firmy a sloučit jej s firemním portálem Sharepoint. Skutečnost, že aplikace je webovým řešením, poskytuje uživatelům možnost správy jejich hesel kdykoliv a z libovolného místa. Portál ADSelfService Plus umožňuje aktualizaci takových údajů uživatele v Active Directory, jako: adresa, telefonní číslo, status, atd. To vše v reálném čase. Navíc díky nástroji ADSelfService Plus jsou tyto funkce dostupné i z prostředí mobilních zařízení!

Audit a reporting pro Exchange server

Exchange Reporter Plus

Exchange Reporter Plus je nástroj sloužící k analýze a tvorbě výkazů ze serverů Exchange, založený na internetovém prohlížeči. Řešení obsahuje přes 100 předdefinovaných výkazů, jež umožňují důkladnou a hloubkovou analýzu každé infrastruktury elektronické pošty Exchange.

Díky vestavěným statickým nástrojům, které analyzují poštovní provoz, objem uložené pošty, dynamiku nárůstu stávající obsluhované pošty, je software skvělým správcovským nástrojem. Software umožňuje sledování poštovních serverů a současně usnadňuje zajištění co nejlepší optimalizace a využití dostupných aktiv. Funkce auditu umožňují lepší kontrolu shody využití softwaru a aktiv.

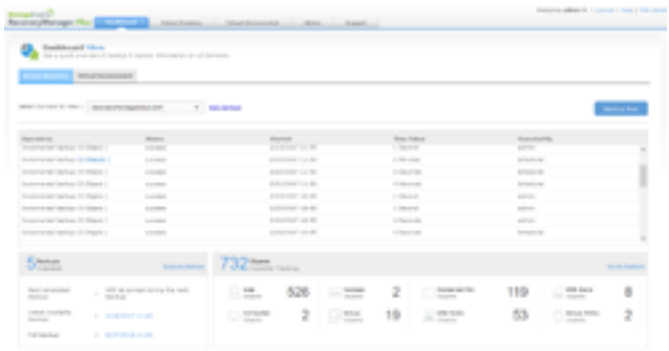
Při pohledu na řešení z jiné perspektivy je nutné se soustředit na nárůst výkonu, dosažený díky nové funkci monitorování provozu ActiveSync. Je vhodné zde zvážit čas nezbytný ke sledování aktivit v ActiveSync. Například, pokud je nutné věnovat dvě minuty analýze aktivity jednoho zařízení, správce Exchange musí analýze aktivit pro 100 zařízení věnovat přes tři hodiny. Exchange Reporter Plus umožňuje sledování těchto aktivit ActiveSync v reálném čase.

Detailní náhledy provozu, vytvořené v Exchange ActiveSync Reporter Plus, pomáhají správcům IT přesně uzpůsobit jejich zdroje serveru Exchange tak, aby vyhověli požadavkům uživatelů mobilních zařízení. Bez těchto detailních náhledů mohou správci IT nadměrně investovat do infrastruktury serveru Exchange v obavě, že může dojít k přetížení aktiva, způsobenému nadměrným využitím ze strany uživatelů.

Nástroj na zálohu a obnovení Active Directory

Recovery Manager Plus

Data Active Directory jsou kritická pro organizace všech velikostí, proto musí být možnost provádění rezervních kopií AD a jejich rychlé obnovy prioritním úkolem správců IT. Jejich realizace pak musí být co nejméně časově náročná, aby nedošlo k narušení chodu firmy. Za účelem eliminace prostojů a zajištění kontinuity provozu byl vytvořen program RecoveryManager Plus, který je vybaven nástroji pro snadnou tvorbu záložních kopií služby AD a funkcí mimořádné obnovy, jež tyto procesy zcela automatizuje.



HLAVNÍ FUNKCE PROGRAMU:

- Granulární obnova objektů prostřednictvím navrácení pouze určitých změn na úrovni atributů
- Plánování zálohování
- Možnost „jít zpět v čase“ a zrušit změny, které byly do objektu zavedeny pro konkrétní datum
- Získání kompletní kontroly nad změnami prováděnými v AD, přičemž je možné zrušit odstranění, přesunutí a veškeré jiné změny prováděné v objektu
- Produkt udržuje záložní kopie na úrovni verze pro každou změnu v AD, je tedy velmi snadné všechny změny zrušit.

Správa a reporting pro platformu Office365

O365 Manager Plus

Microsoft Office 365 je základem spolupráce a komunikace pro mnoho podniků. IT týmy tedy potřebují precizní a vyčerpávající údaje o všech jeho aspektech. Avšak předpřipravené výkazy Office 365 jsou jednoduché a málokdy poskytují skutečný náhled toho, jakým způsobem jsou využívány Exchange Online, Azure Active Directory a jiné složky Office 365.

365 Manager Plus je systém tvorby výkazů pro balíček Office 365. Konsoliduje data z Exchange Online, Skype for Business a jiných složek balíčku Office 365 do jednotlivých výkazů, poskytuje kompletní náhled do prostředí, mj.:

- Výkazy velikostí schránek
- Výkazy obsahu schránek
- Výkazy e-mailového provozu
- Výkazy OWA
- Licenční výkazy
- Výkazy o uživatelích a skupinách
- Výkazy Skype for Business
- Výkazy OneDrive for Business
- Výkazy Azure Active Directory
- Výkazy o mobilních zařízeních

Správa a reporting pro Sharepoint

SharePoint Manager Plus

Platforma SharePoint garantuje snadné ukládání a sdílení podnikových údajů. Díky pružnosti a snadnosti využití firmy implementují SharePoint, aby mohly rychle zpřístupňovat podnikové údaje. Avšak vysoká úroveň spolupráce a dynamický charakter obsahu je pro správce při správě a kontrole serverů SharePoint výzvou. Každý správce potřebuje komplexní nástroj, který mu pomůže monitorovat, analyzovat a kontrolovat platformu SharePoint.

SharePoint Manager Plus je nástroj, který obsahuje nejen to, ale ještě mnohem víc. Pomáhá při správě, auditu a tvorbě výkazů platformy SharePoint jak v prostředí On-premise, tak v Office 365.

SharePoint Manager Plus umožňuje účinnou správu Vašich serverů díky předdefinovaným výkazům, jež pomáhají sledovat změny oprávnění, identifikovat skupinové změny a vytvářet přesné seznamy uživatelů a jejich oprávnění. Řešení generuje také výkazy pro umožnění hloubkového náhledu do infrastruktury SharePoint prostřednictvím detailních informací o aktivech, jako jsou farmy, databáze obsahu, webových aplikací, stránek a jiných.

SharePoint Manager Plus zjednodušuje správu platformy díky přidávání, odstraňování nebo kopírování oprávnění pro vybrané webové stránky. Nabízí další možnosti, jako použití oprávnění pro substránky a kolekce webů, umožňuje ověření oprávnění uživatelů.

Integrovaná správa Active Directory a Exchange

AD360

AD360 je integrovaným řešením správy přístupů v prostředí Windows.

NEJDŮLEŽITĚJŠÍ FUNKCE Z POHLEDU ORGANIZACE

- Správa Active Directory a Office365 v organizaci,
- Audit změn ve Windows,
- Samoobslužný portál,
- Široká škála sestav.

Aplikace založená na webovém prohlížeči integruje funkce, které jsou nezbytné pro fungování společnosti, počínaje vytvářením uživatelů přes samoobslužný portálu po dohled nad uživateli a jejich auditování uživatelů, a to všechno prostřednictvím velmi snadného a intuitivního uživatelského rozhraní.

AD360 UMOŽŇUJE SPRAVOVAT ACTIVE DIRECTORY VELMI JEDNODUCHÝM A PŘÍVĚTIVÝM ZPŮSOBEM A TAKÉ UMOŽŇUJE:

- automatické vytváření a úpravu uživatelů, skupin a objektů AD,
- Zjednodušení sdílení uživatelských účtů,
- Delegování úkolů pomocí vestavěného modulu workflow,
- Bezpečné delegování stanovených úkolů v rámci AD na zaměstnance, kteří nejsou z IT,
- Automatizaci hromadného vytváření a úprav uživatelů, skupinové úpravy, mazání neaktivních uživatelů a mnoho dalšího.

