Mohou pokročilé hrozby ovlivnit digitální transformaci e-governmentu?

Horymír Šíma, Fortinet
Fortinet is among the top 5 public cybersecurity companies in the world. Its broad portfolio of solutions spans Network, Infrastructure, Cloud, and IoT Security.
We Lead The Industry in Innovation

We are the #1 Security Innovator.
Competitor data based on patents issued as listed by the U.S. Patent and Trademark Office.

- **Fortinet**: 596 Global Patents
- **Palo Alto Networks**: 155
- **FireEye**: 167
- **SonicWall**: 165
- **Sophos**: 78
- **Check Point**: 74
- **WatchGuard**: 51
- **Barracuda**: 46

<table>
<thead>
<tr>
<th>Patents</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Patents</td>
<td>566</td>
</tr>
<tr>
<td>International Patents</td>
<td>30</td>
</tr>
<tr>
<td>Global Patents</td>
<td>596</td>
</tr>
</tbody>
</table>
Jaká kybernetická rizika digitální transformace dnes hrozí?

Aktuální hrozby pro e-government.
## Changes in Cyber Since 2007

<table>
<thead>
<tr>
<th>Category</th>
<th>2007</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Actors</td>
<td>&lt;50</td>
<td>&gt;1,000</td>
</tr>
<tr>
<td>Threat Types</td>
<td>&lt;50</td>
<td>&gt;1,000,000</td>
</tr>
<tr>
<td>Alerts/Day (Average Per Firm)</td>
<td>&lt;1,000</td>
<td>&gt;1,000,000</td>
</tr>
<tr>
<td>Security Vendors</td>
<td>&lt;100</td>
<td>&gt;2,300</td>
</tr>
<tr>
<td>VC Investments</td>
<td>&lt;$500M</td>
<td>&gt;$6B</td>
</tr>
<tr>
<td>Security Spending</td>
<td>&lt;$3B</td>
<td>&gt;$80B</td>
</tr>
</tbody>
</table>
Existing approaches are not working…

• Missing basics due to complexity
• Cyber is complex is growing
• IT teams are overwhelmed
• Perimeters are disappearing
• Determined threat actors can break anything
• IT teams are missing security basics
• Less awareness and control
• Make complexity work for us
Kde bezpečnostní technologie obvykle neuspějí?

Představení funkčního systému pro optimální ochranu proti kybernetickým hrozbám (zejména pro ty, kteří ho ještě nemají nebo nevyužívají naplno).
Fortinet Security Fabric

BROAD
Visibility of the entire digital attack surface

INTEGRATED
AI-driven breach prevention across devices, networks, and applications

AUTOMATED
Operations, orchestration, and response
The Broadest Security Portfolio in the Industry

Network Security
- FortiGate
- FortiGate Enterprise Firewall
- IPS
- SD-WAN
- SWG
- VPN

Open Ecosystem
- Partner API
- DevOps
- Connectors

Multi-Cloud Security
- FortiGate Virtual Firewall
- FortiGate Cloud Firewall

Endpoint Security
- FortiClient

Email Security
- FortiMail

Web Application Security
- FortiWeb

Secure Unified Access
- FortiAP

Advanced Threat Protection
- FortiSandbox

Management & Analytics
- FortiAnalyzer
- FortiManager
- FortiSEM

Advanced Threat Protection
- FortiSandbox

Secure Unified Access
- FortiAP

Management & Analytics
- FortiAnalyzer
- FortiManager
- FortiSEM

Open Ecosystem
- Partner API
- DevOps
- Connectors

Network Security
- FortiGate
- FortiGate Enterprise Firewall
- IPS
- SD-WAN
- SWG
- VPN

End-to-End Security
- FortiGate
- FortiGate Enterprise Firewall
- IPS
- SD-WAN
- SWG
- VPN

Multi-Cloud Security
- FortiGate Virtual Firewall
- FortiGate Cloud Firewall

Open Ecosystem
- Partner API
- DevOps
- Connectors

Endpoint Security
- FortiClient

Email Security
- FortiMail

Web Application Security
- FortiWeb

Secure Unified Access
- FortiAP

Management & Analytics
- FortiAnalyzer
- FortiManager
- FortiSEM

Fortinet Inc. All Rights Reserved.
# Fabric-Ready Ecosystem Partners
Expand the Reach of the Fabric

