
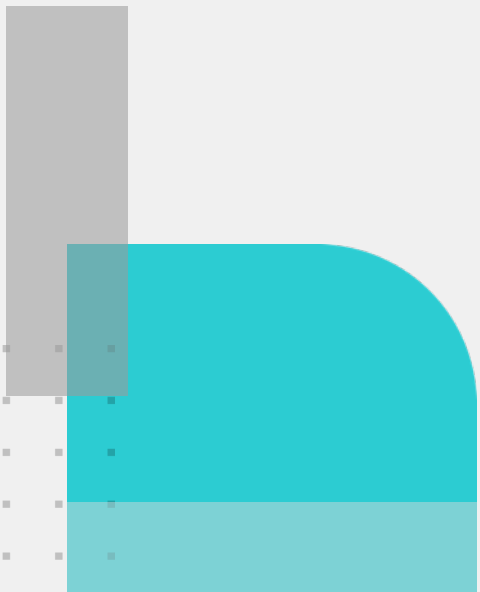





FORTINET®

**Splňuje vaše zabezpečení
emailové komunikace ochranné
opatření NÚKIB?**



Jak spolu komunikují emailové servery?

SMTP

Simple Mail Transfer Protocol



Byla emailová komunikace navržena jako bezpečná?

```
• S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.com
S: 250 smtp.example.com, I am glad to meet
you
C: MAIL FROM:bob@example.com
S: 250 Ok
C: RCPT TO:alice@example.com
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" bob@example.com
C: To: Alice Example alice@example.com
C: Date: Tue, 29 Jan 2024 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test.
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```



Ochranné opatření NÚKIB

Ochranné opatření



Metodika



https://nukib.gov.cz/download/uredni_deska/2021-10-08_OchranneOpatreni_final.pdf
https://nukib.gov.cz/download/uredni_deska/2021-10-08_Metodika_final.pdf

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

Koho se týká?

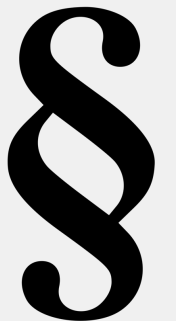
Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti (č. 181/2014 Sb)

c) správce a provozovatel informačního systému kritické informační infrastruktury,

d) správce a provozovatel komunikačního systému kritické informační infrastruktury,

e) správce a provozovatel významného informačního systému,

f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),



Co se po nás chce?

Šifrování (STARTTLS)

SPF (Sender Policy Framework)

DKIM (DomainKeys Identified Mail)

DMARC (Domain-based Message Authentication Reporting and Conformance)

DANE (DNS-based Authentication of Named Entities)



Jak zjistím, zda splňuji požadavky?

Bez odpovědi na email



S odpovědí na email
















<https://internet.nl/test-mail/>
<https://mecsa.jrc.ec.europa.eu/en/>



Jak nám může pomoci Fortinet?