AD360 AUTOMATIZUJE VEŠKERÉ RUTINNÍ AUTENTIZACE A ÚKOLY, TAKOVÉ JAKO:

- Vytváření, jak jednotlivě tak skupinově, nových uživatelů a objektů AD, bezpečná správa hesel, úprava atributů - jak jednotlivě a skupinově - pomocí rozhraní nebo souborů CSV. Správa uživatelských schránek a také pošty,
- Navíc, tímto automatizace nekončí. Po dokončení vybrané úlohy Vám AD360 umožní automatizovat pokračující úkoly. Velmi Velké množství úkolů spojených se správou AD se opakuje a mělo by být automatizováno. Navíc, velká část těchto úkolů může být částečně nebo zcela delegována na vybrané skupiny uživatelů,
- Pro efektivní vytváření nových uživatelů by se měla přenést část jednoduchých, ačkoliv časově náročných, úkolů na jiná oddělení. Díky AD360 můžeme přenést úkol spojený s přidáním nového uživatele do personálního oddělení, což správci ušetří čas pro náročnější pracovní úkoly.
- WORKFLOW AD360 má uživatelsky přívětivý a intuitivní modul nastavování workflow, který Vám umožňuje spravovat a udržovat kontrolu nad automatizací kritických úkolů. Navíc AD360 zaručuje:
- Komplexní zobrazení řídícího panelu pro prostředí AD. Možnost zobrazit nejdůležitější statistiky týkající se správy AD, auditu Windows, samoobslužného portálu a podávání zpráv v jednom přehledném okně,
- Synchronizace konfiguračních nastavení , včetně nastavení domény pro více jednotek a bez ztráty času.

AUDIT SOULADU

Zajištění vhodné úrovně zabezpečení se také stává snazší. Auditování kritických změn provedených na objektech AD umožňuje ověřit, zda jsou změny v souladu s bezpečnostními zásadami.

MONITOROVÁNÍ

Emailových zpráv Tento nástroj umožňuje sledovat provoz generovaný poštovními schránkami a jejich využívání a uživatelská práva. Modul reportingu umožňuje generovat výstrahy a zprávy ve formátech xls, csv, html a pdf.

SAMOOBSLUŽNÝ PORTÁL

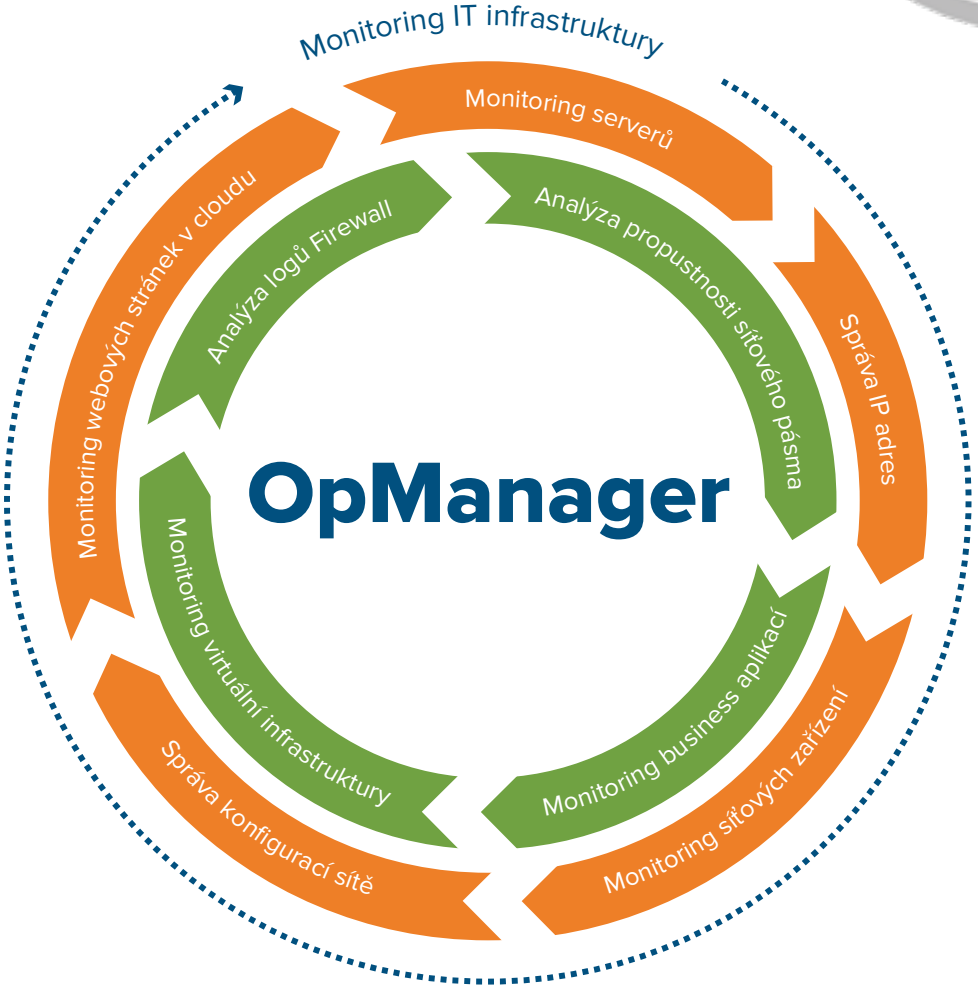
Tento nástroj poskytuje uživatelský portál, který umožňuje uživatelům bez pomoci IT oddělení dělat např. tyto úkoly: změnu hesla, odemknutí účtu a aktualizaci dat. Použití modulu CTRL + ALT + DEL umožňuje uživateli snadno přejít do režimu úpravy hesla, což ve výsledku opět snižuje počet požadavků na IT oddělení, čímž zvyšuje jeho produktivitu.

+ Monitoring IT

Kdy jste naposledy zkontrolovali, zda má vaše auto skutečně tolik koní výkonu, kolik výrobci uvádějí v reklamách? Podívali jste se někdy pod kapotu a hrabali se v motoru? Jednoduše sešlápneme plyn a díváme se na budíky. Stejným způsobem většina organizací přistupuje k výkonu sítě - je OK, dokud funguje.

A co v případě závodních stájí? Žijí z testování a zvyšování výkonu motoru, je to tak? Měří každý takt motoru a věnují mnoho času a energie zvyšování otáček. Několik organizací, které znáte, má přesně stejný přístup ke své síťové infrastruktuře, protože je silně spojena s jejich hlavní podnikatelskou činností. Bez výkonné sítě nemohou obvykle provozovat svou činnost a málokdy je tato činnost spojena s IT.

Sekce ITOM této publikace je pro ty organizace, jež potřebují výkonnou a spolehlivou síťovou infrastrukturu, která je stále a účinně kontrolována.



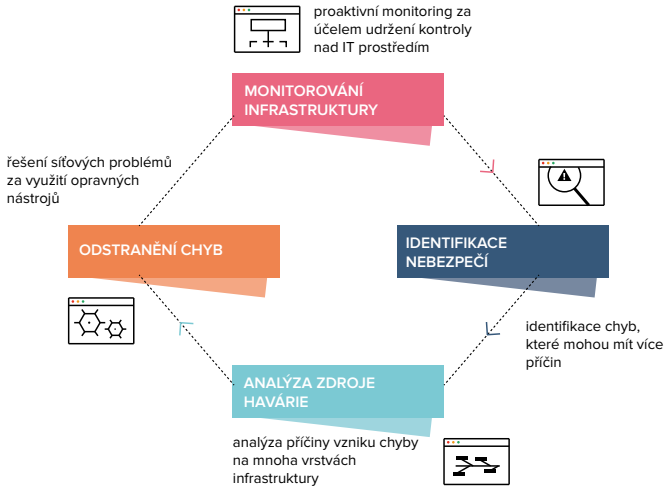
Komplexní správa a monitoring IT infrastruktury

OpManager

„Chtěli jsme řešení, které bude obsahovat všechny klíčové systémy obsluhy sítě a současně bude uživatelsky přívětivé."

