FREEDIVISION

4. 11. 2026 · Enforum, Praha-Karlín

FREEDIVISION SECURITY DAY 2026 · 11:50

FD.io Data

Víte, kde leží vaše citlivá data a kdo k nim má přístup?

powered by VARONIS



Jakub Karvánek
CSO, FreeDivision

11:00 PhishingGym | 11:20 VulnerAbility | **11:50 FD.io Data** | 12:30 FD.io Risk

KDO JE VARONIS

Lídr datové bezpečnosti podle analytiků i zákazníků

Gartner Peer Insights

Customers' Choice pro Data Security Posture Management, třetí rok po sobě

Forrester Wave 2025

Leader v kategorii Data Security Platforms

G2 · jaro 2026

Leader v kategorii DSPM podle hodnocení uživatelů

8 000+ zákazníků ve všech odvětvích

90 %+ zákazníků zůstává

VRNS kótovaná na burze Nasdaq

VJ

VARONIS AMBASSADOR

NÁŠ VARONIS AMBASADOR

Viktor Jahna

Jeden z nejlepších specialistů na Varonis v Evropě.

Celosvětově jediný partner
s plnou autonomií od Varonisu

Exkluzivita
pro Českou republiku a Slovensko

VŠECHNY SLUŽBY U NÁS, BEZ ČEKÁNÍ NA VÝROBCE

- Školení
- Implementace
- Health checky
- Eskalace problémů
- Zadávání feature requestů

I po konci on-prem verze běží v ČR **3 on-prem instalace až do konce roku 2027**. Díky našemu partnerství a Viktorovi.

PROČ ŘEŠIT DATA

EDR, firewall i SIEM chrání cestu. Útočník ale jde vždycky po datech.

Víc dat na víc místech

Souborové servery, Microsoft 365, cloud, SaaS aplikace. Dat přibývá rychleji, než je kdokoli stihne roztřídit.

Přístupy, které nikdo nehlídá

Sdílení „pro všechny“, zděděná oprávnění, staré účty. Každý účet vidí víc, než pro svou práci potřebuje.

Útočníci se přihlašují

S ukradeným heslem se nikam nevlamují. Prostě se přihlásí a mají přístup ke všemu, co vidí uživatel.

CO VŠECHNO UMÍME PŘIPOJIT

- Souborové servery, NAS, databáze
- Microsoft 365
- AWS, Azure, Google Cloud
- Google Workspace, Salesforce, Box, GitHub
- Active Directory, Entra ID, Okta

Kolik dat otevře jeden ukradený účet?

CO DNES VARONIS ŘEŠÍ

Jedna platforma, čtyři oblasti. Dnes se zaměříme na dvě.

Dnes

Data Security Platform

Data Access Governance

DSPM, oprávnění, klasifikace, DLP, detekce hrozeb nad daty

Dnes

Interceptor

E-mailová a prohlížečová ochrana proti phishingu a BEC

Na vyžádání

Atlas

Bezpečnost AI: inventář, posture, guardrails, AI compliance

Na vyžádání

Next-gen DAM

Monitoring aktivit v databázích, bez agentů

Copilot, ChatGPT i AI agenti vidí všechno, k čemu má uživatel práva. **Bezpečná AI proto začíná u dat.**

PURVIEW, DLP A KLASIFIKAČNÍ NÁSTROJE

Klasické projekty se táhnou měsíce. Varonis začne pracovat hned po instalaci.

	START	6 MĚSÍCŮ	12 MĚSÍCŮ	18 MĚSÍCŮ
Klasický přístup Purview, DLP, klasifikace, DSPM	Skeny klasifikace nikdy nedoběhly	Štítky chybějí nebo jsou špatně	Citlivá data našli, opravit nešlo nic	Tisíce tiketů, útoky na data nikdo nevidí
FD.io Data powered by Varonis	**1. hodina:** první rizika **1. –2. týden:** 99 % citlivých dat označeno a opraveno	**Dál už jen automaticky opravuje a 24×7 hlídá. Bez tiketů, bez ruční práce.**		

> *„18 měsíců jsme se trápili jen s klasifikací dat. Bez měřitelného výsledku.“*
>
> CISO globální finanční firmy, podle podkladů Varonis

FD.IO DATA · DATA SECURITY PLATFORM

Najít, opravit, hlídat. Automaticky.

