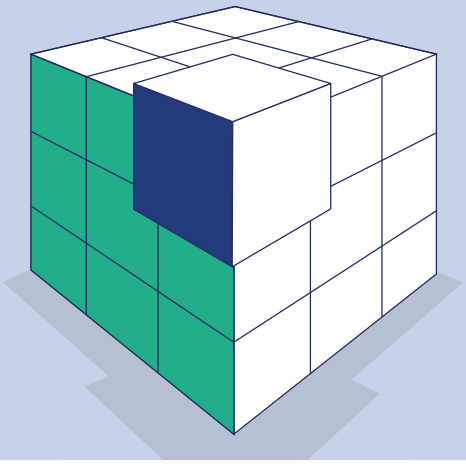


IXTRUST
by IXPERTA

Inteligentní ochrana dat

IXTRUST je řešení, které poskytuje spolehlivou ochranu a efektivní správu dat. Praktické procesy a jednoduché nasazení.

IXPERTA přináší na trh řešení IXTRUST pro inteligentní ochranu dat, logů a záloh. V jednom řešení kombinuje bezpečné zálohování, bezpečnostní analýzu, identifikaci čisté zálohy pro bezpečnou obnovu a rychlou obnovu provozu po kybernetickém incidentu. Je dostupné pro firmy všech velikostí, včetně malých a středních podniků, které chtějí posílit svou kybernetickou odolnost.

IXTRUST není jen další bezpečnostní software. Jde o komplexní SaaS řešení, které umožňuje firmám předcházet kybernetickým útokům, reagovat na incidenty a rychle se z nich zotavit. Je to inteligentní ochrana dat bez starostí.

Je určen firmám, které chtějí ochránit svůj digitální ekosystém rychle, spolehlivě a finančně efektivně – bez potřeby vlastního bezpečnostního týmu.

PROČ IXTRUST

IXTRUST je řešení, které poskytuje spolehlivou ochranu a efektivní správu digitálních identit.

CO nabízí IXTRUST

Poskytuje rychlou a bezpečnou obnovu záloh spolu s analýzou systémů v čase a forenzním zkoumáním znaků kompromitace.

JAK funguje IXTRUST

IXTRUST je SaaS řešení, které propojuje čtyři klíčové oblasti kybernetické odolnosti:

- Backup & recovery prostředí
- Detekce hrozeb z logů i záloh
- Identifikace čistého bodu obnovy
- Rychlé obnovení provozu

Čím je IXTRUST specifický?

1. Inteligentní ochrana dat a logů

IXTRUST propojuje ochranu dat, záloh a logů do jednoho řešení, které pomáhá organizacím předcházet kybernetickým incidentům a minimalizovat jejich dopady.

1. **Ochrana kritických firemních dat**
2. **Uchování logů a důkazní stopy útoku**
3. **Vyšší kybernetická odolnost organizace**

2. Bezpečné zálohování a obnova

IXTRUST zajišťuje bezpečné ukládání záloh a jejich rychlou obnovu v případě kybernetického útoku nebo provozního incidentu.

1. **Zálohy se zvýšenou ochranou proti neoprávněné změně**
2. **Identifikace čisté zálohy**
3. **Identifikace čistého bodu obnovy**
4. **Rychlá obnova provozu po incidentu**
5. **Minimalizace výpadků a ztrát**

3. Detekce hrozeb a analýza logů

IXTRUST průběžně analyzuje logy a bezpečnostní události, díky čemuž pomáhá odhalit i skryté nebo dlouhodobě přítomné hrozby.