Jarosław Leśniak
Oddělení správy sítě
Centrum informačních služeb ve Vratislavi

OpManager je kompletní systém pro správu síťové infrastruktury v organizaci.



Spojuje v sobě možnost monitorování síťových zařízení, serverů, aplikací, analýzy vytížení pásma a správu konfigurace sítě, IP adres a protokolu událostí. Vyspělý nástroj umožňuje správu celé sítě prostřednictvím jedné konzole. Díky monitorování celé IT oblasti v reálném čase je možné rychle reagovat na veškeré prostoje nebo chyby vyplývající z různých oblastí IT. Systém poskytuje vyspělé nástroje pro analýzu dat a tvorbu výkazů, díky kterým se mohou pracovníci IT racionálně a rychle rozhodovat v oblasti infrastruktury, za kterou jsou zodpovědní.

MONITORING DOSTUPNOSTI A VÝKONU
- Monitoring atributů síťových zařízení na základě SNMP, WMI, CLI
- Podpora pro Cisco IPSLA (monitoring VoIP a WAN RTT)

VYSPĚLÉ SYSTÉMY PRO GENEROVÁNÍ ALARMŮ A OZNÁMENÍ
- Oznámení emailem a SMS na základě překročení mezních hodnot
- Provádění automatických akcí v reakci na události

MONITORING VIRTUÁLNÍCH STROJŮ, KONTROLÉRŮ DOMÉNY, DATABÁZOVÝCH SYSTÉMŮ, ATD.
- Vyspělá, nastavitelná sada atributů monitoringu s možností úpravy mezních hodnot
- Jasný přehled hromadných náhledů a grafických prezentací

SPRÁVA KONFIGURACE SÍŤOVÝCH ZAŘÍZENÍ
- Roll-out konfigurace na vybraná zařízení
- Správa verzí, workflow (model potvrzování změn)

ANALÝZA VYTÍŽENÍ PÁSMA
- Náhled nejpopulárnějších aplikací v síti na základě technologie netflow
- Ověření politik QoS díky průzkumu markerů DSCP

SPRÁVA IP ADRES A MAPOVÁNÍ PORTŮ PŘEPÍNAČŮ
- Analýza vytížení rozsahu IP adres v segmentech sítě
- Ověření portů síťových přepínačů z hlediska připojených zařízení

MONITORING VÝKONU APLIKACE
- Monitoring aplikačních, databázových a webových serverů
- Tvorba skupin komponentů mapujících strukturu IT služeb

Monitoring a analýza IT komponentů v heterogenním prostředí

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:
- Funkce RunBook Automation – automatizace procesů workflow
- Správa konfigurace síťových zařízení
- Analýza vytížení pásma
- Správa IP adres
- Automatická, pravidelná detekce sítě
- Automatická tvorba mapy sítě

- Přes 700 šablon zařízení
- Podpora 64bitových systémů
- Monitoring AD, MSSQL, MS Exchange
- Monitoring virtuálního prostředí (VMware, HyperV, Citrix)
- Vestavěné adresáře MIB pro nejpopulárnější zařízení SNMP
- Monitorování deníku systémových událostí
- Monitoring pomocí skriptů
- Monitorování procesů, disků, procesorů, pamětí
- Přes 100 přednastavených výkazů s možností nastavení harmonogramu a editace
- Monitorování služeb Windows
- Prohlížeč adresářů MIB
- Vyspělé systémy notifikace a automatizace operací
- Monitorování dostupnosti
- Monitoring URL
- Rozvinuté systémy obsluhy událostí s možností eskalace
- Nasazený REST API
- Monitoring VoIP a WAN s využitím Cisco IPSLA

ESSENTIAL EDITION

- Obsluha až 1000 zařízení
- Monitoring síťových zařízení a serverů
- Upravitelné hromadné náhledy a CCTV
- Obsluha eventlog, syslog a protokolů SNMP
- Diagramy provozu v reálném čase
- Funkce automatizace workflow
- Obsluha IPSLA
- Hromadný náhled pro SLA
- Monitoring virtuálního prostředí
- Analýza provozu v síti

ENTERPRISE EDITION

- Obsluha až 50.000 zařízení
- Pro organizace, které mají rozsáhlé prostředí a rozptýlenou strukturu
- Obsahuje všechny funkce verze Essential
- Rozšiřitelný: podpora pro monitoring až 5000 zařízení
- Architektura založená na proxy serverech
- Centrální konzole agregující údaje ze všech proxy serverů
- Podpora pro geograficky rozptýlené a rozsáhlé sítě
- Funkce Fail-Over (vysoká dostupnost) pro architekturu založenou na MSSQL

Základní náhled monitorovaného zařízení obsahuje několik prvků: výrobní štítek, na kterém se nacházejí informace o kategorii, výrobci, IP adrese, závislostech, přehled grafů, seznam monitorů, profilů oznámení a alarmů. Na této úrovni lze také provádět správu.

Ucelený náhled v systému OpManager umožňuje rychlé hodnocení stavu monitorované IT infrastruktury. Prezentované statistiky se týkají výkonu, dostupnosti zařízení a vygenerovaných výstrah podle kategorie. Přehled grafických prezentací znázorňuje využití zásob a jejich rozmístění v podniku.

Monitoring webových stránek a aplikací z globální perspektivy (Cloud)

Site24x7

Site24x7 je služba v cloudu (SaaS), která nabízí monitoring kritických webových aplikací, viditelných mimo organizaci, a vnitřních IT aktiv, jako servery nebo síťová zařízení (s využitím kolektoru v síti LAN). Umožňuje tvorbu analýz dostupnosti a výkonu kritických prvků webových aplikací z mnoha míst na světě, bez nutnosti otevírání portů, instalace agentů nebo rekonfigurace sítě.
Pokud má být stránka viditelná mimo organizaci, pak ji nelze monitorovat standardním monitorovacím systémem, který funguje zevnitř sítě.

Site24x7 je ideální řešení pro monitorování dostupnosti a výkonu kritických podnikových aplikací, se zohledněním víceúrovňových webových transakcí. V případě vzniku problémů jsou odeslána automatická oznámení osobám, které jsou odpovědné za obsluhu aplikací. Díky tomu mohou tyto osoby velmi rychle reagovat. Monitoring webových aplikací poskytuje informace o jejich dostupnosti a výkonu.

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:

- Monitoring dostupnosti a výkonu stránek
- Monitoring serverů a síťových zařízení
- Monitoring webových transakcí
- Monitoring webových aplikací
- Okamžité oznámení
- Monitoring serverů DNS
- Monitoring poštovních serverů
- Správa SLA
- Globální síť monitorovacích agentů

V případě vzniku problémů s webovými aplikacemi jsou odeslána automatická oznámení osobám, které jsou odpovědné za obsluhu aplikací. Díky tomu mohou tyto osoby velmi rychle reagovat. Monitoring webových aplikací poskytuje informace o jejich dostupnosti a výkonu.

V souladu se zprávou Gartnerů – přes 50 % návštěvníků WWW stránek rezignuje a odejde, pokud musí čekat na otevření stránky déle než 15 sekund. Díky Site24x7 získáte okamžitou informaci o sníženém výkonu stránky a můžete rychle zabránit ztrátě potencionálních zákazníků.

Integrovaný monitoring IT infrastruktury z pohledu poskytovaných služeb.
Analýza IT komponent orientovaná na poskytované služby.

Applications Manager

„Realizace idejí proaktivního přístupu ke správě informační infrastruktury má, v případě systému Applications Manager, relevantní výsledky v podobě eliminace značného množství hlášení uživatelů ohledně námi poskytovaných služeb IT."

