safetica NXT

Next-gen SaaS DLP

Chraňte svá citlivá data před zneužitím. Odhalte bezpečnostní rizika a předcházejte incidentům. Už od prvního dne.

- **Cloudové DLP** nasazené za pár hodin, implementované v řádu dnů
- **Snadné ovládání** podpořené automatizací a osvědčenými postupy
- **Detekce incidentů založená** na riziku a podporovaná datovou analytikou
- **Ideální pro hybridní pracovní prostředí a práci na dálku**

Verze: 2022-03-07

www.itbezproblemu.cz

safetica NXT

Odhalování bezpečnostních rizika prevence incidentů od prvního dne

Safetica NXT je next-gen SaaS (Software as a Service) DLP, které klade důraz na velmi rychlé nasazení a nenáročnou údržbu. Pomůže vám včas odhalit potenciální hrozby a analyzovat rizika ve firemních datových tocích. Budete tak moci včas reagovat, svá data chránit, nastavit si pravidla pro nakládání s citlivými daty, vzdělávat své zaměstnance a zajistit dodržování předpisů.

Data jsou klíčovým aktivem každé firmy bez ohledu na její velikost. Při ztrátě nebo krádeži citlivých dat organizace často přijde o dobrou pověst, konkurenceschopnost i zisky.

14,4 mil. Kč

Průměrné náklady na incident spojený se insidery, Ponemon Institute, 2020

Jak Safetica NXT řeší zabezpečení dat

Safetica NXT vyhodnocuje riziko všech souborových operací a uživatelů. Dokáže detekovat a blokovat bezpečnostní incidenty v odchozích datech a ukazuje, zda nedošlo k jejich ztrátě nebo zneužití. S využitím moderních technologií kontroluje činnost koncových zařízení a poskytuje podrobnosti o každém přenosu.

Každá operace se soubory je zaznamenána, vyhodnocena a bezpečně uložena v cloudu Microsoft Azure. To vám umožní nejen reagovat a zabránit případnému úniku dat, ale také vzdělávat zaměstnance a měnit jejich chování nebo firemní procesy.

V dnešním distribuovaném pracovním prostředí poskytuje Safetica tolik potřebný přehled o pohybu dat mezi koncovými zařízeními, uživateli i cloudy.

Next-gen SaaS DLP vám umožní

- Na základě automatizované detekce podezřelého nebo neobvyklého chování a analýzy rizik v datových tocích předcházet incidentům, rychle reagovat na potenciální vnitřní hrozby a urychlit vyšetřování nebezpečných aktivit.
- Provádět audit všech dat opouštějících organizace a získat jasný přehled o bezpečnostních incidentech tím, že ukáže, kdo, kdy, kam a jak data odeslal.
- Tiše zaznamenat událost, nebo zaměstnance upozornit na potenciální riziko operace.
- Blokovat vysoce rizikové události, a zabránit tak přenosu citlivých dat z koncového zařízení.

www.itbezproblemu.cz

Hlavní přínosy a scénáře

Rychlý přínos a vysoká flexibilita
- Nasazení za pár hodin, implementace za pár dnů.
- Měsíční fakturace umožňuje flexibilní optimalizaci nákladů a využívání služeb podle potřeby.

Snadná správa
- Šetřete čas díky přednastaveným šablonám, automatizaci a ověřeným postupům.
- Automatická detekce rizikových událostí, uživatelů a bezpečného digitálního pracovního prostředí.

Detekce incidentů využívající riziko
- Komplexní klasifikace rizikse schopností učení. Založené na datové analytice.
- Jedinečná detekce záměrů a skutečných aktivit uživatelů.

Podpora hybridního prostředí
- Vhodné i pro prostředí, kde uživatelé pracují z domova nebo vzdáleně.
- Analytika založená na dynamickém rozpoznání pracovní doby.