Secure Networking



- | | | |
|--|---|---|
|  FortiGate Firewall |  FortiSwitch Switching |  FortiAIOps AI For Networking |
|  FortiGate VM Virtual Firewall |  FortiAP Access Point |  FortiNAC NAC |
|  FortiCNF Cloud-native Firewall |  FortiSwitch Rugged Switch |  FortiExtender LTE/5G |
|  FortiSASE Firewall-aaS |  FortiAP Rugged AP |  FortiExtender Rugged Extender |
|  FortiGate Rugged NGFW | | |













Universal SASE



- | | | | |
|--|---|---|--|
|  FortiSASE SSE |  FortiClient ZTNA |  FortiGate VM Virtual Firewall |  FortiCNP Cloud-native Protection |
|  FortiGate SD-WAN |  FortiMonitor DEM |  FortiWeb (WAAP) |  FortiADC Application Delivery |
|  FortiToken MFA |  FortiPAM PAM |  FortiGate CNF Cloud-native Firewall |  FortiDevSec Application Security Testing |
|  FortiAuthenticator IAM |  FortiTrust Identity | | |

Security Operations



- | | | |
|---|---|--|
|  FortiEDR/XDR EDR/XDR |  FortiAnalyzer Analytics |  SOCaaS |
|  FortiNDR NDR |  FortiSIEM SIEM |  MDR Service |
|  FortiDeceptor Deception |  FortiSOAR SOAR |  IR Service |
|  FortiRecon DRPS |  FortiSandbox Sandbox |  FortiMail SEG |

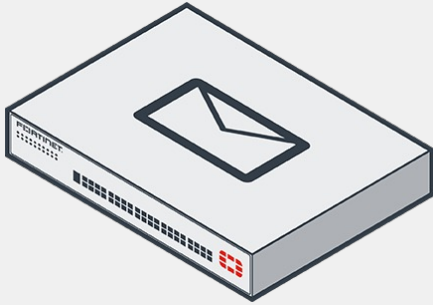


Jak nám může pomoci Fortinet?



FORTINET[®]
FortiMail: SECURE EMAIL GATEWAY

Škálovatelné řešení pro každého zákazníka



Hardware Appliances

- 5 modelů
- Filter 50k až 3.5m zpráv za hodinu
- Podpora 10GE



Virtual Appliances

- 6 VM modelů
- CPU- and Domain-based
- Doživotní licence
- Subscription



SaaS

- Gateway nebo Server mod
- Standard nebo Premium
- Per uživatel Per rok

FortiMail balíčky

Enterprise ATP Bundle

Base Bundle



Antispam Service

