



# Ochrona pracowników i przedsiębiorstw przed głównymi wektorami cyberataku

**Grzegorz Całun**

*Technical Solutions Engineer – Arrow ECS*

# Need for Security Platform



Through 2021,  
**99%** of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

## Need for Cyber Hygiene



## Global Workplace Analytics

**25-30%** of the workforce will be working-from-home multiple days a week by the end of 2021

## Work From Anywhere



Ponemon  
INSTITUTE

**68%** IT security professionals say their company experienced one or more endpoint attacks

## Endpoint Protection Needed

### Sources:

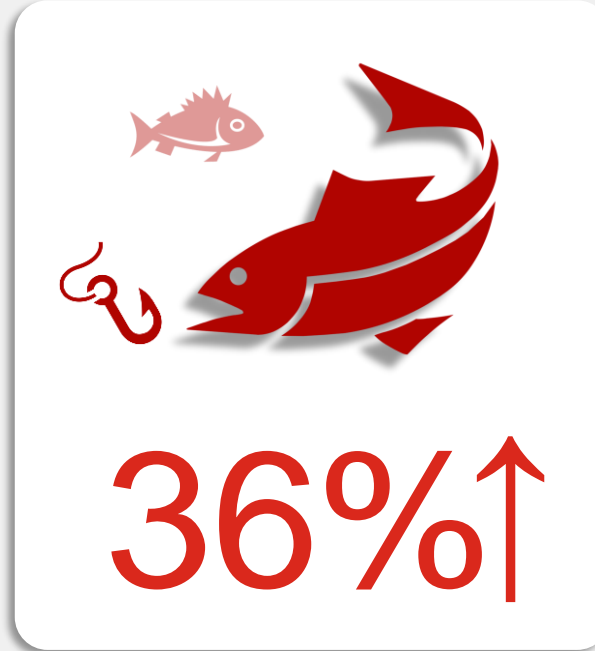
1. Gartner, Craig Lawson
2. Global Workplace Analytics
3. The Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute, 2020



# Email's as a primary threat vector?



Increased use of  
“Misrepresentation” in Social  
Engineering-related incidents.



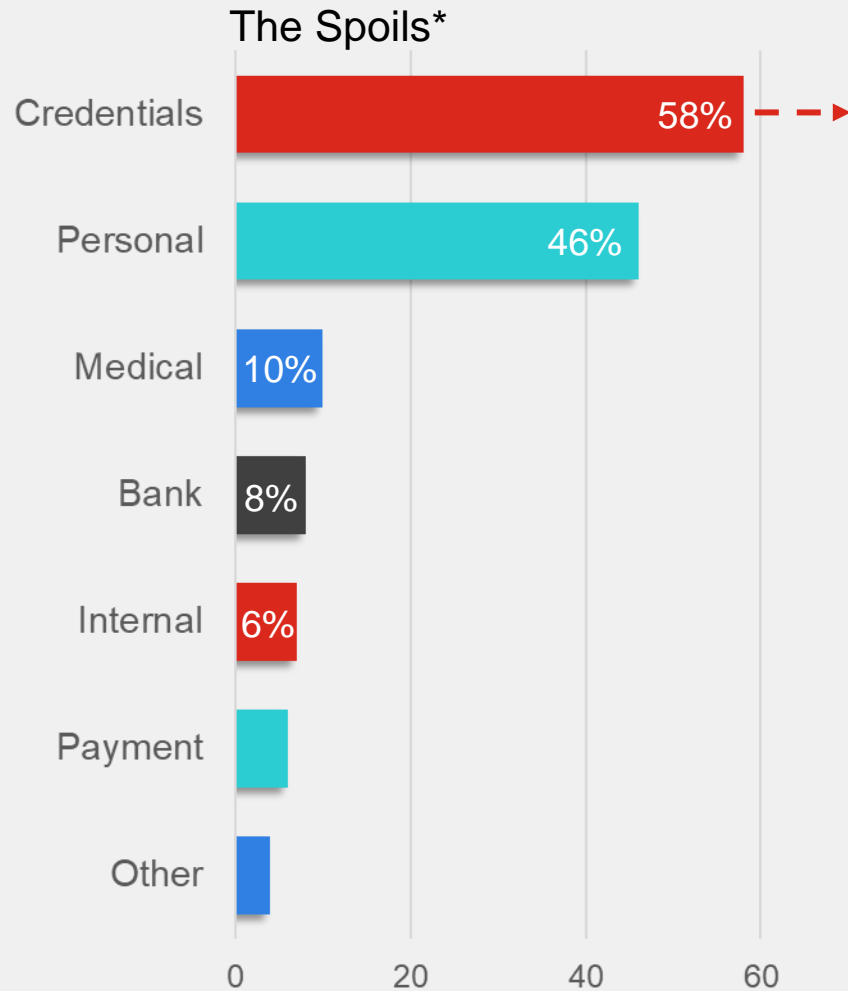
Percent of breaches involving  
phishing, up from 25% YoY.



Percent of Business Email  
Compromise (BEC) attacks that  
were successful.



# Email's use as a primary threat vector?



Percent of breaches involving ransomware, up from ~5% the prior year.\*



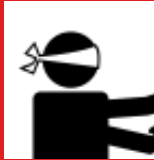

Average cost of a data breach worldwide.\*\*



\*Statistics from Verizon Data Breach Investigations Report 2021.

\*\*Ponemon Institute Cost of a Data Breach Report 2020.

# Endpoint Security Gaps



**63%** of companies can not monitor off-network endpoints, over half can't determine endpoint compliance status


Lack of Visibility

According to Gartner



Through 2021, **99%** of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.

Vulnerabilities



**87%**

Most compromises took minutes, or less

Attacks are fast moving

Sources:

1. The Cost Of Insecure Endpoints, Ponemon Institute, 2017
2. Gartner, How to Respond to the 2018 Threat Landscape, Greg Young, 28 November, 2017
3. Breach Investigation Report, Verizon, 2018