Dominik Adamik
Obchodní ředitel
Avatia Sp. z o.o.

IT infrastruktura podniků se rozvíjí společně s rozvojem obchodu.

Proto je zajištění vysoké dostupnosti a výkonnosti kritických podnikových aplikací stále obtížnějším úkolem. Záležitosti výkonu aplikací již navíc nejsou spojeny pouze s technologií. Mají reálný vliv na obchod. Applications Manager pomáhá při monitorování výkonu a dostupnosti webových aplikací, serverů aplikací, databází, dedikovaných aplikací, systémů a služeb v komplexním podnikovém prostředí. Systém uceleně prezentuje IT infrastrukturu, umožňuje detekci problémů předtím, než ovlivní práci uživatelů, identifikuje zdroje událostí a umožňuje analýzu trendů vytížení infrastruktury pomocí hromadných výkazů.

ORIENTACE NA SERVISNÍ PŘÍSTUP K IT INFRASTRUKTUŘE
- Možnost třídění IT komponentů do skupin prezentujících služby
- Automatická tvorba relací mezi komponenty, odpovídajících stavům služeb

ŘEŠENÍ PROBLÉMŮ SOUVISEJÍCÍCH S PRACÍ PODNIKOVÝCH APLIKACÍ
- Analytické nástroje RootCause
- Systém generování alarmů, který podporuje proaktivní monitoring

GENEROVÁNÍ HROMADNÝCH VÝKAZŮ
- Výkazy pro personal management
- Přehledy z hlediska dostupnosti a výkonu jednotlivých služeb

SPRÁVA SLA
- Podpora pro základní ukazatele SLA
- Monitoring služeb z hlediska plnění podmínek SLA

SPRÁVA SLA
- Analýza funkce IT komponent na základě historických údajů
- Vyspělé metody porovnávání stavů

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:
- Monitoring virtuálního prostředí
- Monitoring operačních systémů
- Monitoring služeb a procesů
- Monitoring serverů aplikací
- Monitoring portálů Middleware
- Testování zkušeností koncových uživatelů
- Rozšířený systém generování výkazů
- Monitoring systémů ERP
- Monitoring transakcí J2EE, .NET, Ruby-on-Rails
- Vyspělý systém alarmů a reakcí na události
- Monitoring databází
- Monitoring poštovních systémů
- Podpora proaktivního monitoringu
- Monitoring serverů a webových služeb
- Monitoring dedikovaných aplikací
- Správa SLA
- Monitoring webových aplikací
- Možnost definování vlastních, atypických monitorů
- Zjišťování anomálií
- Modul automatické detekce aplikací a závislostí (ADDM)

PROFESSIONAL EDITION

- Vhodná pro infrastrukturu do 250 monitorů
- Monitorování databází
- Monitorování serverů aplikací
- Správa smluv SLA
- Správa uživatelů (diferenciace oprávnění a rozsahu)
- Harmonogram výkazů

ENTERPRISE EDITION

- Bez omezení množství monitorů
- Obsahuje všechny funkce verze Professional
- Monitoring WAN
- Podpora klastrové architektury (Fail-over)
- Velká rozšiřitelnost (architektura Admin Server - Managed Server)
- Vysoká úroveň bezpečnosti (komunikace HTTPS)
- Konsolidované údaje z mnoha sítí s omezeným přístupem

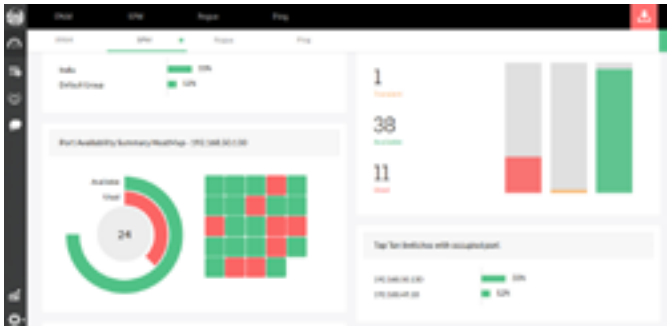
Ucelený náhled v Applications Manageru zobrazuje celkové informace o stavu celé monitorované IT infrastruktury. Prezentované statistiky se týkají alarmů, stavu jednotlivých kategorií monitorů, dostupnosti a využití atributů.

Podnikový náhled skupiny monitorů, která reprezentuje IT službu poskytovanou pobočkou, prezentuje relace mezi jednotlivými zúčastněnými komponenty, jež mají vliv na činnosti IT. Díky grafickému označení a použití barev lze stav služby zhodnotit jedním pohledem.

Správa IP adres a nástroj na mapování portů v přepínači v jednotném pohledu

OpUtils

OpUtils je nástroj pro správu IP adres v korporátní síti.



Systém ukazuje využití IP adres v jednotlivých subsítích a segmentech infrastruktury, informuje správce sítě o dostupnosti adresy, její obsazenosti, dočasnosti, atd. Skládá se z více než 30 nástrojů, jako: diagnostika sítě, monitoring adres, monitoring sítě, funkce SNMP. Umožňuje také tvorbu vlastních funkcí SNMP pro monitorování zařízení na základě knihovny MIB. Systém umožňuje řešení problémů spojených se správou portů přepínačů a adresováním v sítích. Díky výkazům inventarizace, zařízení SNMP, zlodějských systémů, dostupných IP adres, adres MAC systém poskytuje správcům sítě aktuální obraz sítě bez nutnosti neustálé a manuální aktualizace statických informací.

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:

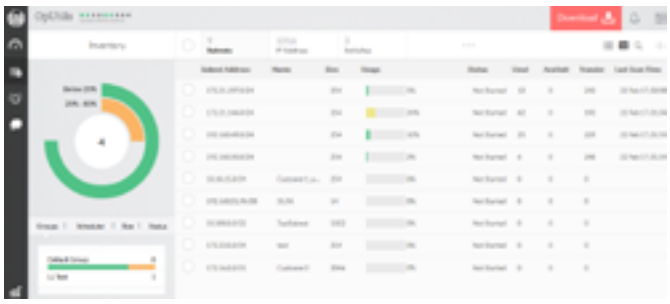
- Správa IP adres a nasycení adres v síťových segmentech
- Správa portů síťových přepínačů
- Detekce podezřelých událostí
- Zálohování konfiguračních souborů zařízení Cisco
- Monitorování propustnosti pásma
- Sada síťových správcovských nástrojů

STANDARD EDITION

- Správa adres MAC
- SNMP Ping
- Skenování sítě
- Správa DNS
- Monitor pásma
- Monitor sítě
- Wake-On-Lan

PROFESSIONAL EDITION

- Všechny funkce Standard Edition
- Správa IP adres (IPAM)
- Mapování portů přepínačů (SPM)
- Správa konfiguračních souborů



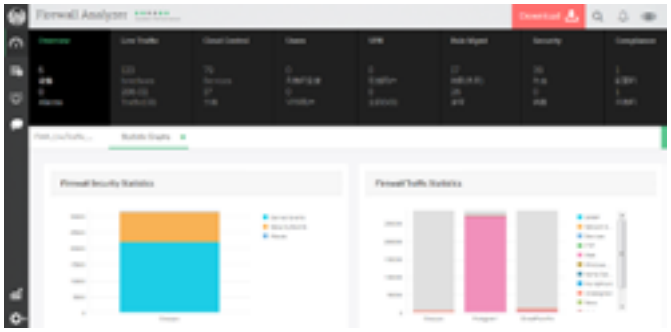
Rozšířený náhled portů přepínače, prezentující informace o obsazenosti portu, IP adrese, připojených adresách MAC, názvu VLAN. Z této úrovně lze definovat také lokalizace zařízení a odečítat rychlost portu.

Náhled segmentu sítě s určitým balíčkem IP adres na zadané síťové masce. Obšírné informace o stavu DNS, řešení IP adres nebo doménových názvů, typu zařízení, s pohodlným přechodem do režimu dalších speciálních síťových nástrojů.