Plné pokrytí perimetru
- Úplná transparentnost datových kanálů.
- Multiplatformní podpora
- Ochrana dočasně odpojených zařízení a ochrana proti neoprávněné manipulaci.

Vyspělá architektura
- Cloudová multitenantní architektura stavící „bezpečnost na první místo“.
- Velmi nízké nároky na výkon koncových zařízení (pod 3 %).

Klasifikace dat a audit datového toku

Detekujte a klasifikujte citlivá data na základě vestavěných šablon. Provádějte audit pohybu dat ve všech důležitých kanálech.

Detekce a reakce na incidenty

Využijte chytrou automatickou detekci incidentů a automatické vyhodnocení rizik a podezřelého nebo nestandardního chování.

Ochrana duševního vlastnictví a citlivých dat

Chraňte před únikem své know-how a další informace o firmě nebo zákaznících. Předejděte nevhodné manipulaci s důležitými daty nebo jejich krádeži.

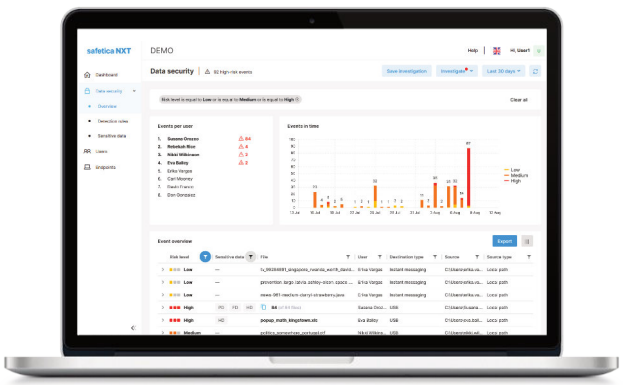
Detekce porušení souladu s předpisy

Detekujte a provádějte audit porušení souladu s pravidly GDPR, HIPAA nebo PCI-DSS. Nastavte adekvátní ochranu a vynucujte dodržování interních pravidel.