1. **Aktivní monitoring bezpečnostních událostí**
2. **Analýza logů a detekce anomálií**
3. **Včasné odhalení potenciálních rizik**

IXPERTA

Jan Rys
Presales System Engineer IXPERTA
jan.rys@ixperta.com
+420 604 296 262

www.ixperta.com

IXTRUST
by IXPERTA

TOP technické vlastnosti IXTRUST

Threat Detection & Backup Security Analysis

- Analýza bezpečnostních událostí založená na lozích
- Skenování záloh a detekce škodlivého obsahu
- Identifikace čisté zálohy
- Multi-tenant model IT architektury

Secure Multitenant Environment

- Bezpečně oddělené prostředí pro ukládání záloh
- Testování obnovy a recovery scénářů
- Okamžitá dostupnost dat při obnově provozu

Security Log Analytics

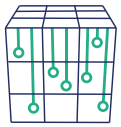
- Automatizace metadat a anonymizace
- Detekce vektorů útoku a podpora forenzní analýzy
- Definice bezpečného recovery procesu

Secure Log Protection & Recovery Intelligence

- Bezpečné uchování a archivace kritických logů
- Podpora forenzní analýzy a vyšetřování incidentů
- Identifikace bezpečného recovery pointu

Recovery Process & Compliance Framework

- Návrh recovery procesů a postupů obnovy
- Podpora bezpečnostních politik organizace
- Optimalizace plánů obnovy a kontinuity provozu

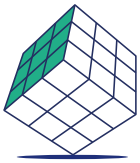


AI-Powered Threat Intelligence

- AI podpora analýzy bezpečnostních událostí
- Prediktivní identifikace rizik a anomálií
- Průběžná aktualizace znalostní báze hrozeb

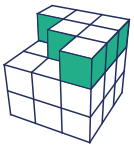
Immutable Backup & Recovery Engine

- Nesmazatelné zálohy chráněné proti manipulaci
- Možnost šifrování uložených dat
- Oddělené uložení záloh mimo dosah kybernetických útoků



Flexible Deployment Model

- SaaS model bez nutnosti budovat vlastní infrastrukturu
- Data bezpečně uložená v České republice
- Přizpůsobení rozsahu ochrany podle potřeb organizace



Integrace bezpečnostních dat a zdrojů

- Integrace na existující IT infrastrukturu
- Připojení vybraných zdrojů logů a bezpečnostních událostí
- Centralizace bezpečnostních dat pro analýzu a reporting
- Napojení na bezpečnostní, provozní a zálohovací systémy

Analýza logů pro detekci a vyhodnocení incidentu

- Sběr a centralizace bezpečnostních logů
- Detekce podezřelých aktivit a anomálií
- Vyhodnocení časové osy kybernetického útoku
- Identifikace zasažených systémů a účtů
- Podpora rozhodnutí o dalším postupu obnovy

IXPERTA

Vytvořeno ve spolupráci s ECCC a ČVUT – FEL,
s podporou EU DIGITAL Europe Programme:

FAKULTA ELEKTROTECHNICKÁ ČVUT V PRAZE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

www.ixperta.com

IXTRUST by IXPERTA

Balíčky služeb IXTRUST

PRO ZAČÁTEK

Essential

Bezpečné zálohování a rychlá obnova.

Balíček obsahuje:

- ✓ Bezpečné zálohování kritických firemních dat
- ✓ Rychlá dostupnost dat pro obnovu provozu
- ✓ Obnova bez nutnosti dodatečného schvalování
- ✓ Šifrovaný přenos dat
- ✓ Nesmazatelné (WORM) úložiště
- ✓ Licence zálohovací platformy
- ✓ Osvědčené procesy zálohování a obnovy, definice pravidel pro uchování a dostupnost záloh

Vyberte si Essential, ak:

Ste organizace, která chce zajistit ochranu dat, mít jistotu rychlé dostupnosti záloh pro obnovu a zachovat si plnou kontrolu nad svými daty bez nutnosti schvalování ze strany dodavatele.

NEJOBLÍBENĚJŠÍ

Advanced

Ochrana záloh před kybernetickými hrozbami.

Balíček obsahuje:

- ✓ Bezpečné zálohování kritických firemních dat
- ✓ Rychlá dostupnost dat pro obnovu provozu
- ✓ Obnova bez nutnosti dodatečného schvalování
- ✓ Šifrovaný přenos dat
- ✓ Nesmazatelné (WORM) úložiště
- ✓ Licence zálohovací platformy
- ✓ Osvědčené procesy zálohování a obnovy, definice pravidel pro uchování a dostupnost záloh
- ✓ Bezpečnostní skenování záloh
- ✓ Identifikace bezpečné („čisté“) zálohy
- ✓ Včasné odhalení potenciálních hrozeb

Vyberte si Advanced, ak:

Ste organizace, která chce nejen zálohovat, ale také průběžně ověřovat bezpečnost svých záloh.