SaaS | Rychlé nasazení | AI-native klasifikace

NAJÍT

Viditelnost v reálném čase

- Kde leží citlivá data: osobní údaje, karty, hesla
- Kdo k nim má přístup a kdo je opravdu používá
- Co je sdílené veřejně nebo pro celou firmu

OPRAVIT

Automatická náprava

- Odebere nadbytečná oprávnění bez rozbití provozu
- Opraví chybné konfigurace a označí data štítky
- Vypne neaktivní účty, archivuje stará data

HLÍDAT (ALERTY)

Detekce nad daty

- UEBA zaměřená na data a identity
- Ransomware, exfiltrace, zneužitý účet
- 24×7 MDDR: analytici Varonis reagují za vás

24×7 MDDR · PŘÍKLAD Z PROVOZU

Z miliardy událostí jedna skutečná hrozba

966 mil.
událostí nad daty

8 951
alertů analyzovaných týmem

7
eskalovaných zákazníkovi

1
potvrzená hrozba

5 minut medián reakce

860 hodin práce SOC ušetřeno

02

ČÁST 2 · INTERCEPTOR

E-mail Security

Většina ukradených hesel přichází e-mailem

INTERCEPTOR · E-MAILOVÁ BEZPEČNOST

Phishing, který dnes projde přes bránu

- ⚠ BEC bez odkazu a přílohy
- ⚠ Phishing z napadené schránky
- ⚠ Důvěryhodní odesílatelé a weby
- ⚠ QR kódy a útoky přes dodavatele

Vision model
OCR, QR kódy, vzhled e-mailu a stránky

Language model
Rozpozná BEC čistě z textu zprávy

Behavior model
Graf vztahů a styl komunikace

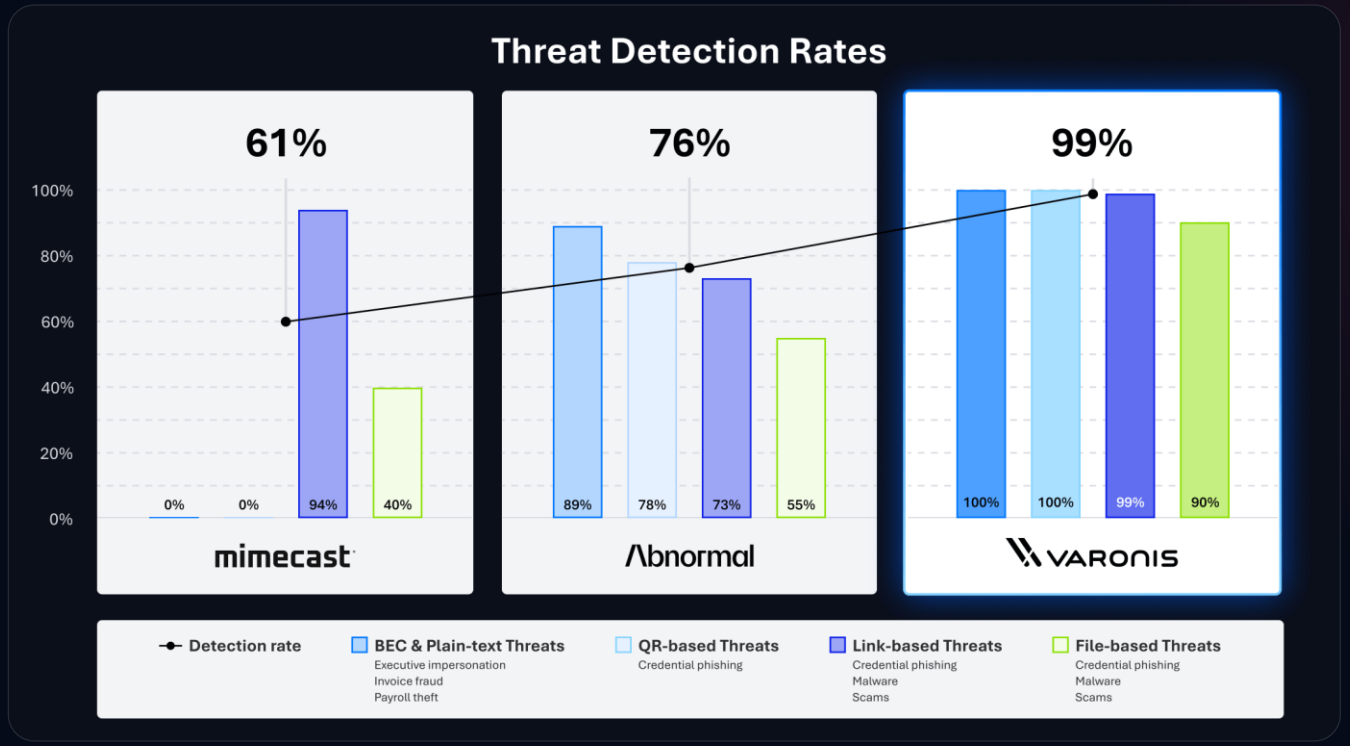
Phishing sandbox
100M+ URL denně, chová se jako uživatel