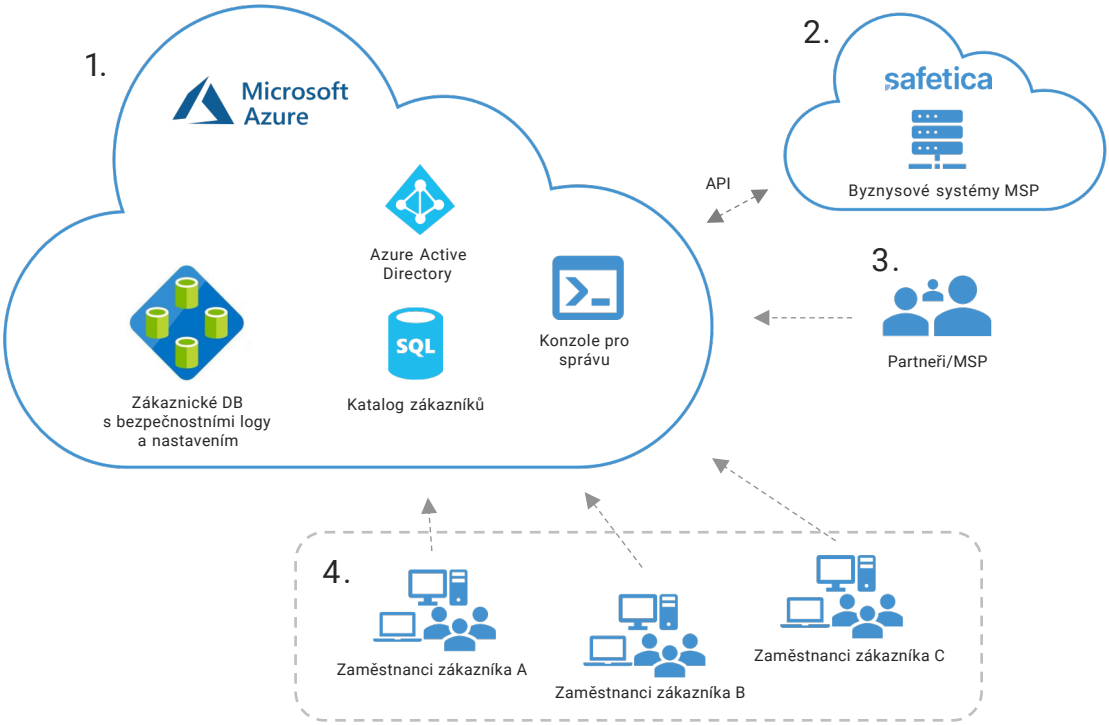
Užitečné reporty

Safetica poskytuje rychlý a srozumitelný přehled o všech možných hrozbách v jediném rozhraní. Užitečné informace získáte kdykoli a na jakémkoli zařízení.

Můžete dostávat e-mailová oznámení o podezřelém chování, číst důležité statistiky na ovládacím panelu nebo exportovat nezpracovaná data do formátu .xls pro další analýzu.



Referenční architektura



1. Hostující platforma

- Cloudová platforma, na které běží Safetica NXT
- MS Azure s datacentry v NL/EU
- Multitenantní architektura
- Vysoká škálovatelnost a zabezpečení
- Uživatelské rozhraní pro partnery a zákazníky
- Není třeba hardware pro nasazení back-endu

2. Supporting infrastructure

- Podpůrné služby Safetica (CRM, partnerský systém, fakturační systém)
- Nativní integrace s hostujícím platformou
- Průběžná automatizace obchodních procesů, která zabraňuje vzniku jakýchkoli překážek

3. Partneři/MSP

- Partneři přeprodávající Safetica NXT (self-managed), MSP poskytující Safetica NXT (spravovaná služba)
- Jednoduchý a rychlý onboarding
- Možnost centralizované správy
- Flexibilní zákaznická podpora
- Měsíční/roční předplatné

4. Zákazníci

- Společnosti chráněné řešením Safetica NXT
- Přístup k reportům přes prohlížeč odkudkoli
- Zasílání okamžitých e-mailových oznámení
- Uživatelé s chráněnými zařízeními* Mac nebo Windows zařízeními*, která mají nainstalovaný Safetica Client
- Rychlý proces nasazení

* Požadavky na Safetica Client:

- 2,4 GHz čtyřjádrový procesor, 2 GB RAM, 10 GB místa na disku
- Windows 7, 8.1, 10, instalační balíček MSI, .NET 4.7.2+
- macOS 10.15+

safetica NXT

Jak to funguje

Extrémně rychlé nasazení umožňuje zahájit audit pohybu dat a detekci incidentů během jediného dne. Předkonfigurovaná detekční pravidla se aktivují automaticky a následně je lze dále ladit a přizpůsobovat. Režim ochrany lze zapnout později na základě získaných informací o rizicích.

1. Prostředí zákazníka automaticky nasazené v zabezpečeném cloudu
2. Aplikace Safetica vzdáleně nainstalovaná na koncová zařízení zaměstnanců
3. Řešení Safetica NXT je připravené provádět audit dat a upozorňovat na incidenty