# Cybersecurity Challenges

## Users & Devices

Travel



WFH



Office



Plant



## Networks

Wi-Fi



Switch



SD-WAN



5G



Cloud On Ramp



## Applications

Cloud



Data Center



SaaS

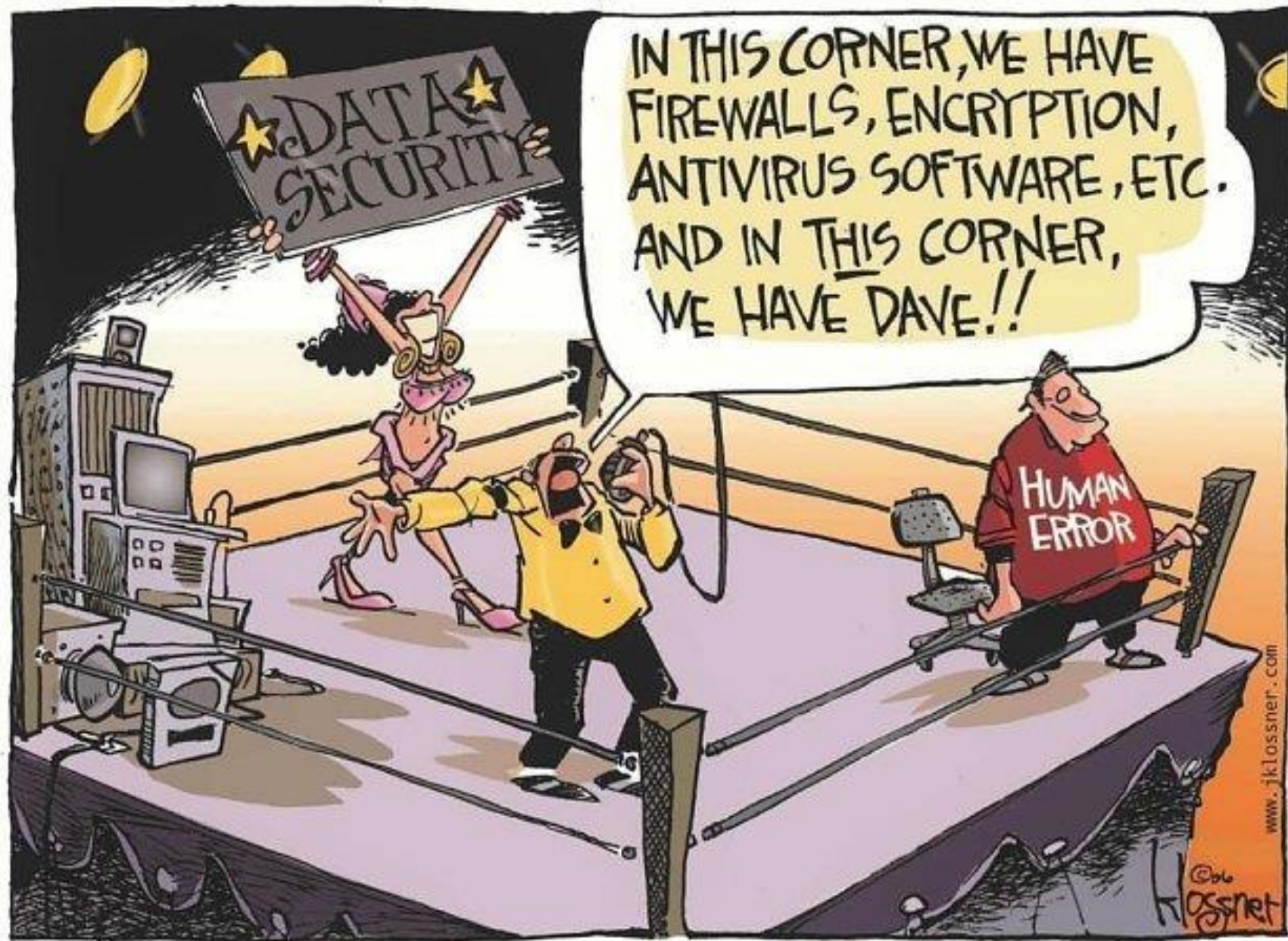


Edge Compute

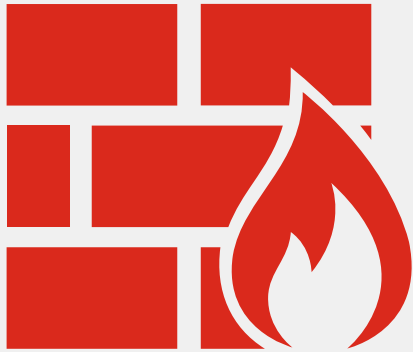


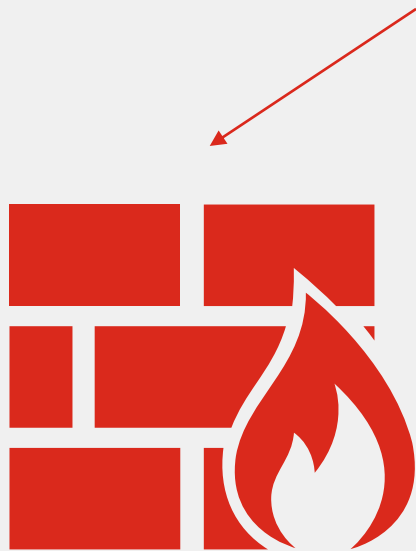
# What to do?







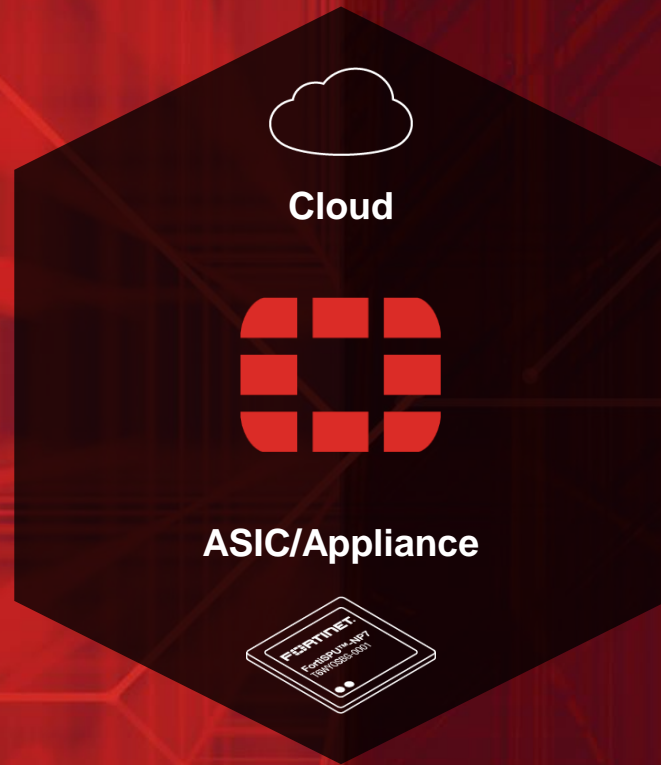




# Security-Driven Networking

## The Next Era of Networking and Security Convergence

**WIDE AREA  
NETWORKING**



**NETWORK  
SECURITY**

Flexible, anywhere and anytime security

# Fortinet Security Fabric

## **BROAD**

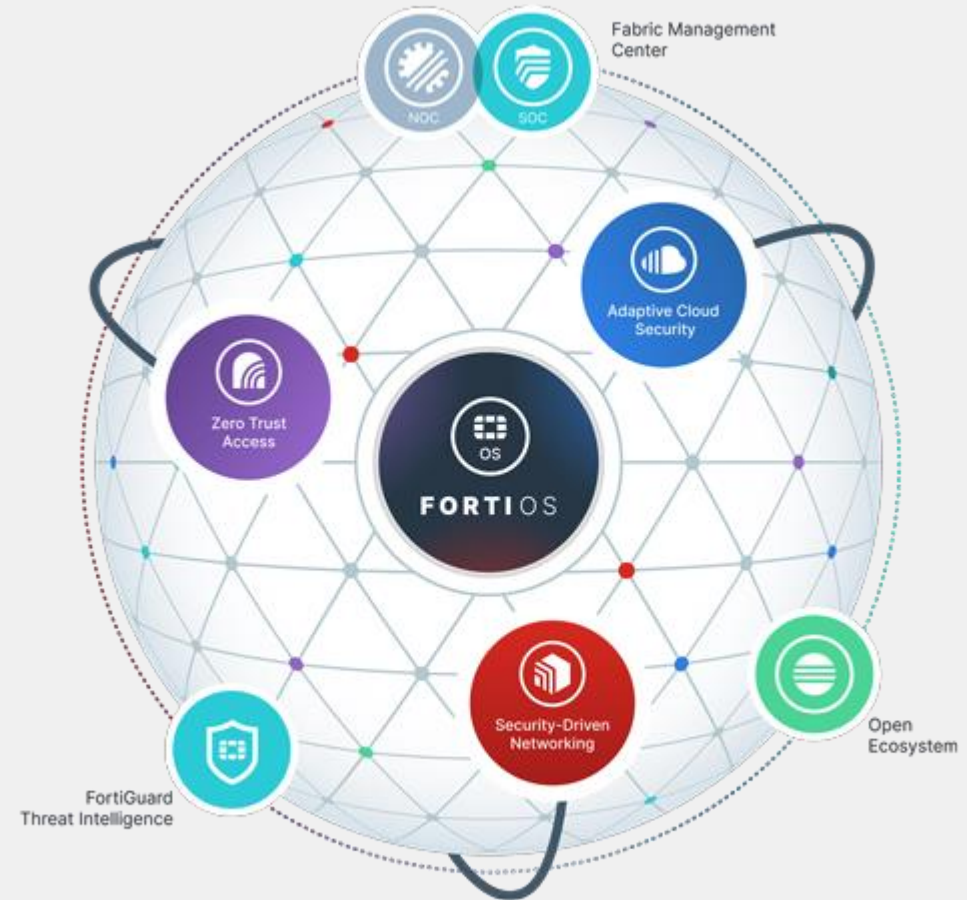
visibility of the entire digital attack surface to better manage risk