PRO NÁROČNÉ

Premium

Komplexní ochrana dat, záloh a logů.

Balíček obsahuje:

- ✓ Bezpečné zálohování kritických firemních dat
- ✓ Rychlá dostupnost dat pro obnovu provozu
- ✓ Obnova bez nutnosti dodatečného schvalování
- ✓ Šifrovaný přenos dat
- ✓ Nesmazatelné (WORM) úložiště
- ✓ Licence zálohovací platformy
- ✓ Osvědčené procesy zálohování a obnovy, definice pravidel pro uchování a dostupnost záloh
- ✓ Bezpečnostní skenování záloh
- ✓ Identifikace bezpečné („čisté“) zálohy
- ✓ Včasné odhalení potenciálních hrozeb
- ✓ Sběr a bezpečné uchování logů
- ✓ Propojení logů a záloh pro rychlejší analýzu incidentů
- ✓ Podpora forenzního šetření
- ✓ Identifikace zdroje a průběhu útoku
- ✓ Podpora compliance a auditovatelnosti

Vyberte si Premium, ak:

Potřebujete vyšší úroveň ochrany dat, pokročilé funkce zálohování a obnovy, větší flexibilitu při správě prostředí a rozšířené možnosti zabezpečení pro kritické firemní systémy.

Od bezpečného zálohování až po pokročilou analýzu logů – IXTRUST roste spolu s potřebami vaší organizace.

IXTRUST: Inteligentná ochrana dát bez starostí

Vyberte si úroveň ochrany dat, která odpovídá vaší organizaci – od spolehlivého zálohování a rychlé obnovy až po komplexní kybernetickou odolnost s analýzou logů a podporou při řešení incidentů.

IXPERTA

Vytvořeno ve spolupráci s ECCC a ČVUT – FEL, s podporou EU DIGITAL Europe Programme:

FAKULTA ELEKTROTECHNICKÁ ČVUT V PRAZE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

www.ixperta.com

IXTRUST by IXPERTA

Proč organizace volí IXTRUST

Proč právě teď

Kybernetický útok dnes neznamená pouze ztrátu dat. Firmy musí řešit výpadek provozu, regulatorní povinnosti, ztrátu důvěry zákazníků i nákladnou obnovu systémů. Klíčovou otázkou proto není pouze ochrana dat, ale schopnost rychle a bezpečně obnovit provoz.

- Nejčastější výzvy, které firmy řeší
- Máte zálohy. Víte ale, zda jsou po útoku skutečně použitelné?
- Bez logů nevíte, co se stalo.
- Jak určit bezpečný bod obnovy po incidentu?
- Jak zvýšit kybernetickou odolnost bez vlastního SOC?
- Jak splnit rostoucí regulatorní požadavky?

Jak IXTRUST pomáhá

Zálohy, které pomohou i po útoku
Průběžně ověřuje stav záloh a pomáhá určit bezpečný bod obnovy.

Ochrana dat i logů
Uchovává a analyzuje logy potřebné pro vyšetření incidentu a obnovu provozu.

Podpora NIS2 a auditovatelnosti
Pomáhá organizacím uchovávat auditní stopu, zvyšovat kybernetickou odolnost a připravit se na regulatorní požadavky.

Bezpečnost bez vlastního SOC
Pokročilé bezpečnostní funkce bez nutnosti budovat vlastní bezpečnostní centrum.

Lokální partner a evropské prostředí
Data uložená v EU, lokální podpora a transparentní přístup k datům.