Správa konfigurace FW & Správa logů

Firewall Analyzer

Samotná instalace firewall síť neochrání. Nutné je neustálé monitorování a analyzování údajů z deníku FW. Tyto soubory obsahují mnoho důležitých informací. Na základě záznamů v denících lze detekovat ohrožení bezpečnosti, jako průnik do sítě, virové útoky, útoky typu „odmítnutí služby“ (DoS), abnormální chování, chování uživatelů v Internetu, provádět analýzu internetového provozu, atd.



Firewall Analyzer je software pro analýzu logů bez agentů a správu konfigurace, určený pro bezpečnostní zařízení. Program je určen k monitorování a analýze zabezpečení, správě změn, monitorování aktivit zaměstnanců v Internetu, monitorování propustnosti, plánování výkonu, vymáhání dodržování pravidel a tvorbě výkazů z inspekcí bezpečnosti a shody - činností prováděných v koncovém bodě. Firewall Analyzer není závislý na dodavateli a obsluhuje téměř všechny typy firewall open source i komerční (Check Point, Cisco, Juniper, Fortinet, Snort, Squid Project, SonicWALL, Palo Alto itd.), IDS/IPS, sítě VPN, proxy servery a podobná bezpečnostní zařízení. Určen je pro správce ochrany sítě a dodavatele spravovaných služeb ochrany (MSSP), kteří potřebují centralizované shromažďování, archivování a analyzování deníků ochranných zařízení a generování výkazů.

PREMIUM EDITION

- Obsluha až 60 zařízení
- Podpora pro mnoho výrobců
- Monitoring virtuálních FW, proxy a VPN
- Výkazy bezpečnosti
- Výkaz internetové aktivity pracovníků
- Výkaz využití webových aplikací
- Audit bezpečnosti firewall
- Správa změn konfigurace
- Správa pravidel FW
- Diagnostika spojení
- Ověřování AD a RADIUS

DISTRIBUTED EDITION

- Obsluha až 1200 zařízení
- Všechny funkce Premium Edition
- Rozšiřitelná architektura
- Obsluha mnoha lokalizací
- Architektura server - kolektor

Monitoring propustnosti sítě & Analýza síťového provozu

NetFlow Analyzer

„Aplikace NetFlow Analyzer umožnila průběžné monitorování provozu v síti, sledování anomálií a detekování atypických balíčků. Přehledně prezentuje údaje a statistiky využití spojení. Program je velmi praktický a pomáhá při správě sítě.“

Grzegorz Staśkiewicz
Ředitel technické sekce IT
Ceramika Paradyż Sp. z o.o.

NetFlow Analyzer je nástroj pro analýzu provozu v síti bez agentů, využívající celou řadu technologií, které jsou součástí routerů, přepínačů, bariér a akcelerátorů WAN. Software podporuje Cisco netflow, Cisco NBAR, IPSLA a CBQoS. NetFlow Analyzer obsahuje velké množství funkcí, které umožňují hloubkový náhled do provozu sítě a hodnocení jeho vlivu na podnikovou činnost.

NetFlow Analyzer navíc podporuje sFlow®, cflowd®, jFlow®, IPFIX®, NetStream®, AppFlow®

RYCHLEJŠÍ ODSTRANĚNÍ INCIDENTŮ V SÍTI
- Náhled do nejpoužívanějších aplikací v síti
- Vzorce provozu pro rozhraní a oddělení

ZAJIŠTĚNÍ VÝKONU APLIKACÍ
- Zajištění optimální propustnosti pro kritické podnikové aplikace
- Ujištění, že aplikace pracují se správnou prioritou

MONITOROVÁNÍ VÝKONU VOIP
- Monitorování klíčových ukazatelů výkonu spojení VoIP
- Vykazování parametrů zpoždění, Jitter, MOS

OCHRANA SÍTĚ PROTI HROZBÁM
- Pomoc při detekci červů a virů s detailní informací o počítačích a portech
- Vyspělý modul analýzy hrozeb

OVĚŘENÍ NASTAVENÍ QOS
- Tvorba výkazů na základě tříd
- Ověření toku dat v rámci markerů DSCP

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:
- Tvorba skupin a oddělení na základě IP
- Možnost definování aplikací na základě portu a IP adresy
- Obsluha autonomních systémů (AS)
- Analýza provozu pro Medianet/Mediatrace
- Automatické upozornění po překročení mezních hodnot
- Harmonogramy pravidelných výkazů
- Podpora technologií Cisco Flexible Netflow NBAR pro inteligentní kategorizaci aplikací (vrstva 7 OSI) na základě hloubkové analýzy balíčků
- Podpora pro SNMPv3 a Cisco ASA
- Technologie Continuous Stream Mining Engine™ v modulu ASAM
- Tvorba výkazů Cisco CBQoS
- Podpora pro technologie Cisco WAAS, Medianet a IPSLA
- Analýza a tvorba výkazů propustnosti sítě
- Monitorování provozu mezi oddělenými lokacemi
- Výkazy plánování kapacity s analýzou nárůstu provozu aplikace
- Vyspělé úložiště dat: všechny záznamy ze zařízení jsou uchovávány v aplikaci až jeden měsíc. Agregovaná data jsou uchovávána pro potřeby historických výkazů

Grafické diagramy NetFlow Analyzer znázorňují detaily spotřeby síťového pásma pro různá časová období, v závislosti na rychlosti přenosu, objemu dat, procentuálním využití spojení a množství packetů.

Díky použití technologie Continuous Stream Mining Engine™ je modul ASAM v NetFlow Analyzer prakticky jediným účinným nástrojem pro detekci a klasifikaci útoků zero-day v reálném čase. ASAM nabízí inteligentní systém detekce širokého spektra vnitřních i vnějších hrozeb a kontinuální hodnocení bezpečnosti v síti.

ESSENTIAL EDITION

- Jednoduchá instalace s integrovaným kolektorem dat a systémem pro generování výkazů
- Vhodná pro monitorování až 5000 rozhraní (až 100.000 flows/sec)
- Výkazy provozu sítě v reálném čase
- Geolokalizace IP adres
- Vyspělý modul analýzy hrozeb

DISTRIBUTED EDITION

- Rozptýlený sběr dat NetFlow a centralizovaná tvorba výkazů
- Monitorování neomezeného množství rozhraní
- Obsahuje všechny funkce verze Professional
- Bezpečná komunikace HTTPS mezi centrálním serverem a datovými kolektory
- Analýza NBAR, CBQoS, ASAM a mnoho jiných.

Správa konfigurace sítě

Network Configuration Manager

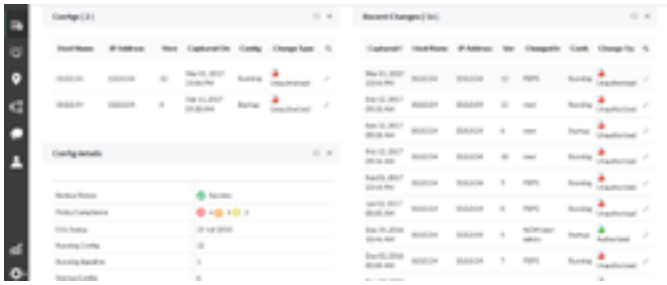
Network Configuration Manager je systém podporující správu konfigurací síťových zařízení typu switche a routery. Při využití tohoto systému v IT prostředí lze definovat harmonogram zálohování konfiguračních souborů, porovnávat dvě konfigurace, tvořit základní a aktuální konfigurace a distribuovat vybrané řádky konfigurace na mnoho zařízení současně.

Bohatá funkčnost nástroje, která obsluhuje automatickou detekci zařízení, šifrované součásti konfigurace, verzování, definování harmonogramů zálohování konfigurací a jiných úkolů a modelování přístupu do systému na základě rolí uživatelů, umožňuje bezpečnou, ergonomickou a účinnou centralizaci správy konfigurace síťových zařízení.