## **INTEGRATED**

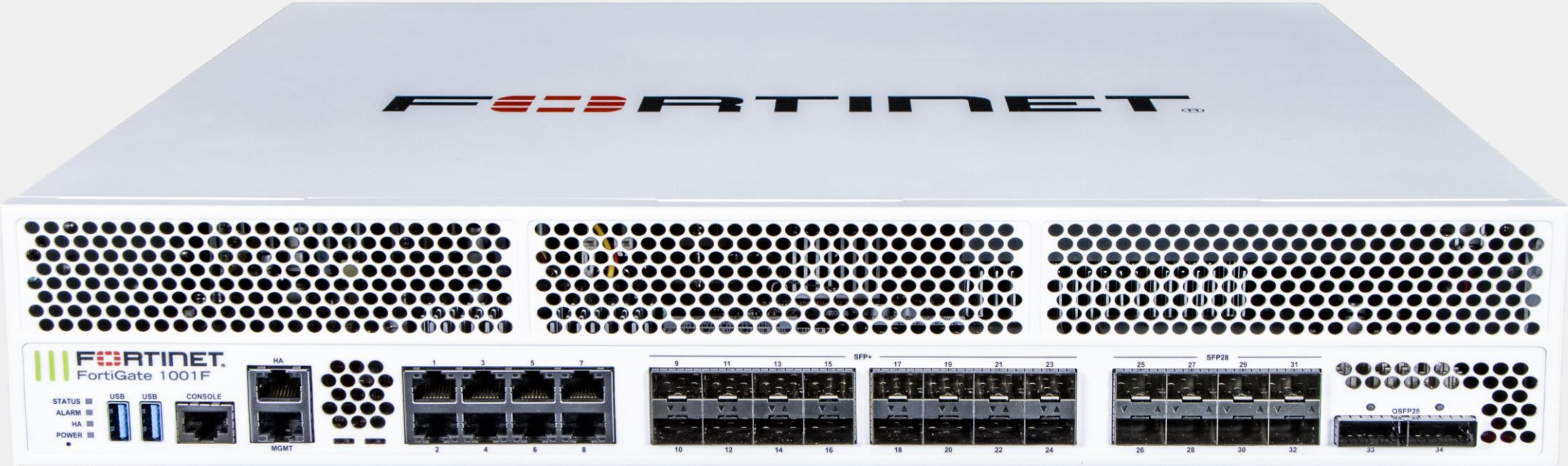
solution that reduces the complexity of supporting multiple point products

## **AUTOMATED**

workflows to increase speed of operations and response

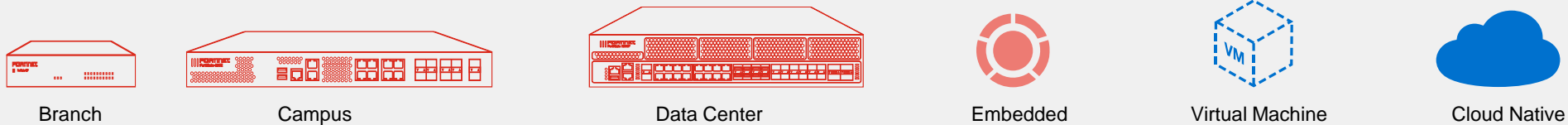
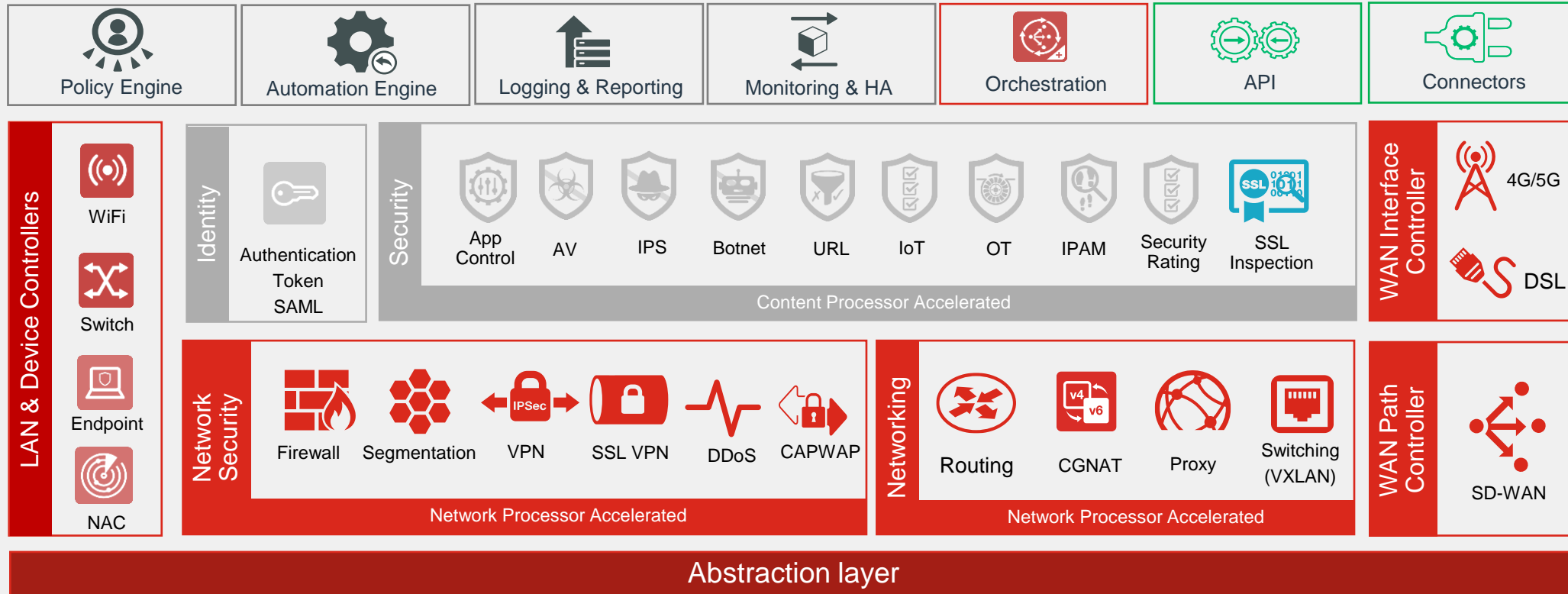


# Fortinet Fortigate – Next Generation Firewall





# FortiOS Innovative Network Operating System





Products &gt; Fortinet FortiGate Next-Generation Firewall



Get It Now

Test Drive

What's Test Drive?

Test Drive duration

3 hours

Pricing information

Cost of deployed template components

Categories

[Compute](#)  
[Networking](#)  
[Security](#)

Support

[Support](#)  
[Help](#)

Legal

[License Agreement](#)  
[Privacy Policy](#)

# Fortinet FortiGate Next-Generation Firewall [Save to my list](#)

Fortinet

★ 3.6 (5 ratings)

[Preferred solution](#)[Overview](#) [Plans](#) [Ratings + reviews](#)

FortiGate NGFW improves on the Azure firewall with complete data, application and network security

[Try FortiGate free for 30 days by selecting pay-as-you-go \(PAYG\)\\*!](#)

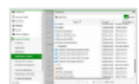
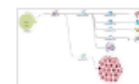
Fortinet's FortiGate Next Generation Firewall (NGFW) provides state-of-the-art protection and automated management for consistent policy enforcement and visibility. To identify and mitigate the latest threats, FortiGate includes application-aware network security, VPN (SSL or IPSec), SD-WAN, virus and malware protection, IPS, and Web filtering, along with advanced features such as an extreme threat database, vulnerability management, and flow-based inspection.

FortiGate NGFWs seamlessly integrate with AI-driven FortiGuard and FortiSandbox services to protect against known and zero-day threats. Consider using with FortiManager for centralized security management and FortiAnalyzer for log analytics.

Select the plan above to start the step-by-step guide through setting up network and resource groups, public IP addresses, pre-defined configurations, and more.

**FortiGate delivers:**

- End-to-end security across the full attack surface in the cloud deployment
- Top-rated security validated by third-party testing
- Protection of Docker/container environments while inspecting application traffic



Filter by title

SaaS application tutorials

Single sign-on tutorials

> 0 - 9

> A

> B

> C

> D - E

> F - G

> H - I

> J - K

> L - M

> N - O

> P

> Q - R

> S

> T - V

> W - Z

User provisioning tutorials

> 0 - 9

> A - F

> G - M

> N - S

> T - Z

Learn / Azure / Active Directory / Application management / SaaS application tutorials /



# FortiGate Azure Virtual Machine Deployment Guide

Article • 11/22/2022 • 7 minutes to read • 3 contributors

Feedback

## In this article

[Redeem the FortiGate License](#)

[Download Firmware](#)

[Deploy the FortiGate VM](#)

[Create a Second Virtual NIC for the VM](#)

[Show 2 more](#)

Using this deployment guide, you will learn how to set up and work with the Fortinet FortiGate next-generation firewall product deployed as an Azure Virtual Machine. Additionally, you will configure the FortiGate SSL VPN Azure AD Gallery App to provide VPN authentication through Azure Active Directory.

## Redeem the FortiGate License

The Fortinet FortiGate next-generation firewall product is available as a virtual machine in Azure infrastructure as a service (IaaS). There are two licensing modes for this virtual machine: pay-as-you-go and bring-your-own-license (BYOL).

If you have purchased a FortiGate license from Fortinet to use with the BYOL virtual machine deployment option, redeem it from Fortinet's product activation page – <https://support.fortinet.com>. The resulting license file will have a .lic file extension.