- Sender IP ratings
- Embedded URL ratings
- Content-based hashes for spam and phishing campaigns
- Separate “newsletter” identifiers



Antivirus Service

- One-to-many signatures
- Heuristic rules
- Emulation
- Decrypting/Unpacking
- Patented content pattern recognition language (CPRL)



Outbreak Prevention

- Pre-signature intelligence
- Covers emerging spam and malware campaigns
- Leverages new sandbox and other intelligence



FortiSandbox Cloud

- FortiSandbox hosted by Fortinet
- Includes prefiltering, emulation and full instrumented analysis
- Subscription-based
- No separate sandbox required



Content Disarm and Reconstruction

- Removes high risk active content
- Supports Microsoft Office and Adobe
- Can be applied by user, group or policy
- Original documents can be retained and restored



Click Protect

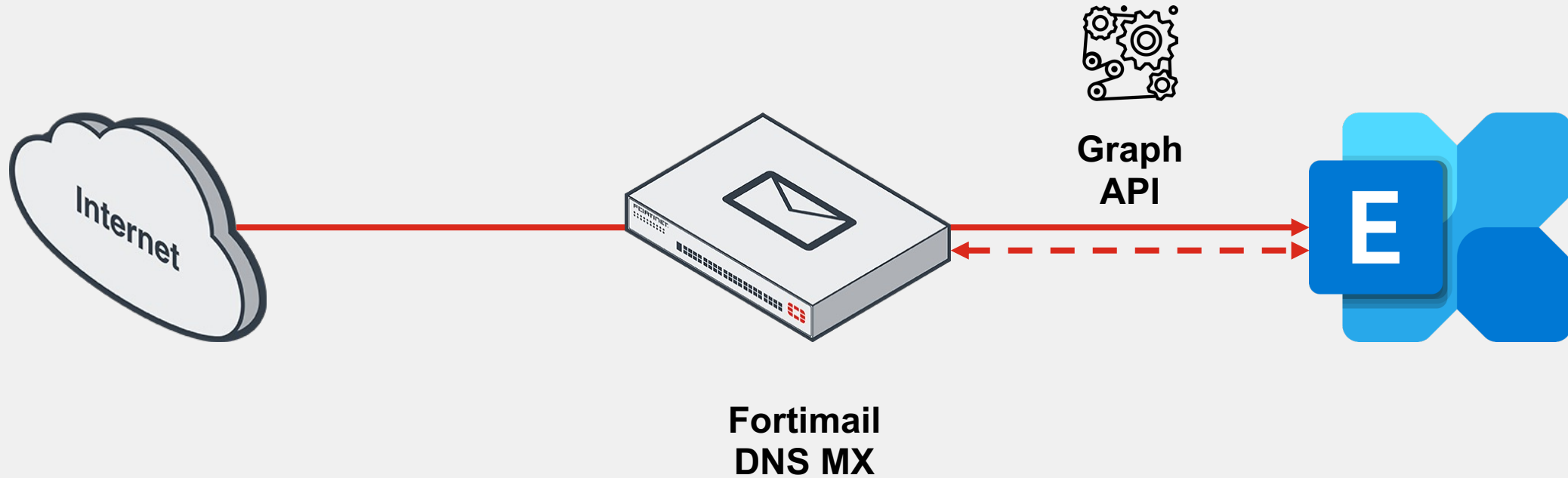
- Dynamic reputation query
- Determines rating at the time of user click
- Identifies recently compromised sites changed shortly after campaigns are launched



Impersonation Analysis

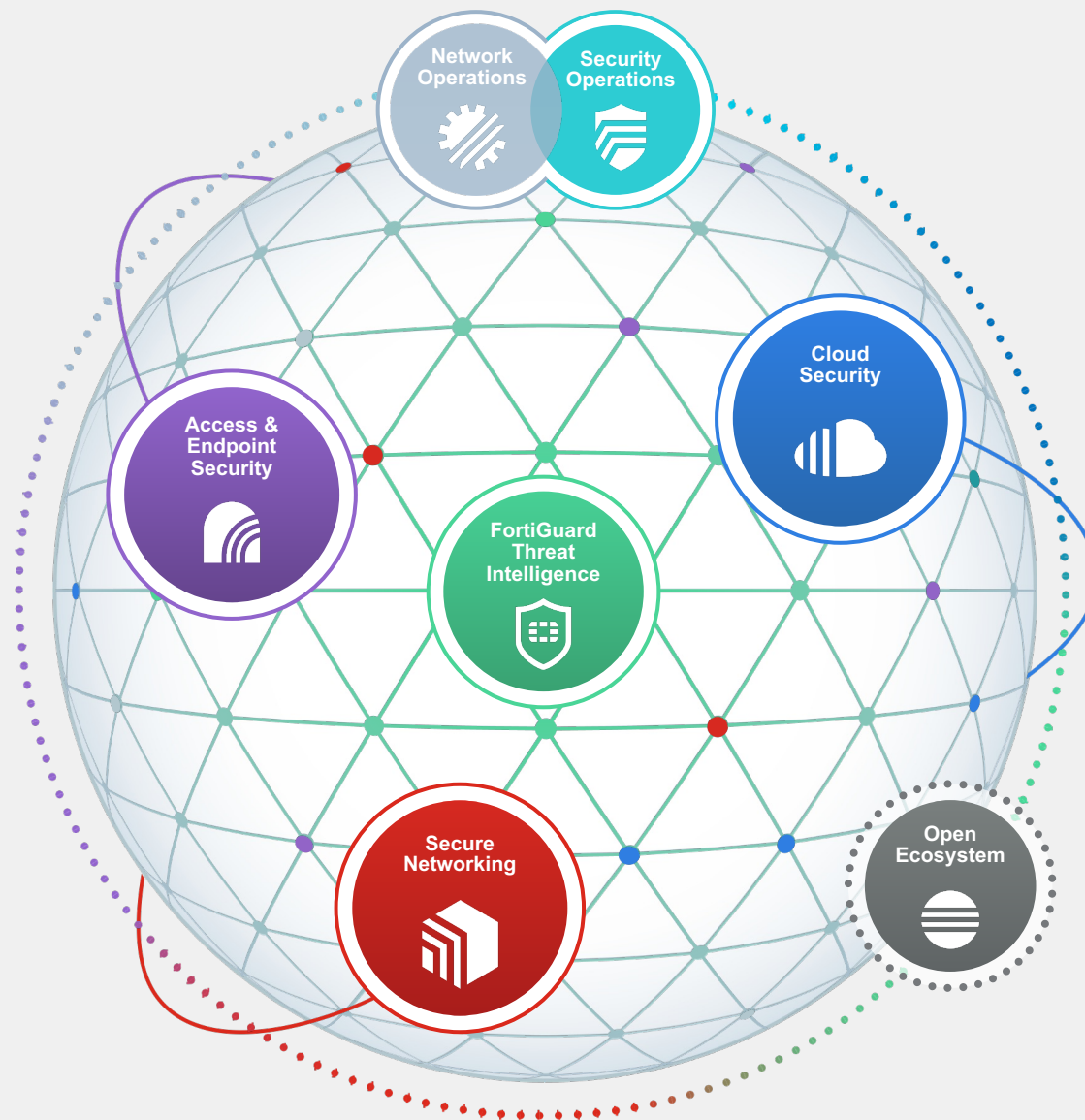
- Identifies spoofed email
- Dynamically builds protections for common email addresses
- Complements sender authentication

Microsoft 365 - Exchange online – API ochrana



Integrace v rámci Fortinet Security Fabric

**Budoucnost
zabezpečení emailu
přesahuje rámec
emailu.**



High marks in performance across 3rd party testers



ComputerHope.com



99.8%

Detection of malicious threats in emails.



99.90%

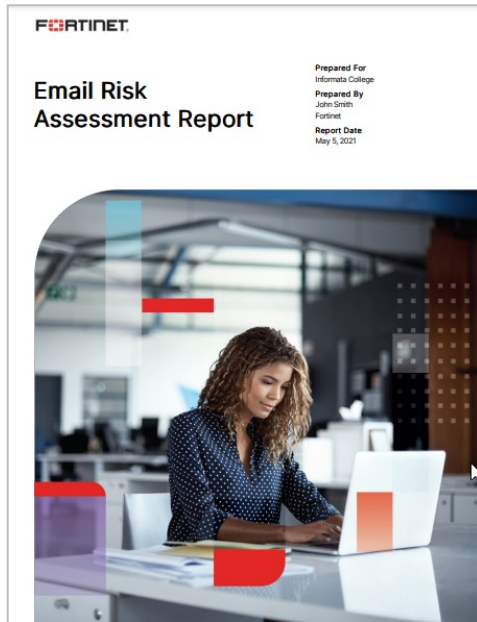
Spam Catch Rate



100%

Malware Detected

CTAP – zhodnocení emailového zabezpečení