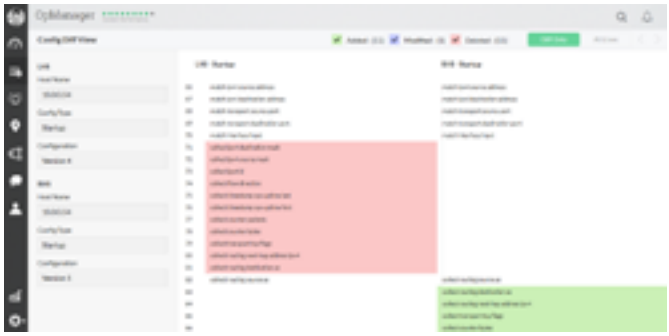
Mechanismus potvrzování konfigurací před implementací na výrobní verzi garantuje stabilitu práce síťových zařízení a kontrolu změny, verzování konfigurací umožňuje rychlou obnovu správného nastavení. Systém obsahuje také mnoho výkazů, které ověřují aktuální konfiguraci z hlediska shody, dobré praxe nebo standardů. Takové výkazy garantují udržení kvality a bezpečnosti konfigurace na vysoké úrovni.

NEJDŮLEŽITĚJŠÍ VLASTNOSTI:

- Podpora pro síťová zařízení nezávisle na výrobci
- Šifrované úložiště konfigurací
- Verzování a porovnávání konfigurací
- Režim základní konfigurace a práce na základě štítků
- Harmonogramy záloh konfigurací a jiných úkolů
- Přístup na základě role
- Mechanismus potvrzování a detekce konfigurací
- Sledování změn konfigurace v reálném čase
- Monitoring shody konfigurace s politikou a standardy
- Automatizace konfiguračních úkolů



Náhled inventarizovaného síťového zařízení umožňuje pohodlnou správu jeho konfigurace. Z tohoto místa je umožněn rychlý přístup do základní a aktuální konfigurace, vyhledávání změn, hardwarových parametrů nebo pravidel správy změn.



Náhled srovnání dvou konfigurací je ideální místo pro ověření změn. Jednotlivé řádky jsou označeny barvami jako změněné, přidané nebo odstraněné. Volitelný režim SyncScroll navíc umožňuje navigaci po obou konfiguracích současně.

+ Bezpečnost IT

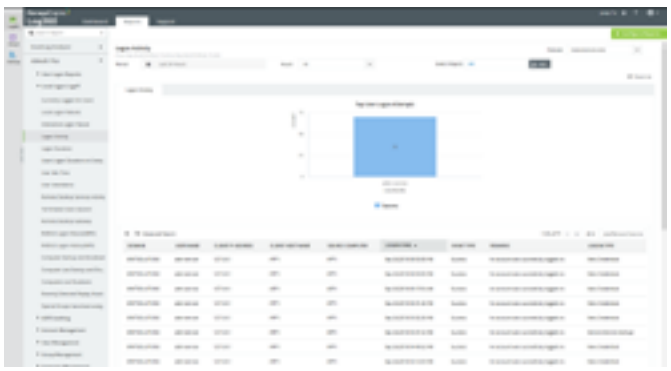
Integrované spravování logů a audit Active Directory

LOG 360

Log360 řeší problémy se správou logů a zabezpečením sítě. Jedná se o integrované řešení, které kombinuje možnosti nástrojů EventLog Analyzer, ADAudit Plus a Cloud Security Plus do jedné konzoly pro usnadnění správy zabezpečení sítě, auditu služby Active Directory a veřejné správy cloudu.

LOG360 ZAJIŠŤUJE BEZPEČNOST SÍTĚ POMOCÍ:

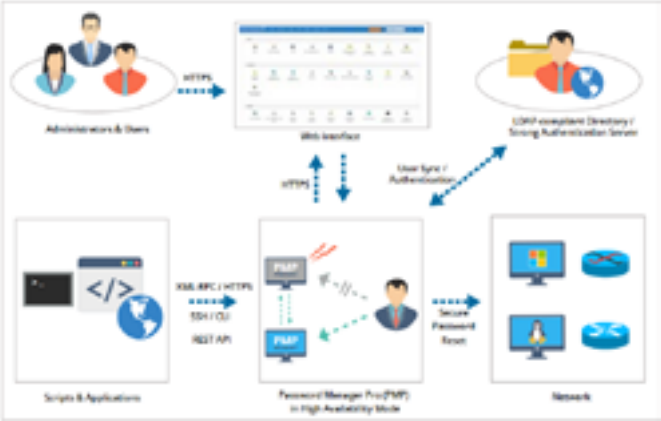
- Shromažďování, monitorování, analýzy a archivace logů ze zařízení syslog/eventlog, síťových zařízení, jako jsou brány firewall, routery a přepínače , servery Linux / UNIX, servery Windows, jakékoli aplikace a další,
- Sledování aktivit privilegovaných uživatelů,
- Sledování a kontrola změn ve službě Active Directory v reálném čase,
- Okamžitá identifikace úprav GPO,
- Sledování změn v OU,
- Seznámení se s vnitřními bezpečnostními hrozbami,
- Zajištění podrobných informací o důvěrném přístupu k souborům a složkám,
- Pomoc při plnění přísných regulačních požadavků, jako jsou PCI DSS, FISMA, HIPAA, SOX, GLBA, GPG 13 a další,
- Boj proti vnějším útokům,
- Sledování databázového serveru a komplexní audit ve všech činnostech souvisejících s databází,
- Kontrola souborových serverů Windows, EMC a NetApp,
- Získání podrobných informací o událostech, ke kterým dochází ve službách Simple Storage Service (S3), Amazon EC2, Virtual Private Cloud (VPC), Route 53, Firewall Web Application (WAF), Security Token Service (STS) a dalších,
- Zajištění podrobných informací o aktivitě uživatele a všech změnách provedených ve skupinách zabezpečení sítě, virtuálních sítích, branách aplikací, zónách DNS, virtuálních počítačích, databázích a dalších.



Centrální úložiště hesel a správa privilegovaných účtů

Password Manager Pro

Password Manager Pro je webová aplikace, určená ke správě hesel v podnicích za účelem kontroly přístupu ke sdíleným správcovským heslům, která chrání veškerá aktiva podniků, jako servery, databáze, síťová zařízení, aplikace, atd., a kontrole hesel k účtům typu Application-to-Application – takzvaným “servisním účtům”, jež jsou aplikacemi využívány interně, bez účasti člověka.



Aplikace umožňuje také synchronizaci hesel. Stávající hesla do vzdálených aktiv mohou být upravována z úrovně systému, změněná hesla jsou uložena do úložiště. Rozšířený mechanismus kontroly v aplikaci Password Manager Pro umožňuje sledování takových informací, jako kdo, kdy a jaké změny provedl. Díky tomuto prostředí, ve kterém pracuje mnoho uživatelů, lze snadno získat informace o tom, kdo je za co odpovědný.

NEJDŮLEŽITĚJŠÍ VLASTNOSTI

- Centralizované úložiště hesel
- Integrace s Active Directory a LDAP
- Proces kontroly přístupu k heslům
- Kontrola přístupu na základě role uživatele
- Sdílená správa správcovských hesel
- Implementace politiky v oblasti hesel
- Automatizovaný reset hesel
- Správa hesel z aplikace do aplikace
- Možnost spuštění nestandardního skriptu po resetu hesla
- Správa servisních účtů Windows
- Automatické přihlašování do cílových systémů, internetových stránek
- Komplexní audity a generování výkazů
- Oznámení o událostech spojených s hesly v reálném čase
- Dvoustupňové ověření
- Vysoká dostupnost
- Tvorba záložní kopie dat a obnova dat z kopie
- Přístup přes mobilní telefon

Správa SSH klíčů a SSL certifikátů

Key Manager Plus

Key Manager Plus je řešení pro správu klíčů SSH a certifikátů SSL, založené na internetovém prohlížeči, které pomáhá konsolidovat, kontrolovat, spravovat, monitorovat a zkoumat celý životní cyklus klíčů SSH (Secure Shell) a certifikátů SSL (Secure Sockets Layer). Zajišťuje náhled do prostředí SSH a SSL a pomáhá správcům přejmout úplnou kontrolu nad klíči za účelem zmaření narušení a zajištění shody.