## Azure Administration Guide

- + About FortiGate-VM for Azure
- **Deploying FortiGate-VM on Azure**
  - Azure services and components
  - Deploying FortiGate-VM from a VHD image file
  - + Deploying FortiGate with a custom ARM template
  - + **Deploying FortiGate-VM using Azure PowerShell**
  - Deploying FortiGate-VM on regional Azure clouds
  - Deploying FortiGate-VM from the marketplace
  - Enabling accelerated networking on the FortiGate-VM
  - Upgrading FortiOS
- + Deploying autoscaling on Azure
- + Single FortiGate-VM deployment
- + HA for FortiGate-VM on Azure
- + SDN connector integration with Azure
  - SDN connector in Azure Stack
- + VPN for FortiGate-VM on Azure
- + Azure AD acting as SAML IdP
- + Azure Sentinel

7.2.0 ↓

[Copy Link](#)[Download PDF](#)

## Deploying FortiGate-VM on Azure





























You can deploy FortiGate-VM next generation firewall for Azure as a virtual appliance in Azure cloud (infrastructure as a service). See [Single FortiGate-VM deployment](#).

Browse apps

- Get Started**
- Analytics
- AI + Machine Learning
- Azure Active Directory
- Blockchain
- Compute
- Containers
- Databases
- Developer Tools
- DevOps
- Identity
- Integration
- Internet of Things
- IT & Management Tools
- Monitoring & Diagnostics
- Media
- Migration
- Mixed Reality
- Networking
- Security
- Storage
- Web

Trials: 
 Operating System: 
 Publisher: 
 Pricing Model: 
 Product Type: 
[Reset filters](#)

All results

 <p><b>Fortinet FortiAuthenticator ID...</b> By Fortinet Access Management establishing Identity for the Fortinet Security Fabric</p> <p>Bring your own license</p> <p><a href="#">Get it now</a> </p>	 <p><b>Fortinet FortiGate Next-Generation Firewall</b> By Fortinet FortiGate NGFW improves on the Azure firewall with complete data, application and network security</p> <p>★★★★★ (5)</p> <p>Price varies </p> <p><a href="#">Test Drive</a> </p>	 <p><b>Fortinet FortiSIEM - SIEM &amp; Analytics</b> By Fortinet Fortinet FortiSIEM provides Multi-vendor SIEM, Analytics, Reporting and Alerting</p> <p>Bring your own license</p> <p><a href="#">Get it now</a> </p>	 <p><b>Fortinet FortiGate Next-Generation Firewall (VM)</b> By Fortinet FortiGate Next-Generation Firewall delivers complete content and network protection</p> <p>★★★★★ (130)</p> <p>Starts at \$0.36/hour </p> <p><a href="#">Free software trial</a> </p>	 <p><b>Fortinet FortiGate for Azure Virtual WAN</b> By Fortinet FortiGate Secure SD-WAN with Firewall in Virtual WAN Hub</p> <p>Plans start at Free</p> <p><a href="#">Get it now</a> </p>
 <p><b>Fortinet FortiWeb Cloud WAF as a Service</b> By Fortinet Defend against known and zero-day threats with machine learning-enhanced web app and API protection</p> <p>★★★★★ (2)</p> <p>Starts at Free </p> <p><a href="#">Get it now</a> </p>	 <p><b>Fortinet FortiGate</b> By Microsoft Sentinel, Microsoft Corp... Fortinet FortiGate</p> <p>Price varies</p> <p><a href="#">Get it now</a> </p>	 <p><b>Fortinet FortiSandbox Zero-Day Threat...</b> By Fortinet Zero-day Malware Protection for Your Cloud and Hybrid Workloads</p> <p>★★★☆☆ (1)</p> <p>Bring your own license</p> <p><a href="#">Free software trial</a> </p>	 <p><b>Fortinet FortiWeb Web Application Firewall WA...</b> By Fortinet AI-based, multi-layered protection for web-based applications</p> <p>Starts at \$0.6975/hour</p> <p><a href="#">Free software trial</a> </p>	 <p><b>Fortinet FortiWeb Cloud</b> By Microsoft Sentinel, Microsoft Corp... Fortinet FortiWeb Cloud</p> <p>Price varies</p> <p><a href="#">Get it now</a> </p>
 <p><b>Fortinet FortiADC Application Delivery...</b> By Fortinet Multi-Service Application</p>	 <p><b>Fortinet FortiWeb Web Application Firewall...</b> By Fortinet AI-based, multi-layered</p>	 <p><b>Fortinet FortiRecorder - Video Surveillance</b> By Fortinet Protect your assets and</p>	 <p><b>Fortinet FortiMail - Secure Email Gateway</b> By Fortinet Stop advanced email threats and</p>	 <p><b>Fortinet FortiProxy Secure Web Gateway</b> By Fortinet FortiProxy Secure Web Gateway</p>

# Recognized Leader in Analysts' Reports

For Firewalls and SD-WAN

## Nov. 2021 Magic Quadrant™ for Network Firewalls



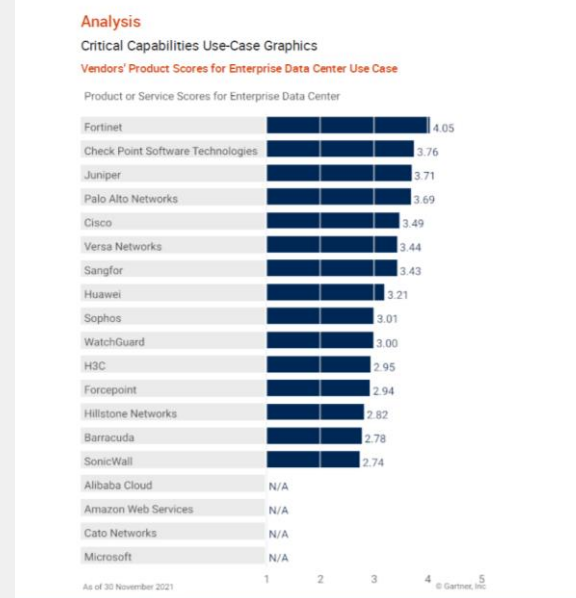
Fortinet Recognized as a Leader 2021 is 12<sup>th</sup> time included in this Magic Quadrant

## Sep. 2022 Magic Quadrant™ for SD-WAN



Fortinet placed highest in Ability to Execute two years in a row and Recognized for Completeness of Vision.

## Jan 2022 Critical Capabilities for Network Firewalls

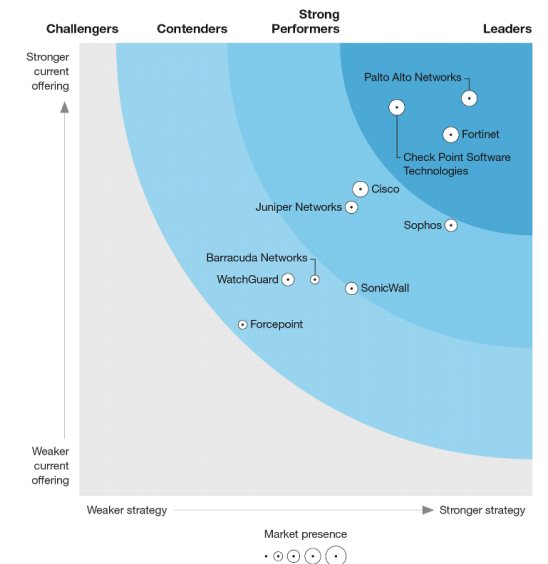


Fortinet #1 in three of five use cases including "Enterprise Data Center", "Distributed Enterprise"