Executive Summary

We aggregated key findings from our email risk assessment within the Executive Summary below. As represented in the summary, this report is divided into three sections: Security, Productivity, and Utilization. While the highlights are listed below, a more detailed view of each section follows. Be sure to review the Recommended Actions page at the end of this report as well for actionable steps your organization can take to mitigate email borne threats and optimize your overall email experience.

842
Known or Suspected Attachment-based Attacks

52
Known or Suspected URL-based Attacks

4
Known or Suspected Impersonation-based Threats

Note that any threats observed within this report have bypassed your existing email security solution, so they should be considered active and potentially dangerous.

Productivity

415,225
Emails Flagged as Spam

19,925
Suspected Newsletters

1,647
Emails Detected with Adult Content

Although not necessarily malicious, spam, newsletters and/or emails with adult content represent a potential nuisance and/or offense. Organizations should consider whether the current level of unwanted or inappropriate email is acceptable.

Utilization

15,215
Average Emails Processed Per Day

1.6GB
Average Email Bandwidth Per Day

110.6KB
Average Email Size

Although you may have moved to cloud-based email infrastructure, utilization statistics can be valuable in a number of ways, they can be used to compare your email utilization against industry norms. Daily usage numbers can be tracked over time; deviation analysis is also helpful when determining anomalous company-wide behavior.