Jaké problémy řeší?

Běžné klíče SSH nejsou kontrolovány a monitorovány, proto bývají organizace vystaveny kybernetickému útoku. V případě absence automatického systému je získání seznamu všech používaných klíčů, nalezení a omezení přístupových práv a zajištění pravidelných rotací velkou výzvou.

Správa prostředí Secure Socket Layer (SSL) může být stejně těžká, pokud organizace používají velké množství certifikátů SSL, vydaných různými dodavateli, s různým obdobím platnosti. Z druhé strany, nemonitorovanému certifikátu SSL může skončit platnost nebo může být použit falešný/chybný. Oba scénáře mohou způsobit odstávku poskytování služby nebo zobrazovat zprávy o chybách, které způsobují ztrátu důvěry v oblasti bezpečnosti dat mezi klienty. V krajních případech mohou vést k narušení bezpečnosti.

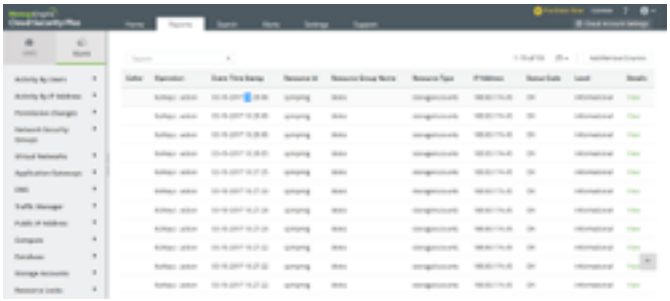
Key Manager Plus byl navržen tak, aby vyřešil všechny tyto problémy. Současně nabízí řešení pro správu všech digitálních totožností.

Zabezpečení cloudu a správa logů

Cloud Security Plus

Cloud otevírá nové možnosti využití podnikových funkcí. Snadná implementace, rozšiřitelnost a ekonomické aspekty cloudových platforem, to jsou argumenty, které přesvědčily mnoho firem k volbě této technologie. Avšak požadavky na dodržování bezpečnostních pokynů a rostoucí obavy ze ztráty dat a neautorizovaného přístupu komplikují využití plného potenciálu platforem.

Cloud Security Plus eliminuje obavy o bezpečnost a chrání cloud. Poskytuje plný náhled do cloudové struktury AWS (Amazon Web Service) a Azure. Komplexní výkazy, jednoduchý mechanismus vyhledávání a nastavitelné profily alarmů - díky tomu lze sledovat, analyzovat a reagovat na události, ke kterým dochází v cloudovém prostředí. Účinný provoz firmy v bezpečném a chráněném cloudu je proto velmi snadný.



Systém shromažďuje a analyzuje údaje z logů a poskytuje informace o všech aktivitách a změnách v prostředí AWS a Microsoft Azure.

Spravování citlivých údajů

Data Security Plus

Data Security Plus je nástroj, který současně plní tři funkce:

- detekuje, analyzuje a hlásí citlivá datauložená na souborových serverech,
- monitoruje a poskytuje informace o tom, kdo kdy udělal jakou aktivitu v souvislosti s konkrétním souborem,
- analyzuje prostředí FS a hlásí staré, neplatné, nemodifikované soubory, pomáhá udržovat pořádek v datech a optimalizovat prostor na serveru.

DSP má schopnost detekovat hrozby typu Ransomware a upozorňovat na ně v reálném čase. To urychluje dobu odezvy na incident díky zabudovaným zprávám, které nám pomáhají splnit požadavky norem jako např. GDPR či ISO. Díky oznámením v reálném čase o změnách provedených v souborech, máme možnost získat následující informace: kdo provedl změnu, jaká to byla změna a v jakém souboru, což nám umožňuje okamžitě jednat a případně obnovit původní verzi souboru.

FUNKCE

- Detekuje a hlásí citlivá data v souborech,
- Definuje svá vlastní pravidla pro detekci dat,
- Sleduje změny v souborech a složkách,
- Hlásí oprávnění k souborům a prostředkům,
- Odhaluje hrozby typu ransomware,
- Upozorňuje v reálném čase,
- Detekuje nepoužívané soubory,
- Sleduje využité místo na disku.

Správa periferních zařízení a zabránění únikům dat

Device Control Plus

Device Control Plus je nástroj DLP (Data Loss Prevention), který chrání organizaci před únikem dat. Umožňuje kontrolovat, blokovat a sledovat přenosná zařízení USB a další periferní zařízení, což umožňuje ochranu před neoprávněným přístupem k citlivým údajům organizace.

CHRAŇTE SVÁ DATA PŘED ÚTOČNÍKY

DCP umožňuje konfigurovat přístupová oprávnění, nastavit režim jen pro čtení, blokovat možnost kopírování dat z a do mobilních zařízení díky jednoduchým zásadám připraveným k použití.

PLNÁ KONTROLA ŘÍZENÍ

Zabezpečení dat a povolení omezeného přenosu dat nastavením omezení na základě velikosti a typu souboru.

ELIMINUJTE ZTRÁTU DAT

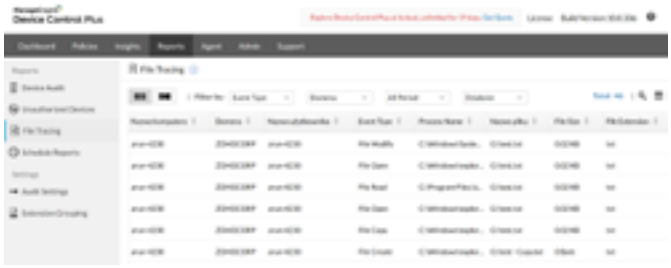
Kontrola zařízení na principu Zero Trust. Identifikování a blokování neautorizovaných zařízení vytvořením seznamu důvěryhodných zařízení.

POSKYTNĚTE PŘÍSTUP VE VHODNÉM ČASE

Možnost poskytnutí dočasného přístupu na stanovené časové období, aby se minimalizovalo riziko snížení produktivity zaměstnanců.

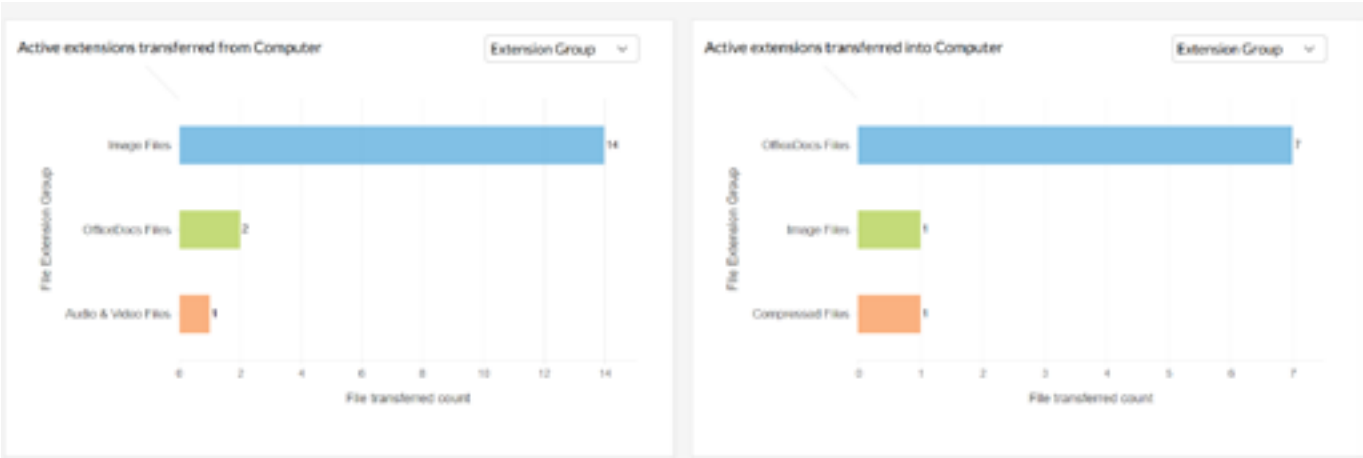
SLEDOVÁNÍ POKUSŮ O ZÍSKÁNÍ NEOPRÁVNĚNÉHO PŘÍSTUPU

Díky vestavěným zprávám, auditům a oznámením zjistěte, kdo používá USB zařízení a na kterých počítačích.