## Oct. 2022 Forrester Wave Enterprise Firewalls

Forrester Wave™: Enterprise Firewalls, Q4 2022

THE FORRESTER WAVE™  
Enterprise Firewalls  
Q4 2022



Fortinet named a Leader in the Forrester Wave



# Introducing FortiClient



## Comprehensive end-point protection & security enforcement



Broad endpoint visibility



Endpoint compliance and vulnerability management



Proactive endpoint defense



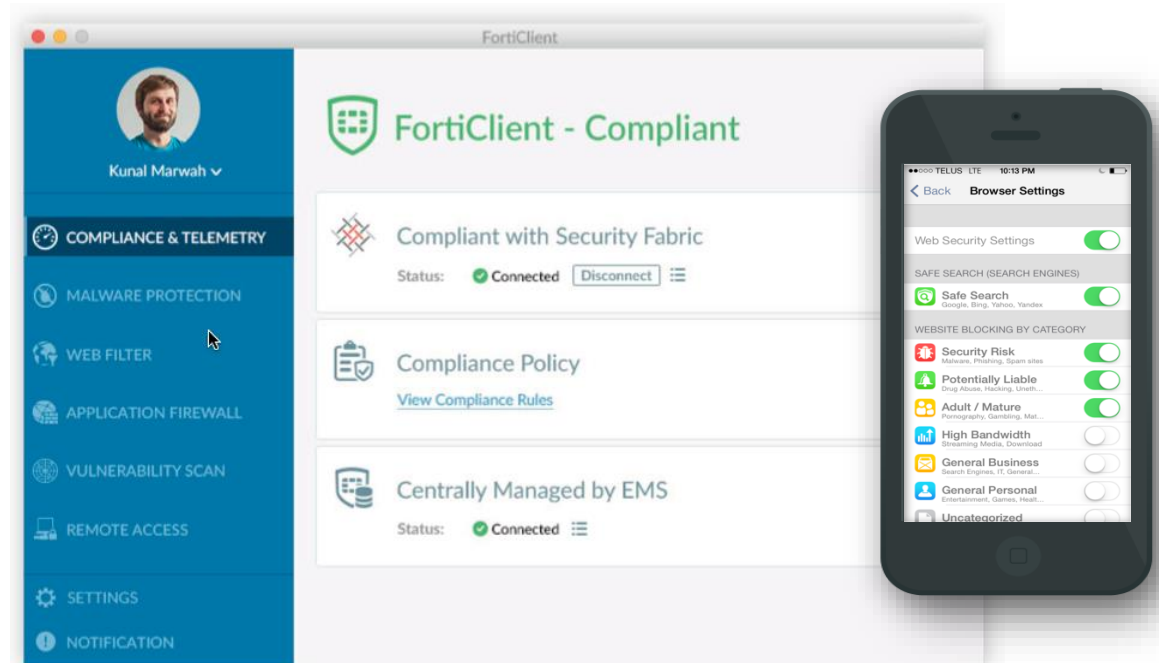
Automated threat containment



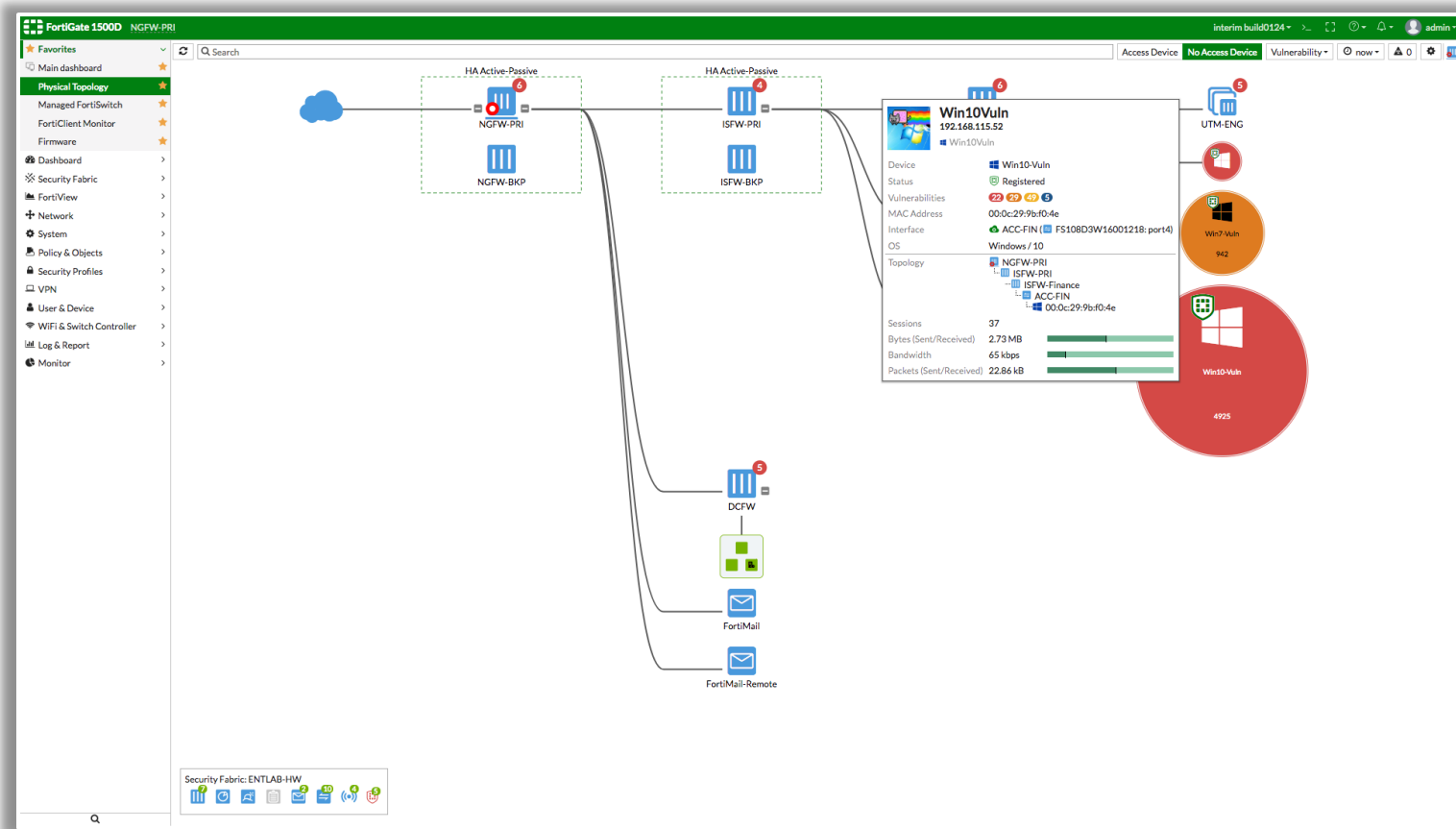
Secure remote access



Easy to deploy and manage



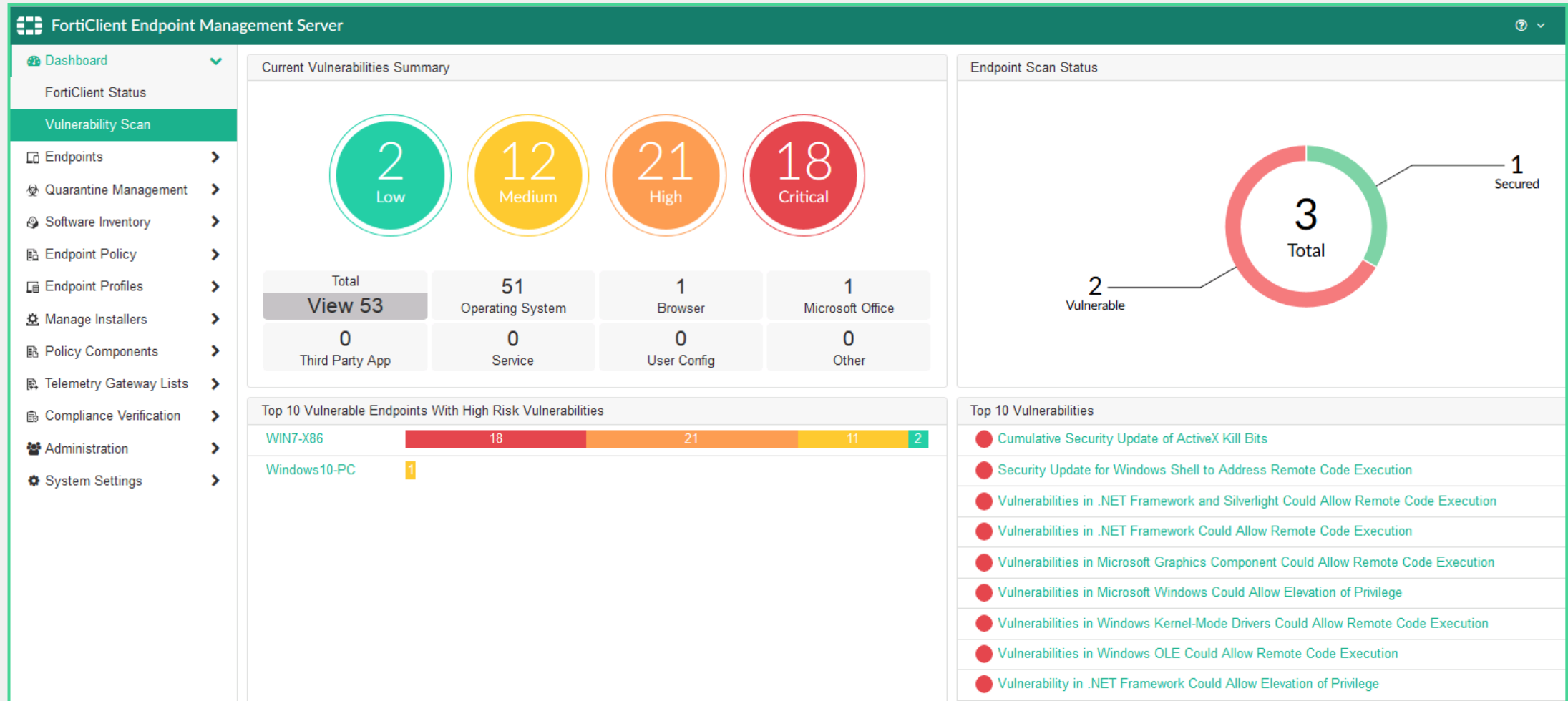
# Risk Visibility



- Device information
  - OS
  - Co-relate multiple MAC
- FortiClient status
- Endpoint vulnerabilities
- Logged-in user
- User avatar
- Social IDs
- Online/off-line
- Endpoint events and logs



