BVS Caleum

BUSINESS VISIBILITY SUITE

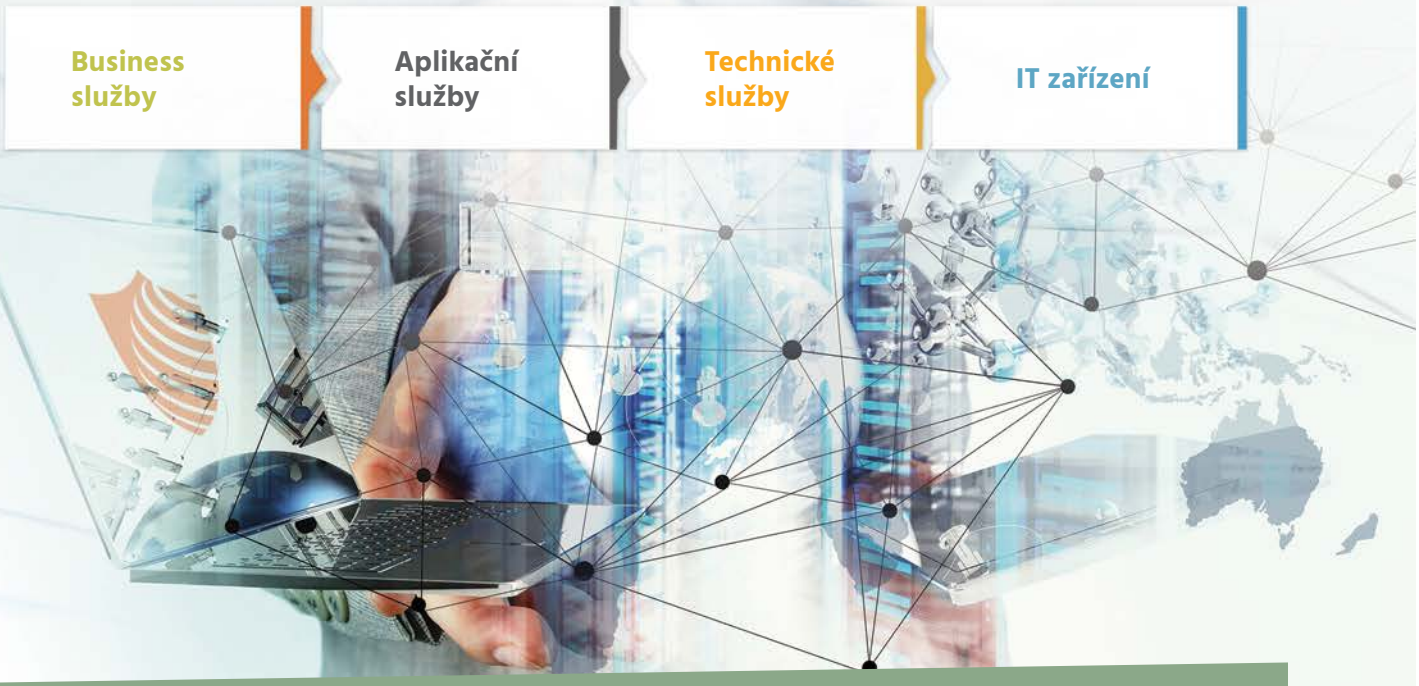
Network & Business Edition

Nástroj pro přehlednou vizualizaci síťových komunikací a modelování souvislostí business služeb s IT infrastrukturou

Řízení IT aktiv je základním předpokladem pro úspěšné zvládání incidentů v rychle se měnícím kybernetickém prostředí. Přehled nad komunikačními vztahy IP zařízení v čase poskytuje Security analytikům i SOC operátorům informace pro servisní zásahy, rychlou identifikaci a šetření bezpečnostních událostí v síťové infrastruktuře.

Nástroj BVS unikátně propojuje svět IT techno-logií a business služeb organizace díky možnostem intui-tivního modelování závislostí mezi těmito vrstvami. Hlavní výhodou je automatizovaný sběr metadat o síťových komunikačních vztazích mezi IT zařízeními s možností modelování zajišťovaných business služeb organizace.

BVS UMOŽŇUJE UCHOVAT NÁSLEDUJÍCÍ VZTAHY:



Business visibility suite je nástrojem pro okamžitý přehled a vizualizaci síťové komunikace IP zařízení pro rychlé šetření a identifikaci bezpečnostních udá-lostí v infrastruktuře. Pomáhá rovněž porozumět dopadům incidentů na provozované business služ-by a předcházet bezpečnostním hrozbám.