ŠIROKÁ ŠKÁLA PODPOROVANÝCH ZAŘÍZENÍ

USB paměti, zařízení Apple, Bluetooth, tiskárny, modemy, WiFi adaptéry, COM a LPT porty, čtečky karet, páskové jednotky, CD mechaniky, myši



Detekce zranitelností a hrozeb

Vulnerability Manager Plus

Vulnerability Manager Plus je integrovaný nástroj pro správu zranitelností a hrozeb, který poskytuje možnost komplexního posouzení rizik pro všechny počítače nacházející se v organizaci. VMP umožňuje skenovat a objevovat zranitelné oblasti organizace, lokálně i v pobočkové síti. Přístup k analýzám založených na typech útoků umožňuje identifikovat a upřednostnit oblasti, které mohou být nejvíce ohroženy útoky.

Díky VMP se schopnost zneužití bezpečnostních chyb v systému výrazně snižuje a zabraňuje vzniku ddalších zranitelností.

POSOUZENÍ ZRANITELNOSTI

Identifikace a vyhodnocení hrozby na základě možnosti využití slabého místa, úrovně hrozby, počtu náchylných systémů a existence „záplaty“ pro zabezpečení zranitelnosti.

SPRÁVA AKTUALIZACÍ

Automatizace procesu aktualizace automatickým stahováním, testováním a implementací aktualizací pro systémy Windows, MacOS, Linux a více než 250 aplikací třetích stran.

SPRÁVA KONFIGURACE ZABEZPEČENÍ

Optimalizace zabezpečení systému vynucováním silných hesel, poskytováním minimálních požadovaných oprávnění a zajištěním souladu s doporučeními CIS a STIG.

ZABEZPEČENÍ WEBOVÝCH SERVERŮ

Přístup k informacím o příčinách, dopadech a nápravných opatřeních týkajících se bezpečnostních chyb serveru. Tyto informace umožní, aby byly servery udržovány a řádně chráněny proti mnoha útokům.

SOFTWAROVÝ AUDIT RIZIK

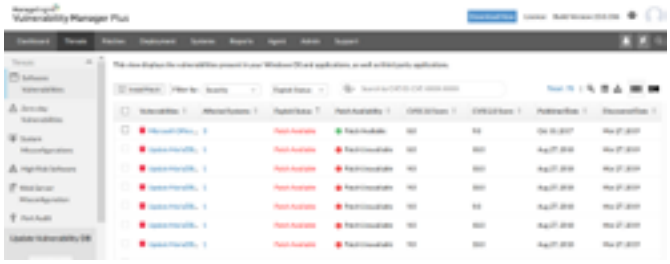
Identifikace nebezpečného softwaru, jako je vzdálené sdílení plochy nebo P2P aplikace, a jejich automatické odinstalování.

OMEZENÍ ZRANITELNOSTI TYPU ZERO-DAY

Implementace ověřených skriptů bez čekání na oficiální bezpečnostní opravu za účelem ochrany před zranitelnostmi typu zero-day

AUDIT ANTIVIROVÉHO SOFTWARU

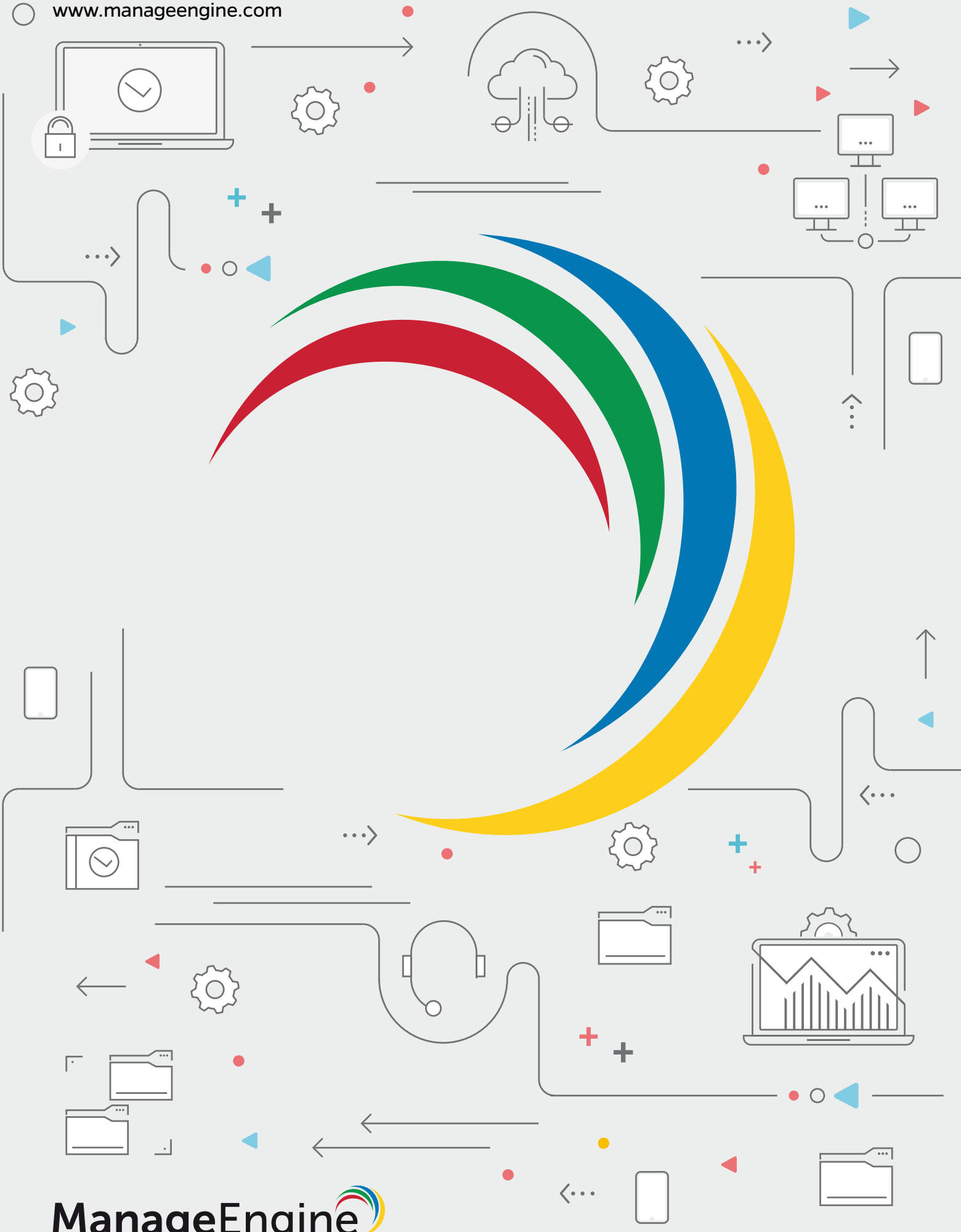
Přístup k informacím o antivirovém softwaru nainstalovaném v jednotlivých počítačích spolu se stavem operace a datem aktualizace.



AUDIT PORTŮ

Sledování používaných portů a procesů, které na ně navazují a identifikace otevřených portů, které mohou být použité k útoku.

www.manageengine.com



ManageEngine