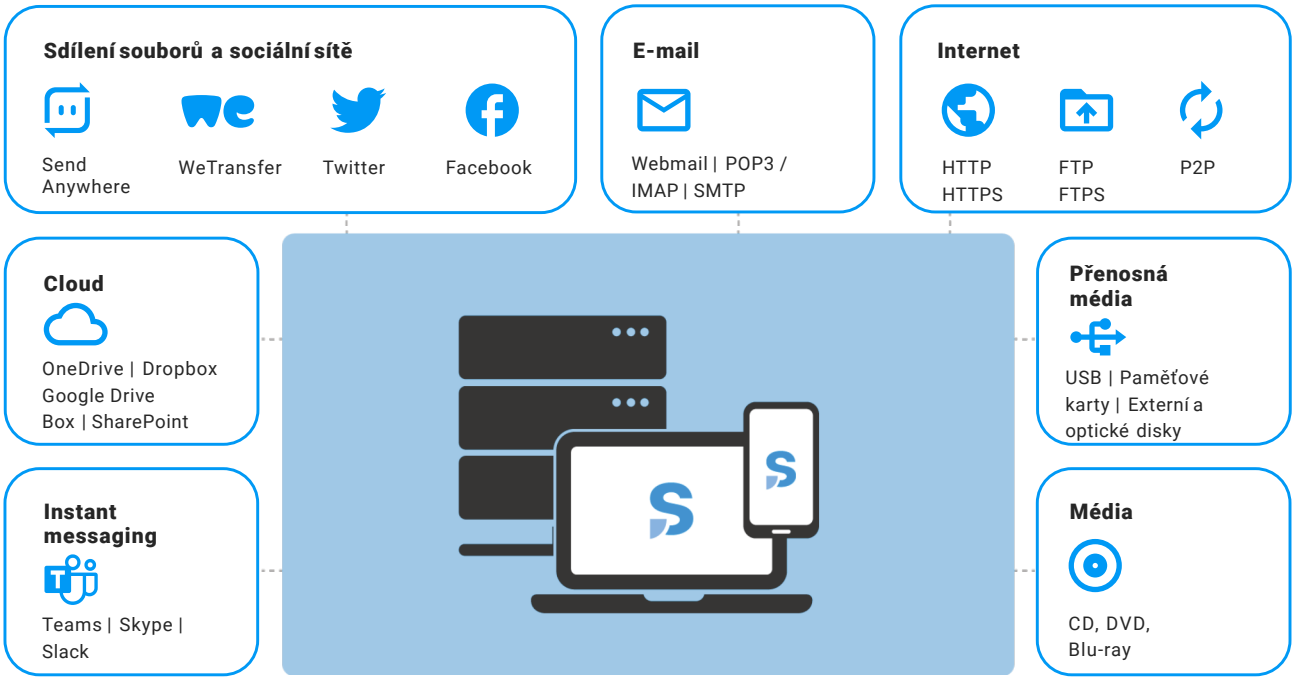
Detekce incidentů je založená na nativní logice, automatické detekci anomálií a průběžném učení. Výstupem je sada rizikových událostí, které Safetica NXT identifikuje a označuje pomocí třístupňové klasifikace rizik (nízké riziko, střední riziko, vysoké riziko).

Vysoké riziko
Střední riziko
Nízké riziko

S režimem ochrany dat (DLP) můžete události tiše zaznamenávat, upozornit zaměstnance na potenciální riziko operace nebo ji zablokovat. DLP s adaptivní ochranou dat využívá dynamickou detekci digitálního pracovního prostoru, jehož definice se průběžně upravuje podle chování uživatelů.

Pokryté datové kanály

Safetica NXT poskytuje přehled o firemních datech napříč různými kanály a platformami, čímž zajišťuje jejich úplnou transparentnost bez ohledu na to, kde se data nacházejí nebo kudy tečou.



www.itbezproblemu.cz

6 000+
počítačů ve správě

200+
firem

Kdo jsme

COM Group nebo také **itbezproblemu.cz** je česká společnost, která poskytuje **komplexní správu IT**, včetně řešení pro IT bezpečnost, špičkového vybavení, školení a digitalizace firem. Pracujeme s těmi nejlepšími, mezi které patří také značka Safetica a její produkty.

Kdo s námi spolupracuje

PS BRNO
Laktos Since 1936
MEGA BOOKS CZ
1CSC
botas
iba
UNCS UNLIMITED CLOTHING STYLE
DESTILA 1947

Špičková ochrana dat.
Jednoduše.

Zeptejte se nás na bezpečnost Vašeho IT:
info@itbezproblemu.cz

safetica