Co získáte s IXTRUST

- Jistotu, že zálohy budou použitelné i po útoku
- Přehled o bezpečnostních událostech a auditní stopu
- Rychlejší obnovu provozu po incidentu
- Podporu při plnění požadavků NIS2
- Ochranu dat i logů v jednom řešení
- Lokální podporu a data uložená v EU

Pro koho je IXTRUST určen

IXTRUST je určen organizacím, které chtějí zvýšit svou kybernetickou odolnost, chránit kritická data a zajistit rychlou obnovu provozu po bezpečnostním incidentu. Největší přínos přináší tam, kde je klíčová dostupnost dat, kontinuita provozu a schopnost reagovat na rostoucí kybernetické hrozby.

Obnova z ověřeného čistého bodu, ne jen ze zálohy

Firmy si IXTRUST volí proto, že po incidentu nestačí vědět, že záloha existuje. Důležité je rychle určit, která záloha je bezpečná, použitelná a nevrátí do provozu kompromitovaná data.

- Bezpečnostní skenování záloh a detekce škodlivého obsahu.
- Identifikace čisté zálohy a čistého bodu obnovy pro bezpečnější restart provozu.
- Propojení informací ze záloh a logů pro lepší rozhodnutí, odkud obnovovat.
- Nižší riziko opětovného zavedení útoku zpět do obnoveného prostředí.

Zálohy chráněné před manipulací a neoprávněným smazáním

Útočníci se při ransomware útocích často snaží zasáhnout i zálohy, protože tím zvyšují tlak na firmu. IXTRUST pomáhá vytvořit bezpečnější zálohovací vrstvu, která je lépe chráněná proti změně, smazání nebo zneužití.

- Nesmazatelné WORM úložiště pro ochranu záloh proti manipulaci.
- Možnost šifrovaného přenosu a šifrovaného uložení dat.
- Oddělené uložení záloh mimo běžný dosah kybernetického útoku.
- Rychlá dostupnost dat pro obnovu bez zbytečných provozních překážek.

IXPERTA

Vytvořeno ve spolupráci s ECCC a ČVUT – FEL,
s podporou EU DIGITAL Europe Programme:

FAKULTA ELEKTROTECHNICKÁ ČVUT V PRAZE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Proč organizace volí IXTRUST

Logy jako základ pro rychlé rozhodování po útoku

Bez logů je obtížné pochopit, co se v prostředí stalo a jaký rozsah má incident. IXTRUST pomáhá logy bezpečně uchovávat, centralizovat a využít je při rozhodování o dalším postupu obnovy.

- Sběr a centralizace bezpečnostních logů z vybraných zdrojů.
- Detekce podezřelých aktivit, anomálií a potenciálních rizik.
- Podpora vyhodnocení časové osy incidentu a dopadu na systémy nebo účty.
- Lepší podklad pro interní reporting, auditní stopu a následná opatření.

Kybernetická odolnost bez budování vlastní infrastruktury

Ne každá organizace má kapacitu budovat vlastní bezpečnostní centrum nebo specializovanou obnovovací infrastrukturu. IXTRUST proto přináší model, který umožňuje posílit ochranu dat, logů a záloh bez velkých vstupních investic do vlastního prostředí.

- SaaS model bez nutnosti budovat a provozovat vlastní platformu.
- Bezpečně oddělené multi-tenant prostředí pro ukládání a práci se zálohami.
- Přizpůsobení rozsahu ochrany podle velikosti, rizik a priorit organizace.
- Vhodné i pro menší a střední firmy, které potřebují praktické a srozumitelné řešení.

Jedno řešení, které roste spolu s potřebami firmy

Organizace často nezačínají s ideálním stavem bezpečnosti, ale potřebují postupně posilovat ochranu podle rozpočtu, rizik a regulatorních očekávání. IXTRUST umožňuje začít bezpečným zálohováním a postupně přidávat pokročilejší ochranu záloh, logů a recovery procesů.

- Essential pro bezpečné zálohování a rychlou obnovu kritických dat.
- Advanced pro skenování záloh, identifikaci čisté zálohy a včasné odhalení hrozeb.
- Premium pro komplexnější ochranu dat, záloh a logů včetně podpory auditovatelnosti.
- Integrace na existující IT infrastrukturu, bezpečnostní zdroje a provozní systémy.