Napojení přes API za 5 minut
Bez změny MX záznamů, doplní stávající ochranu

Pro firmy od 500 schránek
Ochrana e-mailu i prohlížeče

NEZÁVISLÝ TEST · TOLLY GROUP

Zachytí to, co ostatní propustí



99 %

celková přesnost detekce

100 %

útoků přes BEC a QR kódy

3×

víc detekcí než nejbližší AI konkurent

Zdroj: Tolly Group, podklady Varonis

INTERCEPTOR · TEST NA VAŠÍ POŠTĚ

V testu se podíváme až 3 měsíce zpátky

1

Připojení přes API

Pár minut, bez zásahu do toku pošty

2

Zpětná analýza

Pošta až 3 měsíce do minulosti

3

Kudy to prošlo

Přes jakou ochranu a jakou technikou prošel phishing i malware

4

Co pořád leží ve schránkách

Škodlivé zprávy v legitimních schránkách uživatelů

Na konci máte srovnání se stávající ochranou na vlastní poště, ne na cizím testu.

ČÁST 3 · POC

Data Risk Assessment

03

Jak si to vyzkoušet na vlastních datech

Řekněte si v pauze, po akci, nebo na **jakub.karvanek@freedivision.com**

ZDARMA

PRO ÚČASTNÍKY AKCE

DATA RISK ASSESSMENT

Pár hodin práce na vaší straně. Výstupy k nezaplacení.

2–4 h

Příprava prostředí

Servisní účty, přístupy, síť

2–4 h

Instalace

SaaS, připojení datových zdrojů

Analýza

Sběr a vyhodnocení

Data, oprávnění a aktivity běží samy

2×

Workshop

Nálezy, doporučení a plán, jak je vyřešíme

Výstupy zůstávají vám, ať se rozhodnete pokračovat, nebo ne.

DATA RISK ASSESSMENT · 2 WORKSHOPY

Neukážeme jen problémy. Ukážeme, jak je vyřešíme.

Co jsme našli

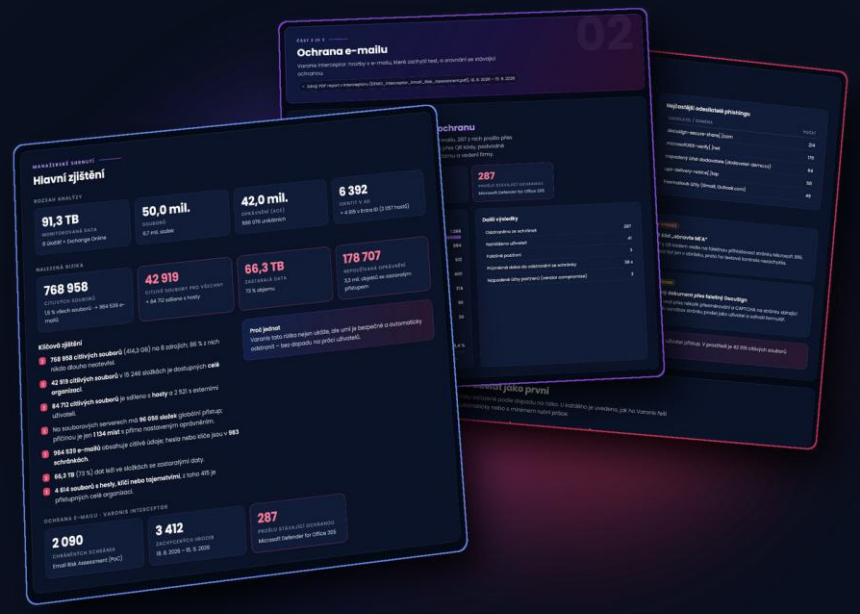
- ✓ Školení a ukázka platformy na vašich datech
- ✓ Nálezy seřazené podle rizika
- ✓ Doporučení pro každý nález

Jak to vyřešíme

- ✓ Jízdní řád celého nasazení
- ✓ Automatizace a odstranění nálezů
- ✓ Audity, compliance a klasifikace dat

Odcházíte s konkrétním plánem, ne jen se seznamem problémů.

Co ve zprávě najdete



768 958
citlivých souborů, 86 % nikdo dlouho neotevřel

42 919
citlivých souborů vidí celá organizace

96 056
složek s globálním přístupem, příčinou jen 1 134 míst

66,3 TB
zastaralých dat, 73 % celého objemu

27 550
citlivých složek otevřených firmě nebo hostům, i pro Copilot

287
hrozeb prošlo přes Defender, z 3 412 zachycených



ZPRÁVA · STR. 2

Celý stav na jedné stránce pro vedení

91,3 TB
analyzovaných dat, 50 mil. souborů, 42 mil. oprávnění

4 hlavní rizika
citlivá data, přístup pro všechny, zastaralá data, nepoužívaná oprávnění

7 zjištění
srozumitelně, bez technického žargonu



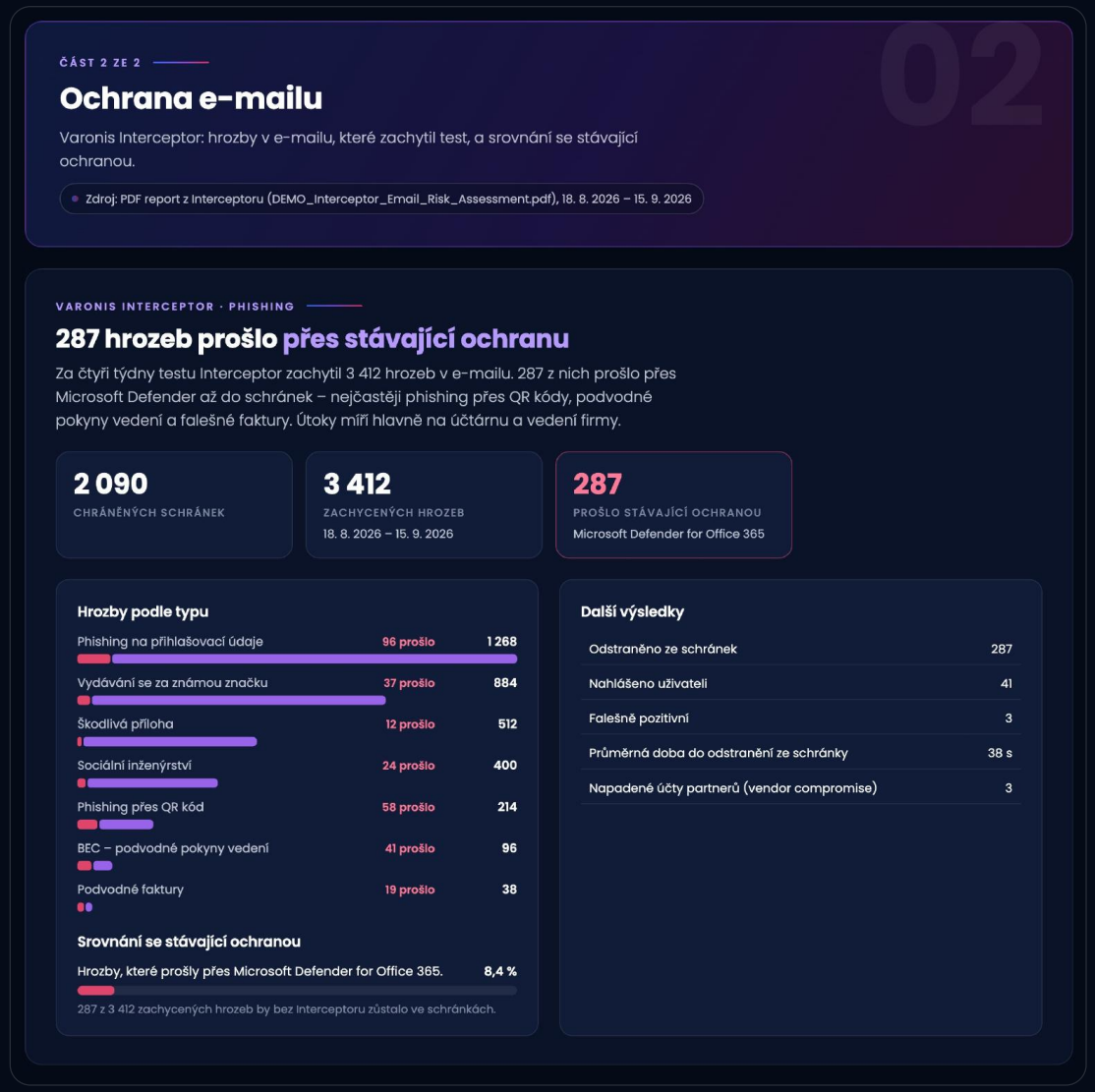
ZPRÁVA · OPRÁVNĚNÍ

96 056 složek otevřených celé firmě

1 134 míst
stačí opravit, ne 96 tisíc složek

15 937
složek, kam může zapisovat každý

8 352
složek s oprávněním pro smazané účty



ZPRÁVA · E-MAIL

287 hrozeb prošlo přes Microsoft Defender

3 412
zachycených hrozeb za 4 týdny na 2 090 schránkách

58 z 214
phishingů přes QR kód prošlo až do schránek

38 s
průměrná doba do odstranění ze schránky



VARONIS INTERCEPTOR · CÍLE A DOPAD

Kdo je cílem a co by útoky stály

Nejčastěji napadení příjemci

PŘÍJEMCE	POČET
Účtárna (sdílená schránka)	312
Finanční ředitel	188
Recepce	143
HR – nábor	121
Generální ředitel	97

Nejčastější odesílatelé phishingu

ODESÍLATEL / DOMÉNA	POČET
docusign-secure-share[.]com	214
microsoft365-verify[.]net	176
napadený účet dodavatele (dodavatel-demo.cz)	64
ups-delivery-notice[.]top	58
freemailové účty (Gmail, Outlook.com)	49

Příklady zachycených útoků

KRITICKÉ
Změna účtu pro platbu faktury
E-mail z napadené schránky skutečného dodavatele navazoval na existující konverzaci a žádal o úhradu na nový bankovní účet. Bez odkazu i přílohy prošel přes stávající filtr.

VYSOKÉ
QR kód „obnovte MFA"
PDF s QR kódem vedlo na falešnou přihlašovací stránku Microsoft 365. Odkaz byl jen v obrázku, proto ho textová kontrola nezachytila.

VYSOKÉ
Pokyn generálního ředitele k nákupu dárkových karet
Krátká zpráva z freemailové adresy s podpisem ředitele cílila na asistentku. Interceptor ji označil podle neobvyklého vztahu odesílatele a příjemce.

STŘEDNÍ
Sdílený dokument přes falešný DocuSign
Odkaz vedl přes několik přesměrování a CAPTCHA na stránku sbírající hesla. AI sandbox stránku prošel jako uživatel a odhalil formulář.

Souvislost s daty: úspěšný phishing dává útočníkovi všechno, k čemu má napadený uživatel přístup. V prostředí je 42 919 citlivých souborů dostupných celé organizaci – tedy i každému napadenému účtu.

DOPORUČENÉ POSTUPY

Co udělat jako první

Kroky seřazené podle dopadu na riziko. U každého je uvedeno, jak ho Varonis řeší automaticky nebo s minimem ruční práce.

Část 1 · Ochrana dat (Varonis Data Security Platform)

1 **Odebrat přístup celé organizace k citlivým datům** KRITICKÉ
42 919 citlivých souborů v 15 246 složkách je dostupných celé organizaci (nejvíc freedivision-my.sharepoint.com, FreeDivision.fileserver01, freedivision.sharepoint.com).
Varonis: Automatická remediace nahradí globální skupiny a odkazy přístupem pro skutečné uživatele podle záznamů o přístupu.

2 **Prověřit soubory s hesly a klíči** KRITICKÉ
4 614 souborů obsahuje přihlašovací údaje, privátní klíče nebo tajemství; 415 je přístupných celé organizaci.
Varonis: Hlídání přístupu k těmto souborům a upozornění při neobvyklém čtení.

3 **Uklidit Active Directory** KRITICKÉ
Administrátorské účty s SPN (1), dlouho neměněné heslo účtu krbtgt (1), 747 aktivních nepoužívaných účtů, 381 aktivních účtů s neexpirujícím heslem, 19 účtů s delegací, 1 účet bez Kerberos pre-autentizace, členové Schema Admins, 53 počítačů s rizikovým OS.
Varonis: Průběžné kontroly konfigurace AD a upozornění na změny v privilegovaných skupinách.

ZPRÁVA · DOPORUČENÉ POSTUPY

17 kroků seřazených podle rizika

Kritické **Vysoké** **Střední** **Nízké**

U každého kroku: co, kde a kolik

Konkrétní složky, účty a schránky

A jak to Varonis vyřeší

Automaticky, nebo s minimem ruční práce

Na workshopu z toho uděláme plán nápravy a jízdní řád.

ŽIVÁ UKÁZKA · RYCHLÝ PRŮLET

Pojďme do konzole

≈ 15 minut

Sedm oblastí, jedna platforma. Naživo v demo prostředí Varonis.

1

Události

Kdo co otevřel, změnil a smazal

2

Oprávnění

Kdo k čemu má přístup a odkud ho má

3

Klasifikace

Kde leží osobní údaje, karty a hesla

4

Microsoft 365

Sdílení s hosty, Teams a OneDrive

5

Alerty

Podezřelé chování a ransomware včas

6

Compliance

GDPR, ISO 27001 a NIST na jednom místě

7

Automatizace

Náprava oprávnění bez ruční práce

Na vašich datech?

Data Risk Assessment zdarma