# Vulnerability Scanning



# Advanced Threat Protection

The screenshot displays the FortiClient Enterprise Management Server interface, showing a process tree for a high-risk file. The interface is divided into three overlapping windows, each showing a different level of detail.

The top window shows the dashboard with a navigation menu on the left and a summary bar at the top. The summary bar indicates 6 Devices, 0 Devices, 2 Devices, 3 Devices, and 4 Devices. The middle window shows the process tree for a high-risk file, 6666xp.exe. The bottom window shows the details for the process tree.

The process tree shows the following structure:

- 6666xp.exe (High Risk) (Red gear icon)
- AcroRd32.exe (Green gear icon)
- svchost.exe (Green gear icon)
- sdclt.exe (Green gear icon with 2 red dots)
- services.exe (Green gear icon)
- svchost.exe (Green gear icon)
- msiexec.exe (Green gear icon)
- taskhost.exe (Green gear icon)
- mscorsvw.exe (Green gear icon with 4 red dots)
- mscorsvw.exe (Green gear icon)
- mscorsvw.exe (Green gear icon)
- mscorsvw.exe (Green gear icon)
- mscorsvw.exe (Green gear icon)
- mscorsvw.exe (Green gear icon)

The details window shows the following information:

Process Information	
PID	3844
File Path	%CURRENTPATH%\loader.exe
File Type	pdf
CMD Line	c:\work\loader.exe c:\work\4035302442377709471.pdf 55000
MDS	494c08f7a144d3cc4cfa661ed1244039
Detail	Executable dropped dll/sys file(s) to system directory





# FortiGuard Web Filter Database

The screenshot displays the FortiClient Endpoint Management Server interface. The left sidebar shows navigation options: Dashboard, Endpoints, Quarantine Management, Software Inventory, Endpoint Policy, Endpoint Profiles, Local Profiles (selected), Default (selected), Manage Installers, Policy Components, Telemetry Gateway Lists, Compliance Verification, Administration, and System Settings.

The main content area shows the 'Web Filter' configuration for the 'Default' profile. The 'Web Filter' toggle is turned on. Under the 'General' section, the following options are checked: Client Web Filtering When On-Net, Log All URLs, Log User Initiated Traffic, and Enable Web Browser Plugin for Web Filtering. Under the 'Site Categories' section, the 'Site Categories' toggle is turned on, and a list of categories is displayed:

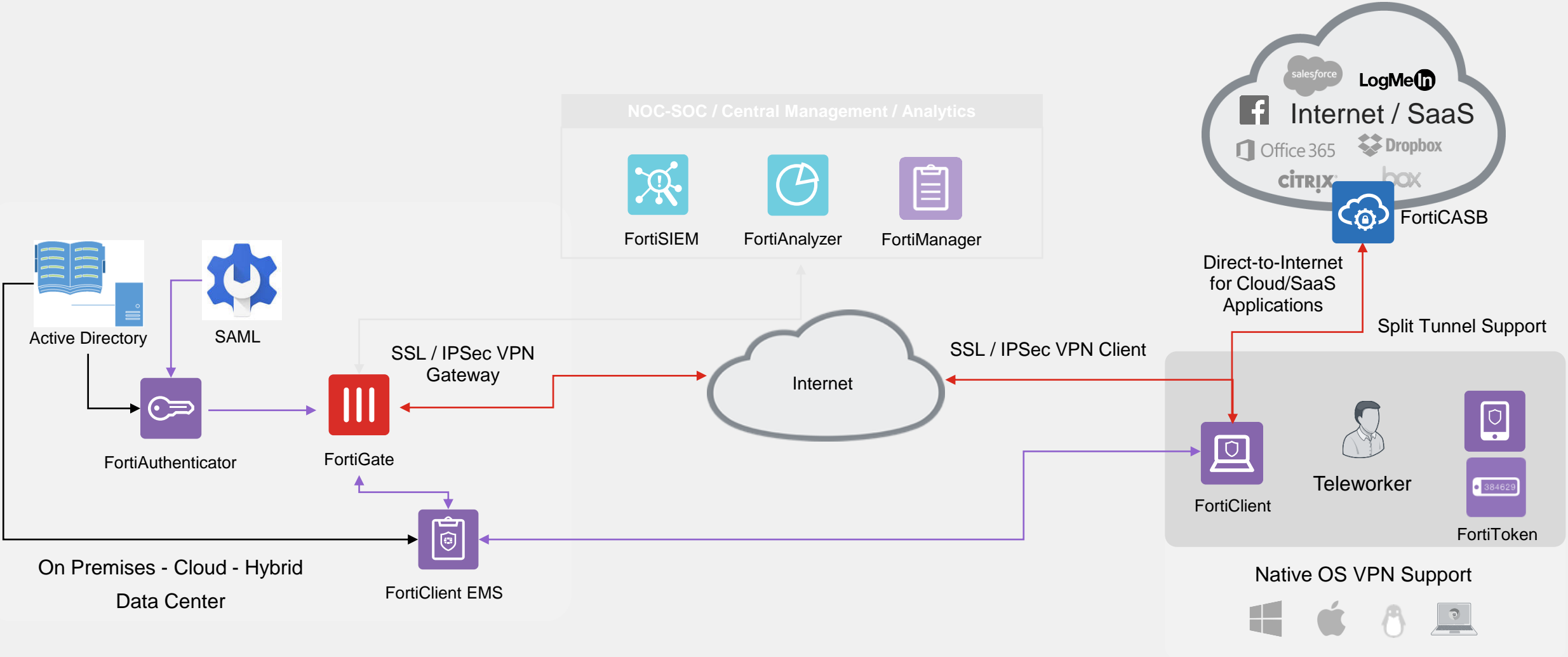
Category	Status
Adult/Mature Content	Disabled
Abortion	Disabled
Advocacy Organizations	Disabled
Alcohol	Disabled
Alternative Beliefs	Disabled
Dating	Disabled
Gambling	Disabled
Lingerie and Swimsuit	Enabled
Marijuana	Disabled
Nudity and Risque	Disabled
Other Adult Materials	Disabled
Pornography	Disabled
Sex Education	Enabled
Sports Hunting and War Games	Enabled
Tobacco	Disabled
Weapons (Sales)	Disabled

Red arrows point from the 'Adult/Mature Content' and 'Weapons (Sales)' categories in the list to their respective entries in the expanded 'Site Categories' panel on the right.