Vytvořeno ve spolupráci s ECCC a ČVUT – FEL,
s podporou EU DIGITAL Europe Programme:

www.ixperta.com

Nejčastější otázky o IXTRUST

Nestačí nám běžné zálohování?

Většina organizací dnes zálohuje data. Po kybernetickém útoku však často řeší jiný problém a to, jak poznat, zda jsou zálohy bezpečné a které z nich lze použít pro obnovu. IXTRUST kromě zálohování přidává bezpečnostní skenování záloh, ochranu logů a podporu při identifikaci bezpečného bodu obnovy.

Máme vlastní IT oddělení. Jak nám může IXTRUST pomoci?

IXTRUST nenahrazuje interní IT tým. Doplňuje jeho možnosti o pokročilé funkce v oblasti ochrany záloh, analýzy logů, detekce hrozeb a obnovy po incidentu.

Nahrazuje IXTRUST EDR nebo XDR řešení?

Ne. EDR/XDR chrání produkční prostředí a pomáhá odhalovat hrozby v reálném čase. IXTRUST se zaměřuje na ochranu záloh, uchování logů a podporu obnovy po incidentu.

Jak se IXTRUST doplňuje s našimi stávajícími bezpečnostními nástroji?

IXTRUST rozšiřuje stávající bezpečnostní řešení o bezpečné zálohování, ochranu logů, identifikaci bezpečného recovery pointu a podporu při obnově provozu po incidentu.

Jakou hodnotu nám IXTRUST přinese?

IXTRUST propojuje bezpečné zálohování, ochranu logů a bezpečnostní analýzu do jednoho řešení. Pomáhá organizacím zvýšit kybernetickou odolnost a zkrátit dobu obnovy po incidentu.

Proč je důležité zálohovat logy?

Útočníci často mažou logy jako první. Bez logů je složité zjistit průběh útoku, splnit regulatorní požadavky nebo určit bezpečný bod obnovy.

Jak IXTRUST pomáhá při ransomware útoku?

Pomáhá identifikovat bezpečný bod obnovy, ověřit stav záloh a podpořit rychlé obnovení provozu.

Pomůže nám IXTRUST s požadavky NIS2?

IXTRUST podporuje organizace v oblastech uchovávání logů, auditovatelnosti, obnovy provozu a zvyšování kybernetické odolnosti.

Jsou data uložena v Evropské unii?

Ano. Data jsou ukládána v prostředí splňujícím evropské bezpečnostní a regulatorní požadavky.

Jak náročné je nasazení?

Záleží na zvolené variantě služby. Zálohování a bezpečnostní skenování lze nasadit velmi rychle. Analýza logů vyžaduje napojení vybraných zdrojů.

Je IXTRUST vhodný i pro menší firmy?

Ano. IXTRUST byl navržen tak, aby byl dostupný i organizacím bez vlastního bezpečnostního týmu.

V čem se IXTRUST liší od běžných zálohovacích služeb?

IXTRUST přidává bezpečnostní skenování záloh, ochranu logů, analýzu bezpečnostních událostí a podporu při obnově po kybernetickém incidentu.

Jaké balíčky IXTRUST nabízí a jak se liší?

IXTRUST lze využít podle potřeb organizace v úrovních Essential, Advanced a Premium. Essential se zaměřuje na bezpečné zálohování kritických dat a rychlou dostupnost záloh pro obnovu provozu. Advanced přidává bezpečnostní skenování záloh, včasné odhalení hrozeb a identifikaci bezpečné čisté zálohy. Premium rozšiřuje ochranu o sběr a bezpečné uchování logů, propojení logů se zálohami, podporu forenzního šetření a auditovatelnost.

Vytvořeno ve spolupráci s ECCC a ČVUT – FEL,
s podporou EU DIGITAL Europe Programme:

Nejčastější otázky o IXTRUST

Co znamenají nesmazatelné zálohy a proč jsou pro firmu důležité?