S pomocí nástroje BVS se lze snadno zorien-tovat v reálném stavu vlastní IT infrastruktury a vztazích mezi IT aktivy (visibilita komunikací mezi síťovými zaří-zeními), a to díky automatizovanému zpracování síťové komunikace. Je možné tak získat vstupy pro okamžité řešení bezpečnostních incidentů v kontextu dopadu na provozované služby.

BVS nabízí následující dva funkční moduly:

1. BVS Network Edition – vizualizace aktuálního stavu IT infrastruktury a zachycení komunikací mezi IT zařízeními s uložením historie komunikací. Poskytuje představu o chování sítě – jaký typ provozu se v dané lokalitě vyskytuje.

2. BVS Business Edition – nadstavba nad síťovým modulem, která umožní modelování business služeb a jejich závislostí na IT infrastruktuře. Dává tak aktuální pohled na význam a kritičnost IT zařízení při provozování klíčových služeb pro koncové zákazníky.

BVS Network Edition

Základní modul **BVS Network Edition** pomůže odpovědět na základní otázky:

- Jaká zařízení jsou v daný okamžik přítomna v síti?
- Nejedná se o nová a neautorizovaná zařízení?
- Jaká zařízení na síti již nejsou dlouhodobě využívána (tzv. dead woods)?
- Jaká jsou nová spojení a pokusy o komunikaci mezi zařízeními? Nejedná se o projev nežádoucího a škodlivého chování zařízení? Nejedná se o nová a neautorizovaná zařízení?
- Kdo je technickým vlastníkem zařízení?
- Jaké služby (porty) jsou v síti provozovány?
- Jaká další zařízení ovlivní dostupnost sledovaného zařízení?
- Jaká je komunikační historie (profil) vybraného zařízení a změny na něm provedené?
- Jaká je množina dotčených zařízení, která komunikovala s danou IP ve vybraném časovém rozpětí?
- Jaké jsou poslední změny zařízení (otevřené porty, změna rizika, zranitelnosti a další)?

Možné scénáře využití BVS Network Edition:

1. **Migrace ICT infrastruktury do prostředí cloudu**
   > Lokalizace aktiv (segment, vlastník, risk)
   > Identifikace všech provozovaných služeb a závislostí
   > Export komunikační matice zařízení
2. **Identifikace rozsahu kybernetického incidentu**
   > Organizace získá informace o možné kompromitaci informačního systému
   > Jako identifikátor je uvedena IP adresa systému
   > BVS vizualizuje ve vybraném časovém úseku všechna dotčená zařízení
3. **Implementace NAC nástrojů**
   > Okamžitá orientace v aktuálním síťovém prostředí umožní rychlejší nasazení NAC nástrojů, včetně AddNetu

Možné scénáře využití BVS Business Edition:

1. **Podpora práce SOC týmu**
   > Prioritizace šetření incidentů dle kritičnosti aktiva
   > Predikce šíření útoku ve vazbě na kritičnost aktiv
   > Rychlá identifikace rozsahu kybernetického incidentu
   > Reporting na úroveň business služeb
2. **Plánování změn v infrastruktuře s dopady na kontinuitu služeb**
   > Podpora pro rychlé vytvoření Business Impact Analýzy
   > Identifikace a snadná údržba informací o existenci aktiva a jeho vazbě na konkrétní provozované služby
3. **Podklady pro optimalizace IT infrastruktury**
   > Podklady pro oddělení kritických a nekritických aktiv
   > Identifikace „Single Point of Failure“

BVS Business Edition

Modul **BVS Business Edition** je svým zaměřením a funkčností vhodný pro pracovníky SOC, manažery IT a IT security, kteří chtějí mít přehled o aktuálních rizicích provozovaných služeb a jejich dostupnosti včetně vazeb na podpůrné IT prostředky.

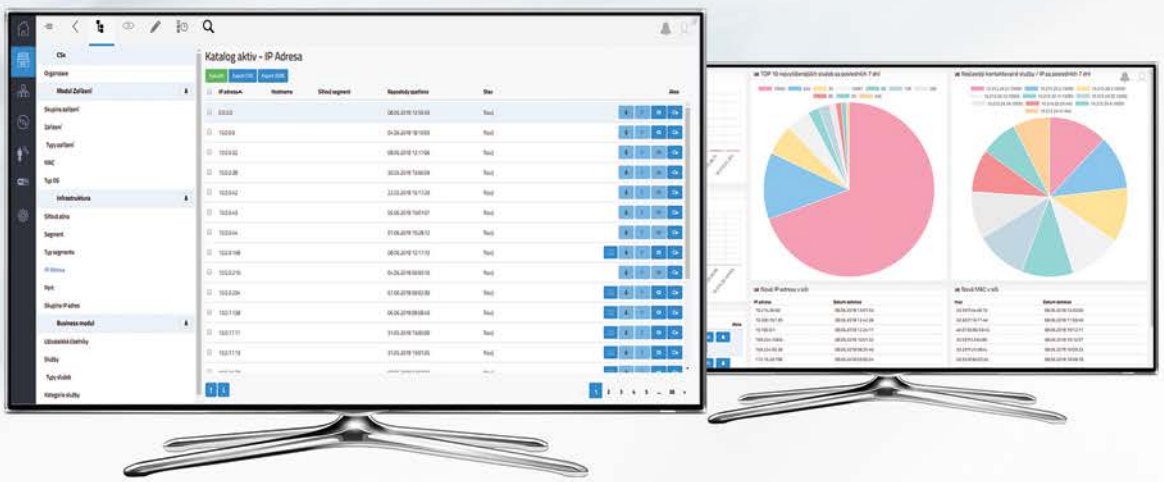
BVS Business Edition modul přináší následující možnosti:

- Tvorbu logických aktiv reprezentujících technické, aplikační a business služby organizace.
- Katalogizaci poskytovaných služeb s volitelnými atributy.
- Upozorňování na změnové stavy IT aktiv a jejich dopad na definované služby.
- Vizuální modelování závislostí mezi business službami, aplikacemi, IT službami a IT zařízeními (tzv. Business Impact analýza) s automatizovanou podporou identifikace a chování aktiv díky BVS Network Edition.
- Snadná správa a sledování aktuálního stavu business služeb v rámci servisního modelu (přehled klíčových provozovaných služeb, jaké aplikace je zajišťují, na jakých prostředcích běží).
- Identifikace dopadů provozních událostí na business služby organizace (what-if scénáře).
- Přehled o možném dopadu zranitelností detekovaných u podpůrných technických IT aktiv na poskytované služby (pro prioritizaci eliminace rizik zneužití zranitelností s dopadem na kritické služby).
- Zajištění kontinuity služeb díky lepšímu přehledu o podpůrné infrastruktuře.

BVS

Přehled funkcí a možností BVS
(Network & Business Edition)

Vizualizace IT zařízení (aktiv), která jsou přítomna v komunikační infrastruktuře	Identifikace vztahů mezi objekty, které jsou součástí síťové komunikace, v Business edici rovněž vizuální modelování závislostí mezi službami, aplikacemi a zařízeními.
Grafické ovládání	Možnost pohybovat se ve vztazích hierarchickým způsobem od hlavních uzlů a síťových segmentů, přes IP adresy zařízení až po služby provozované na souvisejících portech (drill-down).
Alerting	Upozorňování na změny v infrastruktuře, notifikace vlastníků aktiv na změny.
Automatizovaný sběr metadat o prvcích infrastruktury a jejich komunikacích	Využití autonomní sondy pro extrakci metadat o síťových komunikacích a jejich vizualizace v téměř reálném čase. Základní informace o komunikačních vazbách (segment sítě, IP zdroj, IP cíl, protokol, cílová služba, tj. cílový komunikační port).
Možnost tagování uzlů (zařízení)	Pro účely seskupování prvků, podléhajících auditním požadavkům nebo interním směrnicím, je možné zařízení označovat dle libovolných tagů.
Zobrazování odchozí / příchozí komunikace IT zařízení	IP adresa komunikující na porty dalších zařízení, včetně opačného zobrazení, tj. příchozí komunikace na služby provozované na portech této IP adresy.
Evidence popisných informací	• název aktiva, • typ aktiva, • identifikátor aktiva (dle typu aktiva, např. IP adresa, MAC, port...) • technický vlastník (správce), • možnost vytváření uživatelsky definovaných metadat
Přehledový seznam katalogu aktiv	Export do XLS, CSV.
Časová osa	Umožňuje porovnávat aktuální stav infrastruktury s vybraným časovým okamžikem v minulosti (např. zvýrazněním nově identifikovaných aktiv v infrastruktuře).
Přehled událostí	Úvodní portál s přehledem událostí, možnost aktivní práce s grafy (např. zoom na detail vybraných prvků).
Centrální fulltext	Upozorňování na nová neschválená zařízení umožní předcházet incidentům (alerting).
Datová retence a výkonnost	Umožňuje vyhledat zařízení dle libovolných atributů.
Oddělený přístup k funkcím aplikace	Schopnost systému zpracovávat a uchovávat velký objem dat na vstupu (více než 10 GB dat za den) a uložení klíčových metadat pro šetření incidentů na dostatečně dlouhou dobu. Autentizace uživatelů, bezpečný přístup ke konkrétním funkčním oblastem aplikace na základě vytvořených rolí.