# Teleworker Remote and Secure Access



# Introducing FortiMail



Appliance



Virtual Machine



Hosted



Cloud



**Advanced anti-spam and antivirus filtering solution, with extensive quarantine and archiving capabilities.**



Top-rated Antispam and Antiphishing



Independently certified advanced threat defense



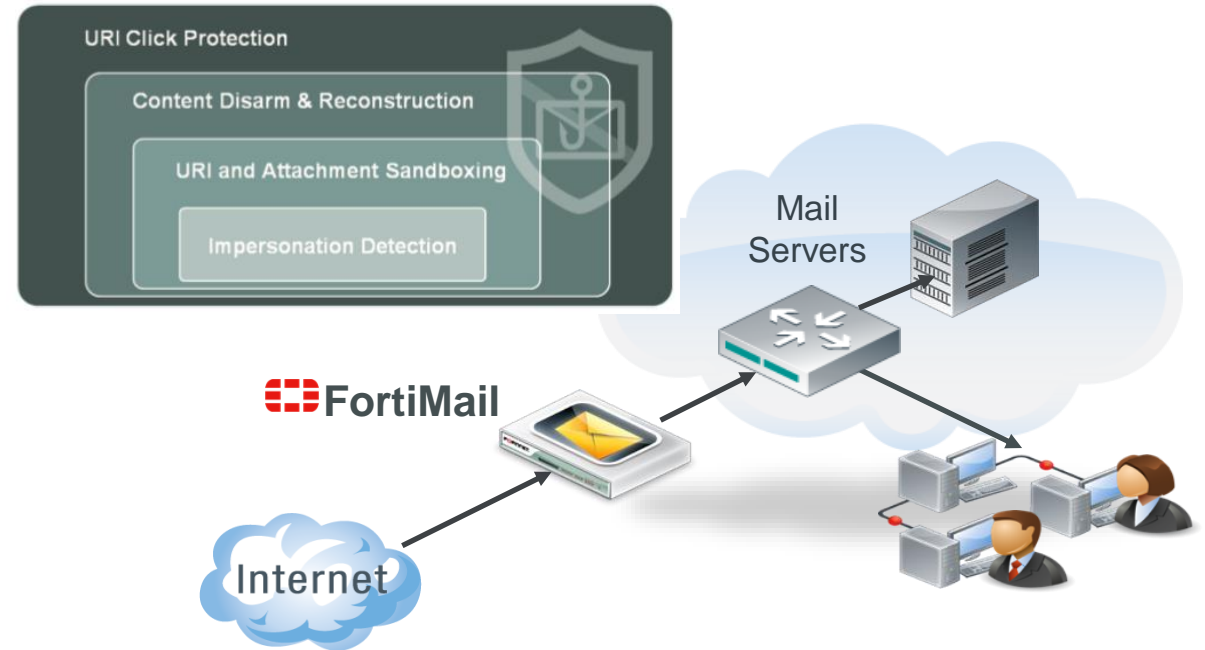
Integrated data protection



Enterprise-class management



High-performance mail handling



# Anti-Spam / Anti-Phishing

- **FortiGuard Reputation Databases**

- Cloud database query to identify know spam IP and content
  - FortiGuard Antivirus, Outbreak, Anti-Spam and URL Filtering
  - FortiGuard IP Reputation including Botnets
- Removes volumetric spam at low cost

- **Advanced Filtering Techniques**

- Detects new spam and phishing campaigns using a variety of techniques
  - Header Analysis
  - Dynamic Heuristics
  - Behavior Analysis
  - Sender Reputation
  - Suspicious Newsletter
  - DKIM / SPF / DMARC
  - Greyware Scanning

- **Targeted Attack Protection**

- **URI Click Protection**
- **Business Email Compromise - Impersonation Analysis**



**Fortinet FortiMail contd.**

**Final score:** 99.997

**Project Honey Pot SC rate:** 99.995%

**Abusix SC rate:** 99.999%

**Newsletters FP rate:** 0.0%



# Atak na polskie samorządy

Phishing podszywający się pod aktualizację oprogramowania BeSTi@ do zarządzania budżetami jednostek samorządu terytorialnego.

niebezpiecznik.pl

*From: Pomoc BeSTi@ [mailto...@budzetjsf.pl]*

*Sent: Monday, March 17, 2014 8:49 AM*

*To: ...*

*Subject: Aktualizacja systemu BeSTi@ do wersji 3.02.012.07*

*Witamy,*

*Pragniemy poinformować, iż dnia dzisiejszego została udostępniona nowa aktualizacja do systemu BeSTi@ w wersji 3.02.012.07.*

*Aktualizacja usuwa błędy związane z bezpieczeństwem bazy danych oraz poprawia problem z podpisem elektronicznym sprawozdań.*

*Instalacja jest bardzo prosta i nie wymaga dodatkowej pomocy oraz czynności.*

*Ze względu na znaczące poprawki bezpieczeństwa aktualizacja nie jest dostępna z menu programu BeSTia, należy przeprowadzić ją ręcznie.*

*Poniższy plik "Bestia.3.02.012.07" należy zapisać na pulpicie lub w innym miejscu a następnie go uruchomić co spowoduje zainstalowanie uaktualnienia do systemu BeSTi@.*

*hxxp://budzetjsf.pl/Update/BeSTia/Bestia.3.02.012.07.exe*

*Instalacja nie powinna zająć więcej niż minutę.*

*Dziękujemy i przepraszamy za niedogodności*

*-----  
Sputnik Software*

*tel. 61 622 00 60*





Technologie

# Atak hakerów na pocztę Outlook. Do skrzynek mieli dostęp przez trzy miesiące [CZYTNIK]

Maciej Orłowski 16 kwietnia 2019 | 09:36



czytnik



1 ZBIERKI

Maciej Orłowski Czytnik Technologie (Fot. Agata Jakubowska / Agencja Gazeta)

Jeśli masz pocztę na Outlooku, lepiej uważnie czytaj przychodzące maile. Microsoft poinformował o ataku hakerskim na swoje skrzynki pocztowe - hakerzy mieli do nich ograniczony dostęp przez trzy miesiące. Użytkownicy mogą teraz odbierać maile, które mają za zadanie wyłudzić wrażliwe dane.

## NAJCZĘŚCIEJ CZYTANE



PIS traci w ostatnich sondażach przed wyborami



Nowe laptopy z serii Lenovo Yoga. Komputery, jakich jeszcze nie było



Piotr Adamowicz, brat zamordowanego prezydenta Gdańska: "Nie chcę grać tragedii. Bo to także moja tragedia"



Sędzia Łączewski zrzeka się urzędu. I donosi do prokuratury na Ziobrę i hejlerską grupę "Kasztę"



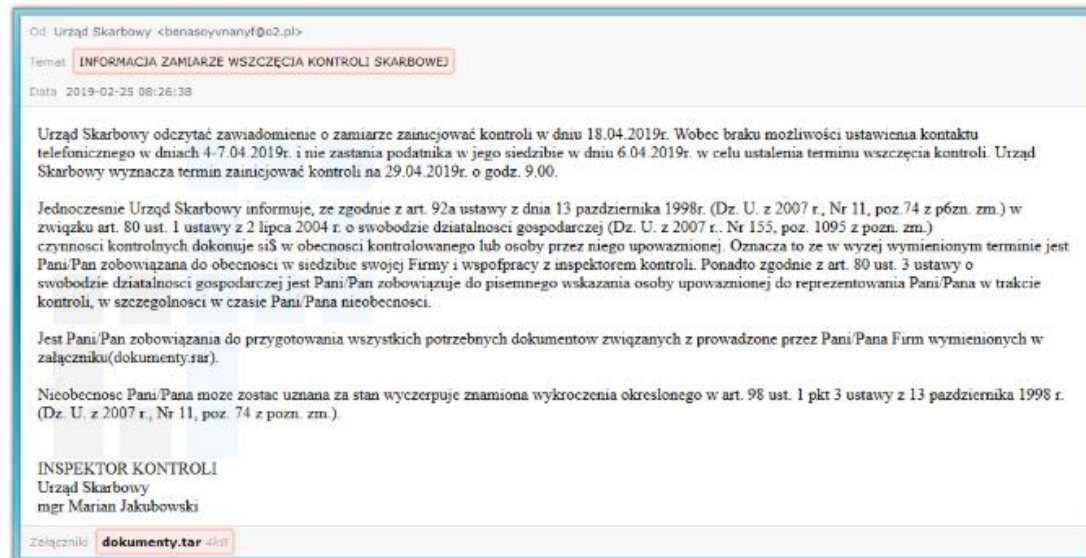
Po skardze "Wyborczej" na "Wiadomości" TVP KRRI bezta prezesa faczka Kurskiego

## Wiadomości spam podszywające się pod Urząd Skarbowy

PREBYTES SECURITY INCIDENT RESPONSE TEAM · 8 MIESIĘCY TEMU · 1 MIN READ

Od wczoraj trwa kampania spamowa, w której cyberprzestępcy podszywają się pod Urząd Skarbowy. Wszystkie wiadomości mają ten sam temat - **INFORMACJA O ZAMIARZE WSZCZĘCIA KONTROLI SKARBOWEJ**. Treść wiadomości informuje o rzekomej kontroli skarbowej, jednak tekst ma sporo błędów.