Email Risk Assessment Report

Security

Quick Stats

- 842 known or suspected attachment-based attacks
- 52 known or suspected URL-based attacks
- 4 known or suspected impersonation-based attacks
- VBA/Agent.6A13tr.didr is the top known malware detected in attachments
- 748 known malware identified
- mode.us?reservation.org is the top suspicious domain from URL-based attacks

Known Malware Identified

By applying the existing intelligence of FortiGuard Labs to your email traffic, we've identified known malware on their way to your end user inboxes (via attachments). Below you can see the top 8 known malware identified by volume.

Malware Name	Count
VBA/Agent.6A13tr.didr	164
VBA/Agent.7DA5tr.didr	88
VBA/Agent.D8A3tr.didr	85
VBA/Agent.F78Etr.didr	59
VBA/Agent.LP1tr.didr	55
VBA/Agent.LM1tr.didr	52
VBA/Agent.LR8tr.didr	42
VBA/Agent.LR8tr.didr	41

Known Malware Identified with Details

For the known malware we identified, we have presented more detail about the most persistent messages and malware:

#	Sender	Subject	Malware	Count
1	qian.chen@chirooising.com	External Invoice Available	VBA/Agent.6A13tr.didr	6
2	luzema.vega@itico-group.com	External Outstanding Invoice	VBA/Agent.7DA5tr.didr	6
3	esanchez@informata.edu	Cambion de pago de sus servicios	VBA/Agent.LP1tr.didr	6
4	en4yanket@mountainman-ycoil.com	External Invoice Query	VBA/Agent.LP1tr.didr	5
5	vwb829f@mail.shobot.com	External: 20217 - SHABOT INC Invoice # 9385580072112072018	VBA/Agent.F78Etr.didr	4
6	ARDept@glovelare.net	External: Versa Comm / Account 63092	VBA/Agent.LR8tr.didr	4
7	investigstic@gmail.com	External: Purchase Order	RTF/CVE201711982_OIEexploit.dll	3
8	khuram@koyalbranding.pk	Billing Notification - New Invoice(s)	VBA/Agent.3ABFtr.didr	3

Email Risk Assessment Report

Productivity

Quick Stats

- 415,225 emails flagged as spam
- no-reply@edumarketnews.com is the top spam sender
- arh@harcour.com is the top spam domain
- 91:100 spam versus valid email ratio
- new@edumarketnews.com is the top newsletter sender
- 19,925 suspected newsletters
- 1,647 emails detected with adult content

Top Spam Senders

Spam is a persistent annoyance with most organizations. By understanding sources, enterprises can simply blacklist senders. Should they find they are the senders, often in the case of marketing communications sent internally, it is recommended that volume is rate controlled to avoid the organization ending up on blacklists. The top 10 spam senders by volume to your domain are listed below.

Sender	Count
no-reply@harcour.com	23,717
ms.aunderson@edumarketnews.com	14,684
quarantain@mesaging-microsoft.com	11,103
dsellers@edmodo.com	10,419
informata@eduafrate.com	10,135
rpe@hanacademy.org	9,339
info@degreed.com	6,032
donotreply@fwd.com	5,167
no-reply@markquize.com	4,296
ecommerce@freight-fax.com	4,181

Newsletter Domains

Generally not considered spam, but sometimes equally as impactful are newsletters that your email users subscribe to. If newsletters are a burden on your email infrastructure, we recommend modifying or enforcing corporate use policies and asking subscribers to use their personal email addresses for such communications.

Domain	Count
edumarketnews.com	1,367
schoolcool.org	894
messagecentral.com	688
gmail.com	654
tradeplus.educationr.net	572
shopiqe-tool.com	326
knowledgecloud.com	300
utiv-crowd.com	296
missionnetwork.org	288
smartflex.com	247

Email Risk Assessment Report



FORTINET®