Přínosy produktu:
BVS – Business Visibility Suite

- Jednoduchý a intuitivní nástroj s významnou podporou pro rychlejší šetření kybernetických incidentů.
- Rychlá orientace v komplexním prostředí síťových komunikací.
- Zmapování chování komunikační a síťové infrastruktury zákazníka pro rychlý start služeb SOC
  - Síťová infrastruktura a identifikace zařízení spojená např. s aktivitami „shadow IT".
  - Monitoring Wi-Fi a síťových komunikací.
- Rychlá identifikace síťových komunikačních vztahů mezi IT zařízeními pro zkrácení doby implementace a nastavení nástrojů typu Network Access Control.
- Integrace s NAC umožňuje komplexní pohled od vrcholových business služeb až na úroveň konkrétně fyzicky identifikovatelného zařízení.
- Minimální požadavky na součinnost se zákazníkem, postačí předání základních informací o adresních rozsazích, v nichž se nacházejí komunikující prvky.
- Identifikace a snadná údržba vztahů a závislostí mezi business službami / aplikacemi a infrastrukturou – rychle zjistíte, které služby jsou ohroženy bezpečnostními riziky.
- Přehledná a bezproblémová migrace infrastruktury do cloudu díky přehledu komunikačních závislostí mezi systémy, které je třeba migrovat, a hlavními IS. Tím je zajištěna spolehlivá migrace všech potřebných systémů a předchází se výpadkům provozovaných služeb.
- Lepší plánování nákladů na správu zařízení s ohledem na to, jaké business služby, a s jakým rizikem, jsou na něm provozovány.
- Evidence základních kontextových informací přímo u IT aktiva znamená úsporu času (není vždy třeba dohledávat informace ve více nástrojích).
- Rychlá identifikace aktuálního „zdraví infrastruktury" a vyhledání původců potenciálních bezpečnostních hrozeb (prevence před nekontrolovaným spouštěním nových služeb v síti, apod.).
- Podpora vysoce efektivního provedení business impact analýzy.

Neznalost chráněného prostředí znemožňuje rychlou reakci IT a efektivní práci SOC při zvládání incidentů.

Technické prostředky pro BVS

Do prostředí zákazníka jsou instalovány následující zařízení:

- Fyzické sondy pro monitoring síťových spojení (standardní 1U do racku, se 2 síťovými rozhraními – pro data ze SPAN/monitoring rozhraní síťových přepínačů na vstupu 10 Gbit/s + rozhraní 1 Gbit/s pro komunikaci s BVS serverem)
- Volitelně fyzické Wi-Fi sondy pro monitoring Wi-Fi spektra (standardní Mini PC zařízení kompatibilní s většinou Wi-Fi standardů)
- Management a kolektor na HW zařízeních dodaných společně s řešením BVS nebo vlastních prostředcích zákazníka
  - Podpora pro virtualizaci v prostředí VMware i na fyzickém zařízení
- Využívají se osvědčené hardwarové Appliance

Implementace BVS

- Implementace probíhá podle standardních implementačních postupů, na které jsou partneři trénováni.
- V první fázi dojde k nasazení potřebné BVS infrastruktury do sítě zákazníka a ke spuštění modulu BVS Network
- Modul BVS Business je možné efektivně využívat po provedení business impact analýzy

Součinnost při implementaci BVS

- Zapojení sond na switche sledované infrastruktury (pro modul IT infrastruktura)
- Definice rozsahu sledovaných segmentů
- Interpretace vybraných komunikací podrobených analýze
- Zajištění prostupů mezi komponentami nástroje BVS
- Zpřístupnění základních síťových služeb DNS a NTP
- Vzdálený přístup pro obousměrnou komunikaci a přístup k/ze zařízení (provozovatel zařízení BVS > prostředí zákazníka; prostředí zákazníka > provozovatel zařízení BVS)

Caleum

Caleum a.s., Itaská 438
Praha 3, Česká republika

www.caleum.cz
sales@caleum.cz

BVS