Nesmazatelné zálohy jsou chráněné proti neoprávněné změně, smazání nebo manipulaci. Díky tomu má organizace vyšší jistotu, že po incidentu bude mít k dispozici použitelná data pro obnovu. IXTRUST počítá také s možností šifrování uložených dat a odděleným uložením záloh mimo přímý dosah útoku. To pomáhá snižovat riziko, že útočník poškodí i záložní kopie.

Umí IXTRUST pracovat s naší existující IT a bezpečnostní infrastrukturou?

Ano. IXTRUST je navržen jako integrační platforma, která se může napojit na vybrané zdroje logů, bezpečnostních událostí, provozních systémů i zálohovacích nástrojů. Cílem je centralizovat důležitá bezpečnostní data pro analýzu, reporting a rozhodování při obnově. Organizace tak nemusí začínat od nuly, ale může rozšířit stávající prostředí o ochranu záloh, logů a recovery procesů.

Jak IXTRUST pomáhá odhalovat skryté nebo dlouhodobě přítomné hrozby?

IXTRUST průběžně analyzuje logy, bezpečnostní události a zálohy, aby pomohl identifikovat anomálie a podezřelé aktivity. Díky propojení detekce hrozeb se zálohami může lépe určit, zda je konkrétní záloha vhodná pro bezpečnou obnovu. AI vrstva podporuje analýzu událostí, prediktivní identifikaci rizik a práci se znalostní bází hrozeb. To je užitečné zejména u útoků, které v prostředí probíhají delší dobu bez okamžitého odhalení.

Jak IXTRUST podporuje forenzní analýzu a rozhodování po incidentu?

IXTRUST bezpečně uchovává kritické logy a pomáhá sestavit časovou osu kybernetického útoku. Díky analýze logů lze lépe identifikovat podezřelé aktivity, zasažené systémy, účty a možný průběh incidentu. Tyto informace podporují rozhodnutí, který recovery point je bezpečný a jaký postup obnovy zvolit. Současně pomáhají organizaci při auditu, vyšetřování incidentu a plnění interních bezpečnostních politik.

Jak poznáme, že je IXTRUST vhodný právě pro naši organizaci?

IXTRUST dává největší smysl tam, kde jsou pro provoz klíčová data, zálohy a schopnost rychle se vrátit do bezpečného stavu. Je vhodný pro organizace, které nechtějí řešit pouze to, zda záloha existuje, ale také zda je čistá, použitelná a dohledatelná. Typickým signálem potřeby je požadavek na vyšší kybernetickou odolnost, auditovatelnost a jasný postup obnovy po incidentu. Řešení lze přizpůsobit od základní ochrany dat až po pokročilou analýzu logů a podporu forenzního šetření.

Pomůže nám IXTRUST určit RTO a RPO pro obnovu provozu? RTO znamená maximálny akceptovateľný čas výpadku RPO znamená maximálne akceptovateľnú stratu dát vyjadrenú v čase.

Ano, IXTRUST podporuje praktické nastavení recovery procesů, ve kterých se řeší dostupnost záloh, čistý bod obnovy a priorita obnovovaných systémů. RTO pomáhá určit, jak rychle se má organizace vrátit do provozu, zatímco RPO řeší, jak velká ztráta dat je ještě přijatelná. Díky propojení záloh, logů a analýzy incidentu lze lépe rozhodnout, odkud obnovovat a jak minimalizovat dopad výpadku. IXTRUST tak pomáhá převést obecný plán obnovy do konkrétnějšího a ověřitelnějšího postupu.

Dokáže IXTRUST ověřit, že záloha je opravdu použitelná pro obnovu?

IXTRUST se nezaměřuje jen na samotné uložení záloh, ale také na jejich bezpečnostní ověřování a identifikaci čisté zálohy. To je důležité zejména u útoků, které mohly v prostředí probíhat delší dobu ještě před odhalením. Analýza záloh a logů pomáhá snížit riziko, že organizace obnoví data zpět do kompromitovaného stavu. Výsledkem je vyšší jistota, že vybraný recovery point je pro obnovu bezpečnější a obchodně použitelný.

Vytvořeno ve spolupráci s ECCC a ČVUT – FEL,
s podporou EU DIGITAL Europe Programme: