RICOH
imagine. change.


# RICOH RansomCare

## Zastavte ransomware, než se rozšíří !

**Radek Nebeský**
Cyber Security Consultant

RICOH
imagine. change.

# 01 Hrozba jménem ransomware

Postřehy a názory, proč potřebujete další vrstvu zabezpečení před ransomware

# Hrozba jménem ransomware

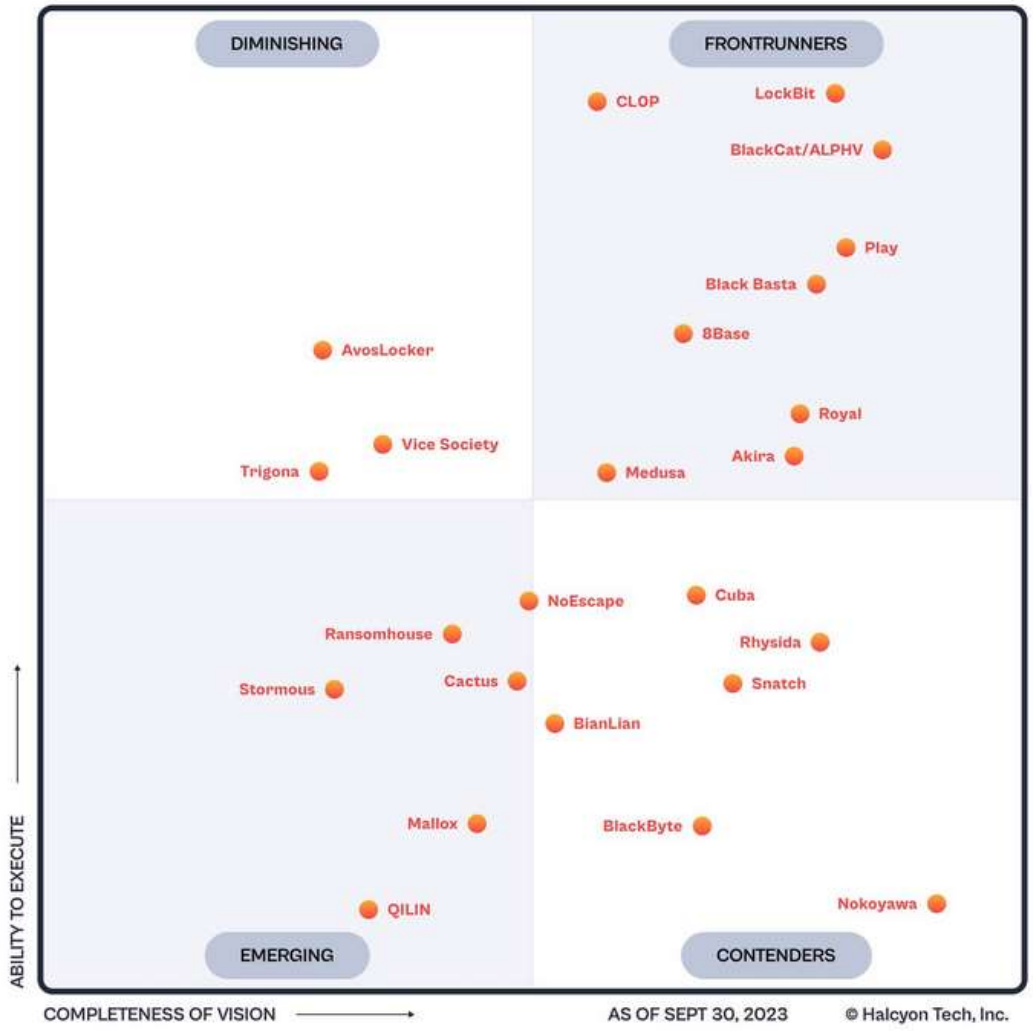
RICOH
imagine. change.


**4**
**útoky**
za minutu


**734**
**útoků**
za minutu

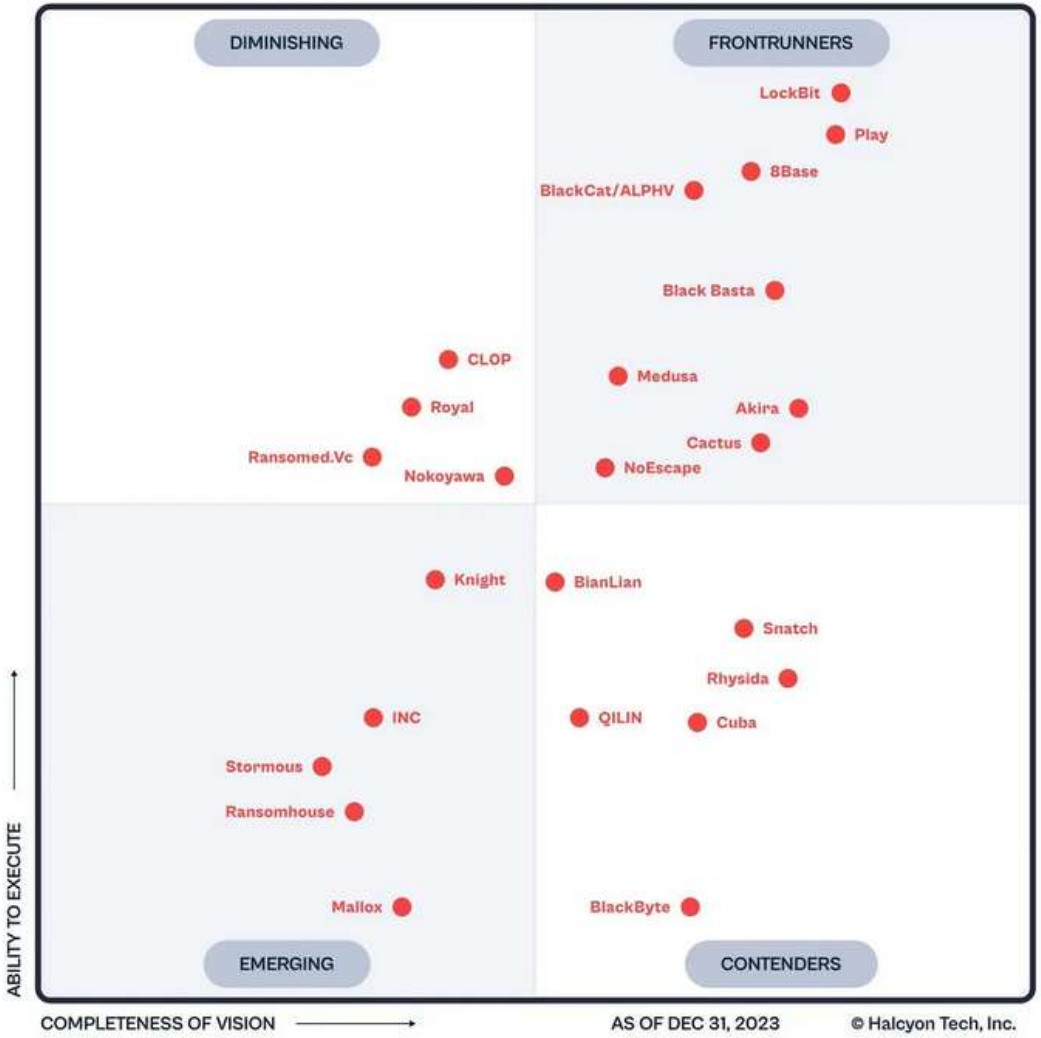
# Hrozba jménem ransomware …

Figure 1: Top Threat Groups for Ransomware-as-a-Service Ecosystem




Source: Halcyon (Q3 2023)

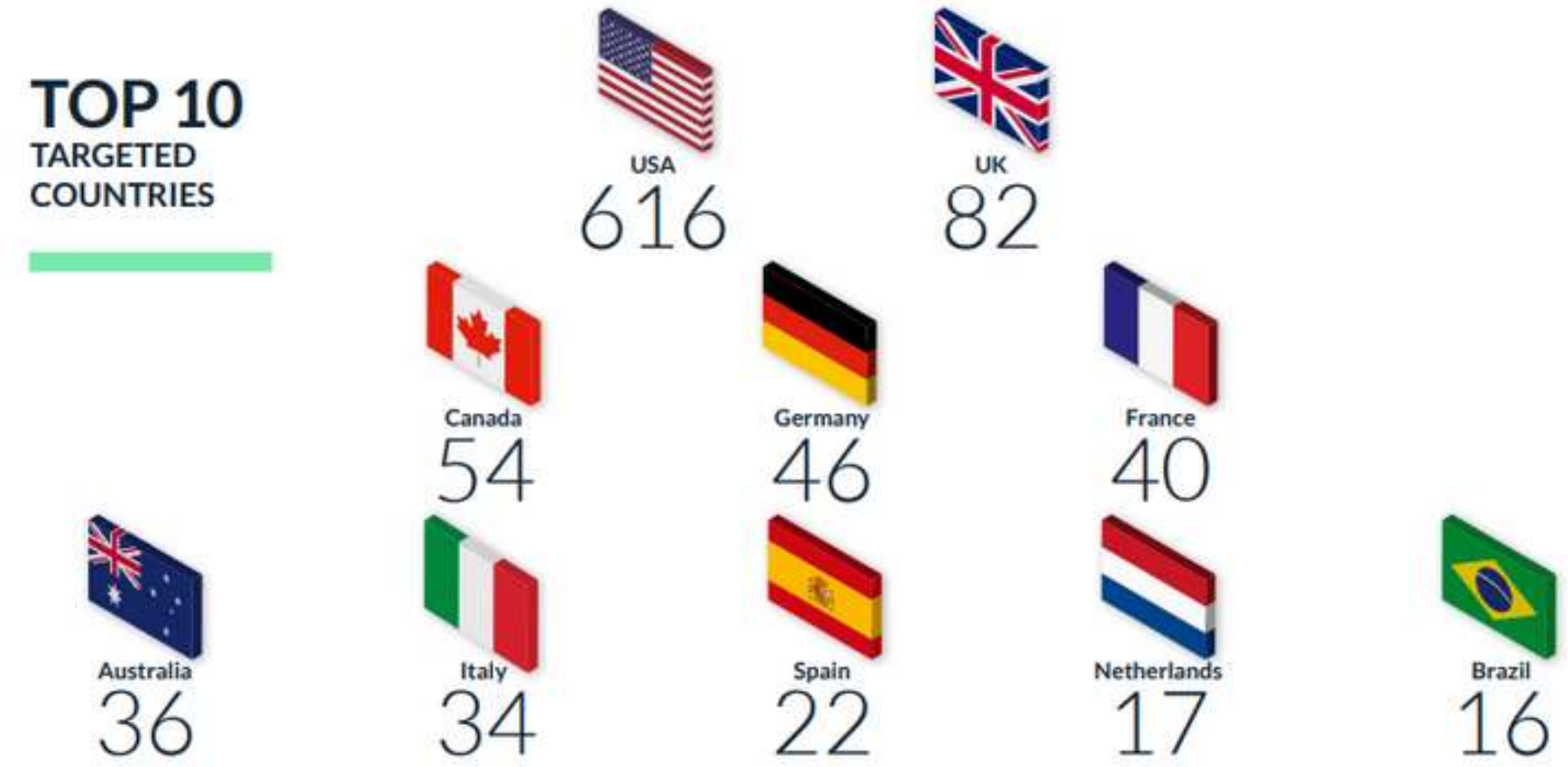
Figure 1: Top Threat Groups for Ransomware-as-a-Service Ecosystem




Source: Halcyon (Q4 2023)

# Hrozba jménem ransomware … JUNK GUN

# Hrozba jménem ransomware …




*https://cyberint.com/blog/research... Top Countries Targeted By Ransomware in Q3 2023*

# Ochrana proti ransomware …


**ZADRŽENÍ PROBÍHAJÍCÍHO ÚTOKU**

Rychlé zastavení nebezpečného šifrování

# 02 RICOH RansomCare

Jak zabezpečit své pracoviště pomocí řešení RICOH RansomCare?

# RICOH RansomCare - jak to vzniklo?

založena společnost Bullwall Dánsko — 2015

RICOH a Bullwall v Evropě — 2018

Launch CZ&SK — 11 2022

první objednávky RICOH RansomCare v CZ&SK — 8 2023

# Cyber Kill Chain – kde je RansomCare?

RICOH
imagine. change.

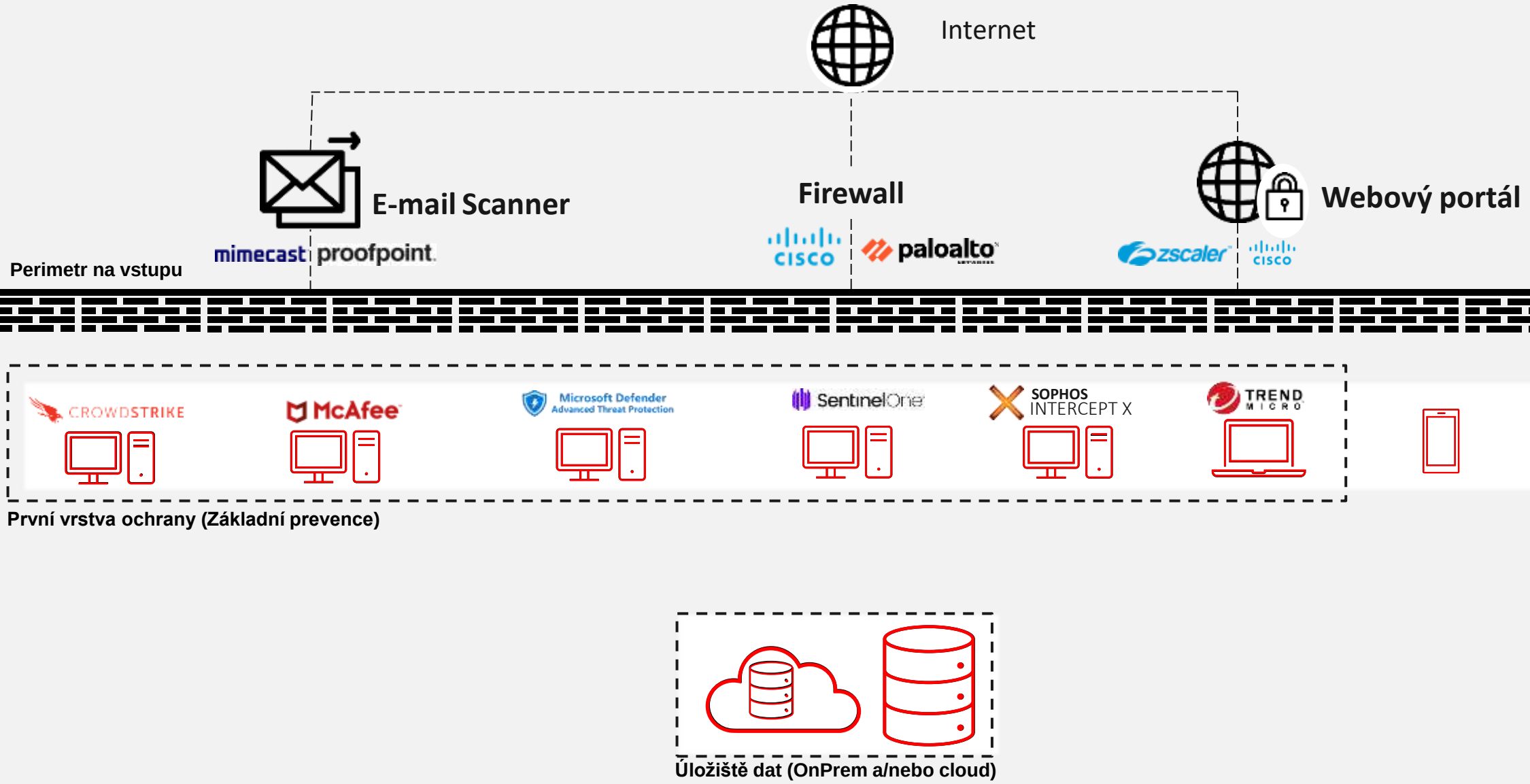
**Přípravná fáze** — hodiny až měsíce

**Fáze infiltrace** — vteřiny

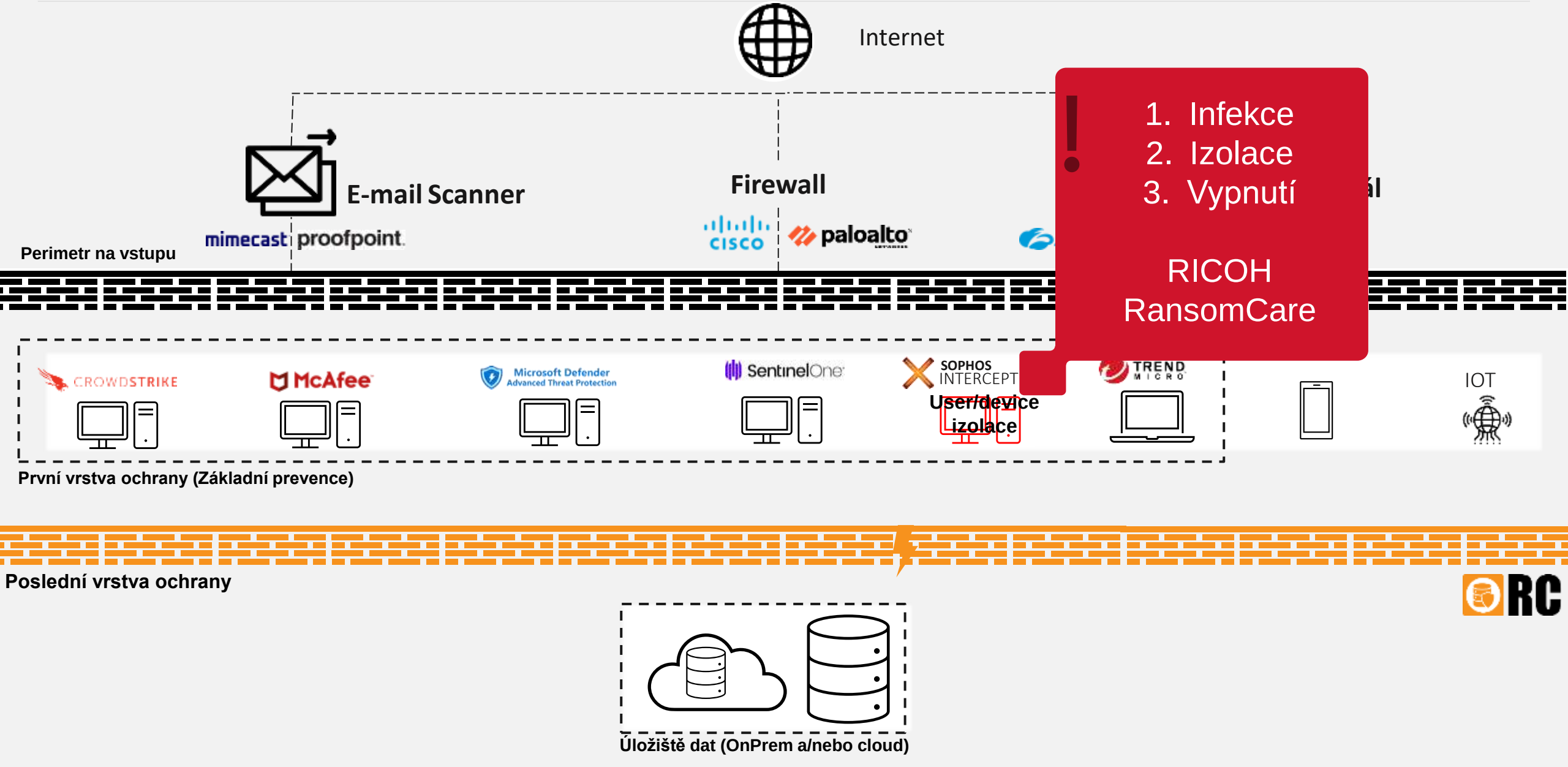
**Fáze útoku** — měsíce

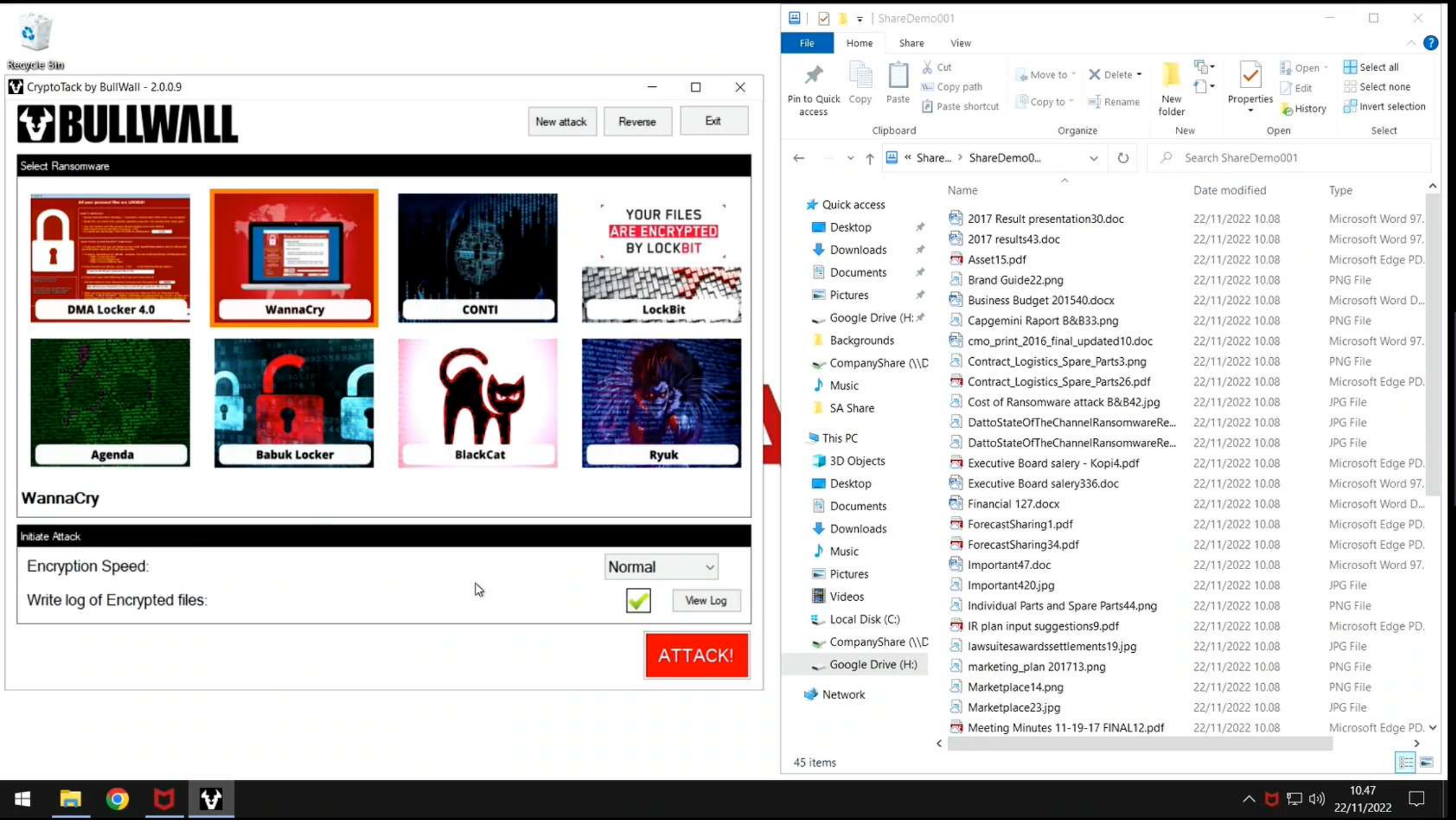
- ex-filtrace dat,
- narušení systému,
- spuštění ransomware,
- jiná škodlivá akce.


# Simulace útoku BEZ RansomCare

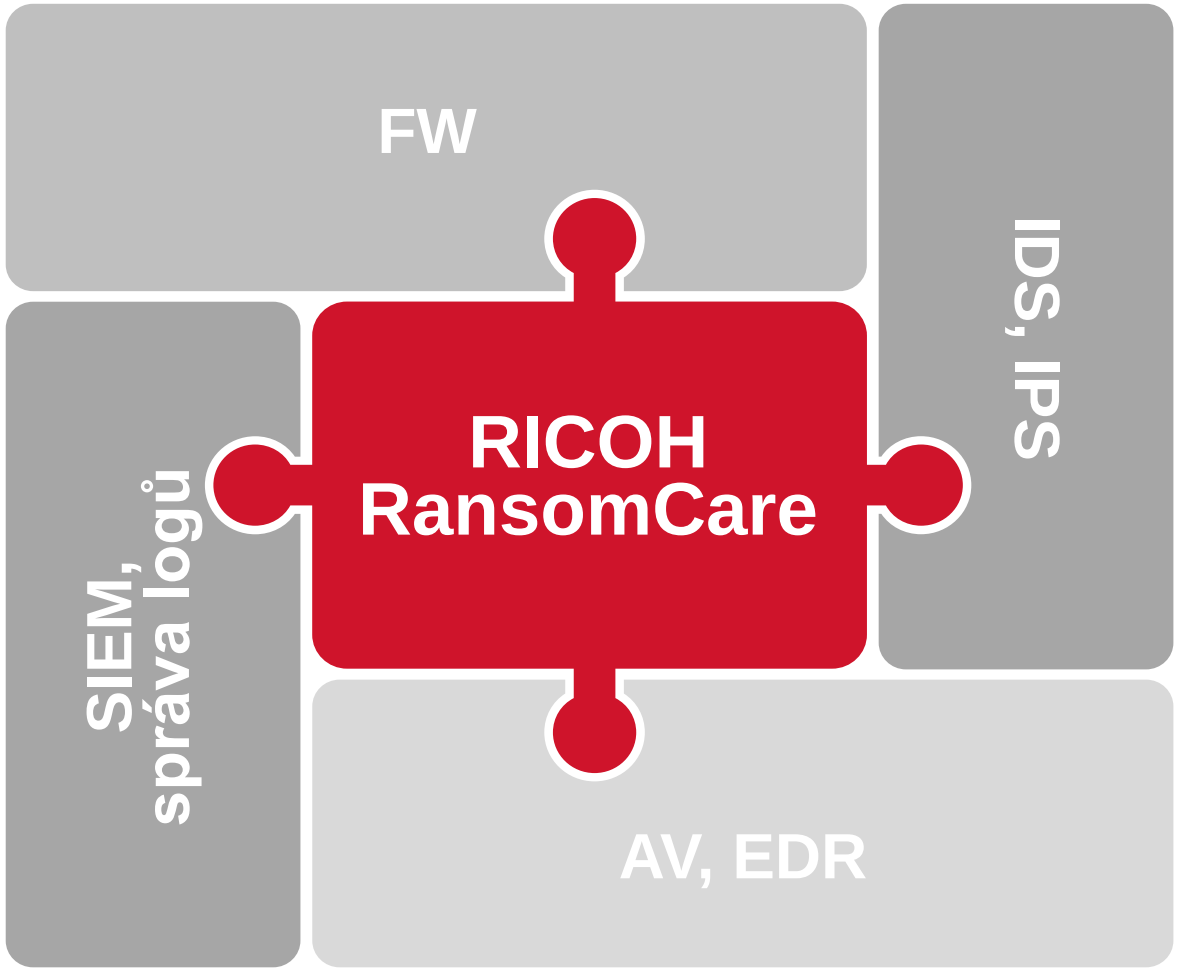


# RICOH RansomCare - další bezpečnostní vrstva !




Recycle Bin
CryptoTack by BullWall - 2.0.0.9
BULLWALL
New attack
Reverse
Exit
Select Ransomware
DMA Locker 4.0
WannaCry
CONTI
YOUR FILES ARE ENCRYPTED BY LOCKBIT
LockBit
Agenda
Babuk Locker
BlackCat
Ryuk
WannaCry
Initiate Attack
Encryption Speed:
Normal
Write log of Encrypted files:
View Log
ATTACK!
ShareDemo001
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Move to
Delete
Copy to
Rename
New folder
Properties
Open
Edit
History
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
Share... › ShareDemo0...
Search ShareDemo001
Quick access
Desktop
Downloads
Documents
Pictures
Google Drive (H:
Backgrounds
CompanyShare (\\C
Music
SA Share
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CompanyShare (\\C
Google Drive (H:)
Network
Name
Date modified
Type
2017 Result presentation30.doc 22/11/2022 10.08 Microsoft Word 97.
2017 results43.doc 22/11/2022 10.08 Microsoft Word 97.
Asset15.pdf 22/11/2022 10.08 Microsoft Edge PD.
Brand Guide22.png 22/11/2022 10.08 PNG File
Business Budget 201540.docx 22/11/2022 10.08 Microsoft Word D...
Capgemini Raport B&B33.png 22/11/2022 10.08 PNG File
cmo_print_2016_final_updated10.doc 22/11/2022 10.08 Microsoft Word 97.
Contract_Logistics_Spare_Parts3.png 22/11/2022 10.08 PNG File
Contract_Logistics_Spare_Parts26.pdf 22/11/2022 10.08 Microsoft Edge PD.
Cost of Ransomware attack B&B42.jpg 22/11/2022 10.08 JPG File
DattoStateOfTheChannelRansomwareRe... 22/11/2022 10.08 JPG File
DattoStateOfTheChannelRansomwareRe... 22/11/2022 10.08 JPG File
Executive Board salery - Kopi4.pdf 22/11/2022 10.08 Microsoft Edge PD.
Executive Board salery336.doc 22/11/2022 10.08 Microsoft Word 97.
Financial 127.docx 22/11/2022 10.08 Microsoft Word D...
ForecastSharing1.pdf 22/11/2022 10.08 Microsoft Edge PD.
ForecastSharing34.pdf 22/11/2022 10.08 Microsoft Edge PD.
Important47.doc 22/11/2022 10.08 Microsoft Word 97.
Important420.jpg 22/11/2022 10.08 JPG File
Individual Parts and Spare Parts44.png 22/11/2022 10.08 PNG File
IR plan input suggestions9.pdf 22/11/2022 10.08 Microsoft Edge PD.
lawsuitesawardssettlements19.jpg 22/11/2022 10.08 JPG File
marketing_plan 201713.png 22/11/2022 10.08 PNG File
Marketplace14.png 22/11/2022 10.08 PNG File
Marketplace23.jpg 22/11/2022 10.08 JPG File
Meeting Minutes 11-19-17 FINAL12.pdf 22/11/2022 10.08 Microsoft Edge PD.
45 items
Scott Anderson
10.47
22/11/2022

# RICOH RansomCare




RICOH RansomCare není náhrada, ale **doplněk**

# Spolupracujeme

RICOH
imagine. change.

RICOH
imagine. change.

# 03 Jak začít ?

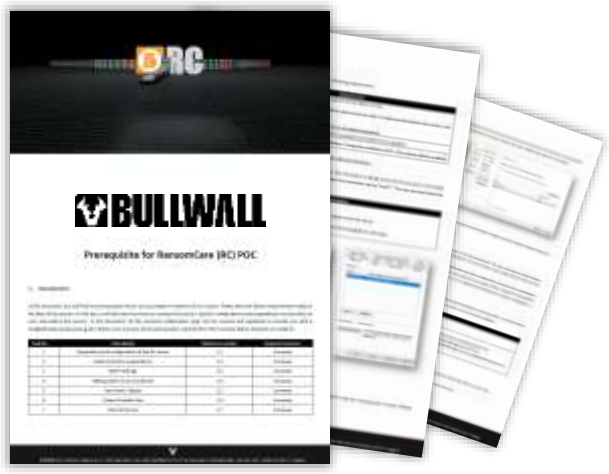
Hodnotící test (PoC) ve vašem prostředí

# Hodnotící test Ransomware – PoC (Proof of Concept)

RICOH
imagine. change.

## Krok 1

- 30 minut
- Příprava prostředí
- Příprava monitorovaných zón




## Krok 2

- Jak bude vaše síť reagovat?
- Vyzkoušejte si RC ve svém prostředí
- Bude vaše stávající zabezpečení reagovat?


## Krok 3

- Více než 1.000 provedených PoC
- Report z PoC
- Poznejte svou odolnost vůči šifrovacímu útoku

# 04 Jak probíhá instalace?

Průběh instalace

# Jak probíhá instalace?

**KICK OFF**

**INSTALACE - TEAMS**
2-4 hodiny

**MACHINE LEARNING**
4-6 týdnů

**GO TO LIVE**

1 2 3 4

# 05 Jak to pokračuje?

Prodeje řešení RICOH RansomCare

# Jak to pokračuje?

RICOH
imagine. change.

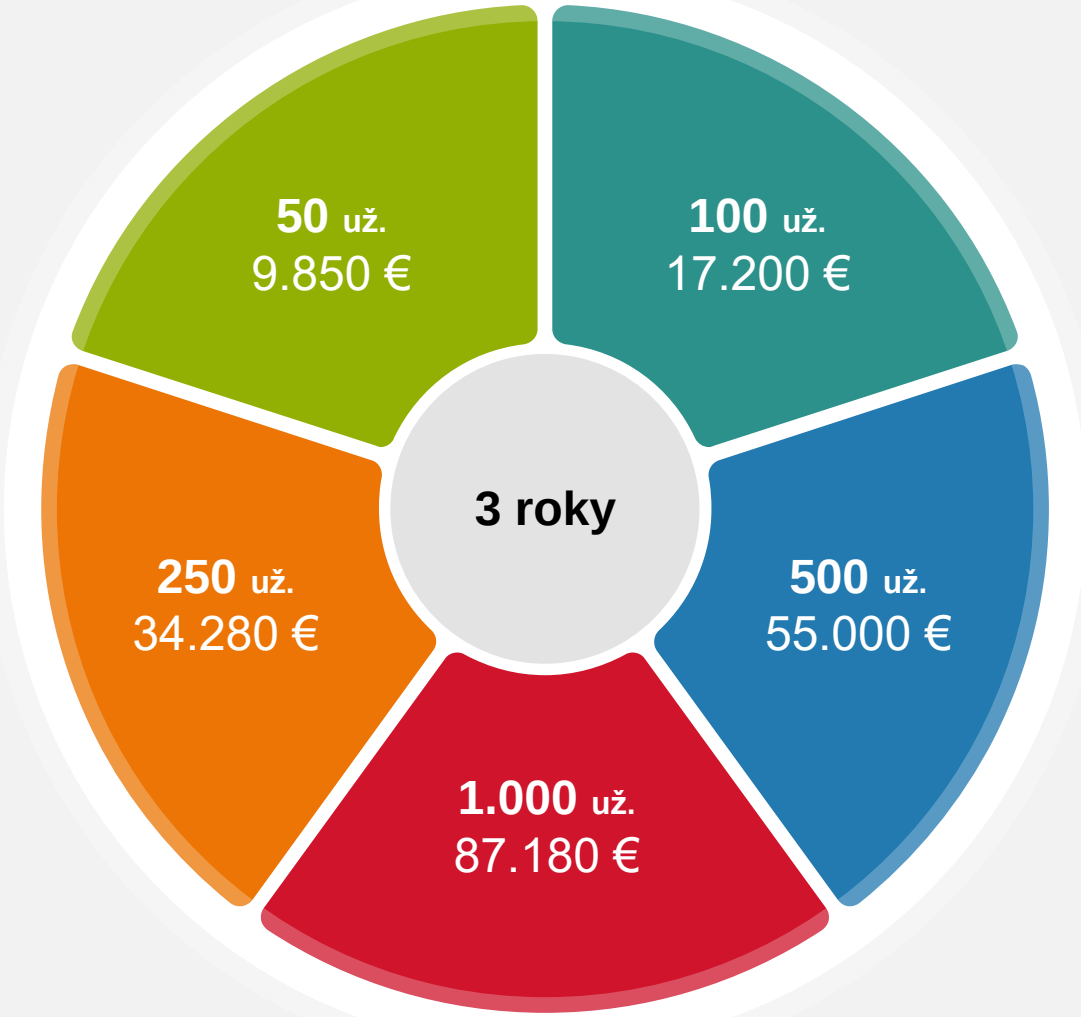

Rakovník

VZÚ
PLZEŇ

# 06 Kategorizace cen

Ceny dle počtu uživatelů v AD

# Kategorizace cen

RICOH
imagine. change.

# Dotazy?

**Radek Nebeský**
Cyber Security Consultant
radek.nebesky@ricoh.cz
607 050 887