### Wiadomość spam:

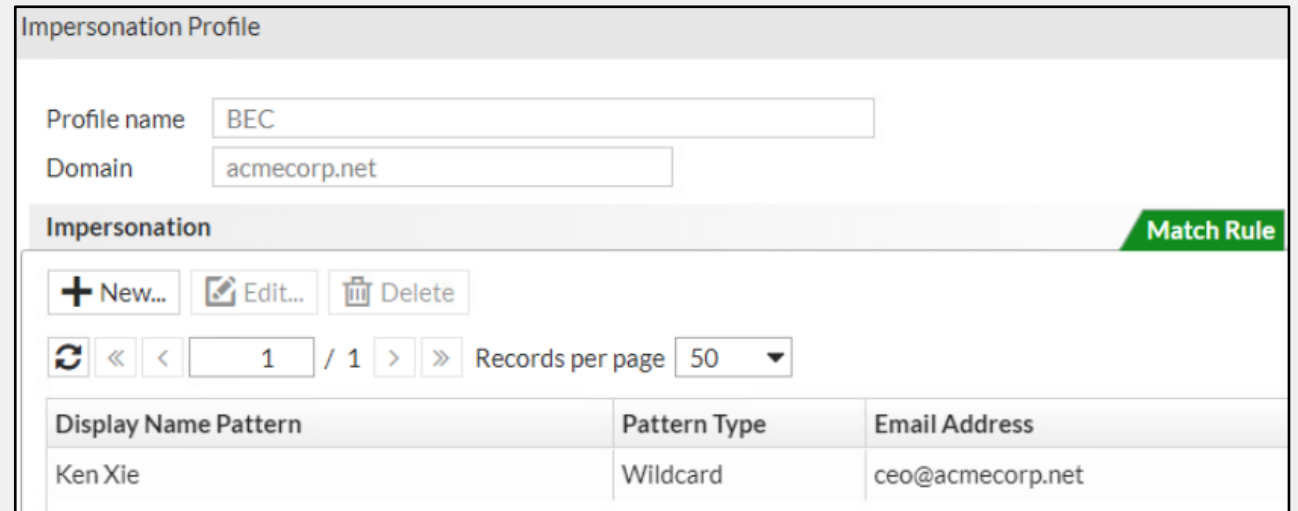


Wiadomość zawiera załącznik o nazwie **dokumenty.tar**. Po rozpakowaniu archiwum otrzymujemy złośliwy skrypt VBS o nazwie **dokumenty\_100780911.vbs**.



# Impersonation Analysis

- Impersonation analysis is part of a FortiMail antispam profile
- Prevents whaling attacks where the email of a company executive is spoofed by mapping a display name to the correct email address
- Two types of mapping:
  - Manual: Manually entering entries and creating impersonation analysis profiles
  - Dynamic: FortiMail learns entries dynamically using the mail statistics service
- The default mapping type is manual



Impersonation Profile

Profile name

Domain

Impersonation Match Rule

[+ New...](#) [Edit...](#) [Delete](#)

[Refresh](#) [<<](#) [<](#)  / 1 [>](#) [>>](#) Records per page

Display Name Pattern	Pattern Type	Email Address
Ken Xie	Wildcard	ceo@acmecorp.net

# Targeted Attack Prevention

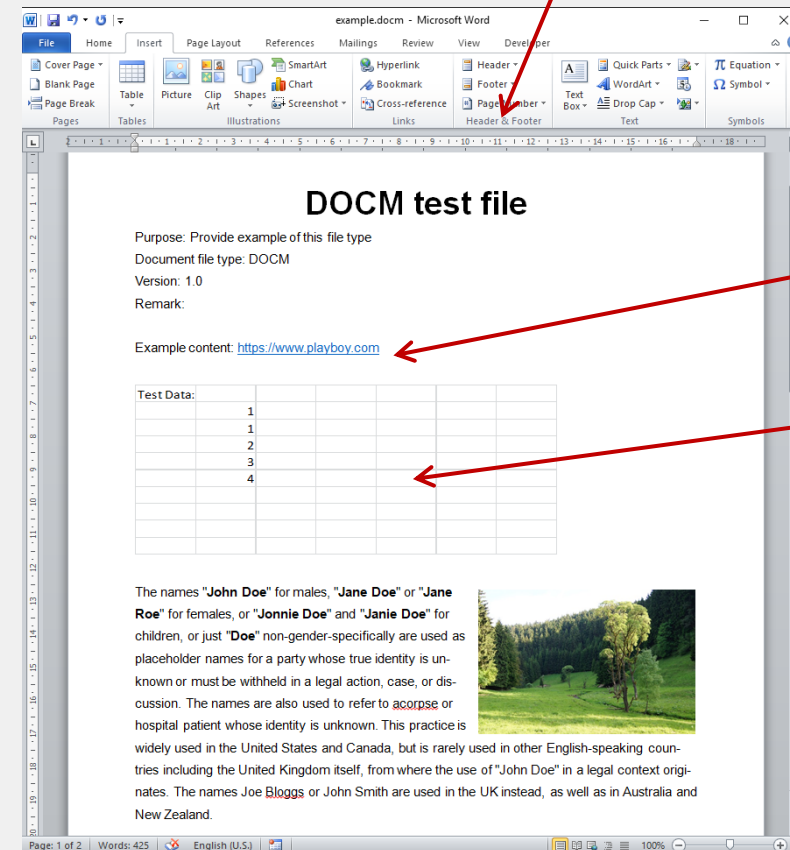
- **Content Disarm & Reconstruction**

- Select URI category to strip when disarming HTML
- Select a URL filter to selectively disarm URLs in CDR

- **Password Decrypt Office Docs**

- Password decryption of archives, PDF and Office documents
- Passwords automatically identified
  - Common password list
  - Admin defined password list
  - Detect passwords in email body

Remove macros



Neutralize URLs

Remove embedded content





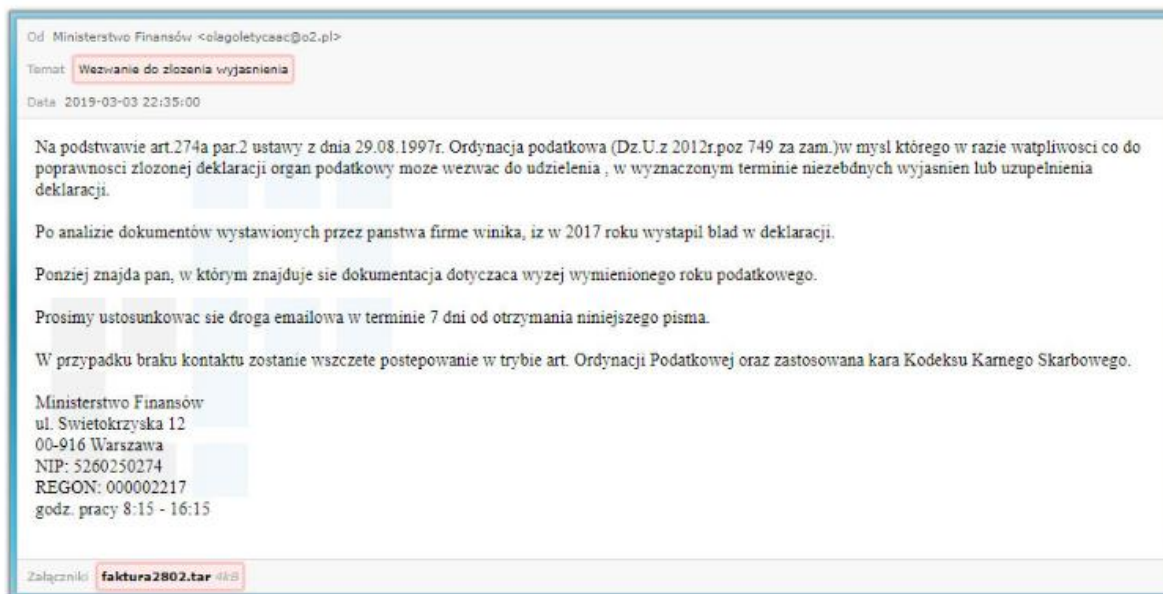
MALWARE

## Kolejna duża kampania spamowa. Zobacz co mogło trafić do Twojej skrzynki!

PREBYTES SECURITY INCIDENT RESPONSE TEAM · 7 MIESIĘCY TEMU · 3 MIN READ

Od początku tygodnia obserwujemy dużą kampanię spamową. Cyberprzestępcy rozsyłają wiadomości spam o różnych tematach i treści. Wiadomości podszywają się pod popularne firmy oraz instytucje, m.in. **Ministerstwo Finansów, ZUS, TAX CARE, PZU, Play, Castoramę.**

Poniżej znajduje się przykładowa wiadomość spam podszywająca się pod Ministerstwo Finansów. Wiadomość zawiera załącznik o nazwie **faktura2802.tar**



**FORTINET®**