<table>
<thead>
<tr>
<th>MANAGEMENT</th>
<th>ENDPOINT</th>
<th>CLOUD/NFV/SDN</th>
<th>VULNERABILITY/SIEM</th>
<th>TECHNOLOGY</th>
<th>IOT/OT/NAC/IDENTITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>algosec</td>
<td>McAfee</td>
<td>aws</td>
<td>qualys</td>
<td>Centrify</td>
<td></td>
</tr>
<tr>
<td>servicenow</td>
<td>Attivo Networks</td>
<td>azure</td>
<td>ibm security</td>
<td>nozomi</td>
<td>cyberark</td>
</tr>
<tr>
<td>ARISTA</td>
<td>Carbon Black</td>
<td>google cloud</td>
<td>Micro Focus</td>
<td>ADVA</td>
<td>Rad</td>
</tr>
<tr>
<td>tufin</td>
<td>Symantec</td>
<td>vmware</td>
<td>WhiteHat Security</td>
<td>Intel</td>
<td>ForeScout</td>
</tr>
<tr>
<td>cybrary</td>
<td>euglass</td>
<td>nuagen networks</td>
<td>Splunk</td>
<td>ribbon</td>
<td>Pulse Secure</td>
</tr>
<tr>
<td>Cyber Observer</td>
<td>Hughes</td>
<td>NEC</td>
<td>IBM</td>
<td>Communications</td>
<td></td>
</tr>
<tr>
<td>Phantom</td>
<td>SentinelOne</td>
<td>CISCO</td>
<td>Micro Focus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIORE Mono</td>
<td>ziften</td>
<td>Brocade</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BACKBOX</td>
<td></td>
<td>Hewlett Packard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rubrik</td>
<td></td>
<td>Enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSPi</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Fortinet Inc. All Rights Reserved.
Co můžeme udělat více než aplikovat sandboxing?

Mohou uživatelé využívat Internet opravdu bezpečně?
Forti Deceptor *in DMZ mode*
Forti Deceptor

WHY USER NEEDS FORTIDECEPTOR

- Traditional defenses cannot defend a perimeter with 100% certainty. It’s not a question that if your network can be compromised or not, but when and how frequently.

- Challenges of current internal network protections
  - FACTS: Under 4% of alerts are investigated. Users receive overwhelming alerts every day, with a lot of FP
  - FACTS: Hackers use legitimate tools and tokens to do lateral movement which are always white listed
  - FACTS: On average, an ATP attack is discovered after 7 months after initial breach. Hackers spend 80% of their time at lateral movement step

- Customer needs a way to detect hackers existence in a fast and accurate way.

- FortiDeceptor (FDC) considers from hacker’s point of view and methodology to create decoys and tokens and mix them within existing IT resources to lure hackers to engage during their lateral movement

- Alerts are almost 100% accurate without FP. Any party that seeks to identify, ping, enter or utilizes a decoy is immediately identified

- It can integrate with other product to kill attacks quickly

1. Phishing and Zero day attack
2. Back door
3. Lateral movement
4. Data gathering
5. Exfiltrate
A handful of users are targeted by two phishing attacks; one user opens Zero day payload (CVE-02011-0609)
The user machine is accessed remotely by Poison Ivy tool
Attacker elevates access to important user, service and admin accounts, and specific systems
Data is acquired from target servers and staged for exfiltration
Data is exfiltrated via encrypted files over FTP to external, compromised machine at a hosting provider
# Forti Deceptor

## FortiDeceptor Highlights

### Deceive
- Utilize deception technology
- Manage, update, view and scale decoys and deception tokens at a centralized location
- Auto detect user’s production network; setup deception hosts and install decoys to allure hackers to engage
- Deception VMs and decoys are real OS, high-interaction and appear indistinguishable from real IT assets

### Expose
- Detect, trace and correlate hacker’s lateral movement
- Sys Admin is notified immediately of network compromise through Web UI, Email, SNMP traps and logs
- Provide detailed forensic information of hacker’s lateral movements and activities
- Further analysis of dropped payload with FortiSandbox technology

### Eliminate
- Increase hacker’s cost
- Redirect hacker’s attack to deception hosts from production servers
- Quarantine infected endpoints and stop connection to C&C servers to break the kill chain
- Slow down ransomeware’s infection by generating endless fake documents on protected endpoint

### Fabric
- Integrate with FortiGate, FortiSwitch, EMS/FortiClient and 3rd party products to stop the kill chain
- Work with FortiSIEM for faster detection
- Generate IOC
Forti ISOLATOR

Product Summary

- Clientless remote browser isolation
  - Works with any modern HTML5 capable browser

- Mitigate against web based threats whilst retaining productivity
  - No server side code runs on the local machine
  - Browser session runs in clean remote container
  - Rendered page image displayed to client
  - Supports web page interactivity e.g. links, forms, video, audio
Forti ISOLATOR

Fortilsolator
Product Summary

Web

Email

Gmail

Proxy

Malicious Web Page

User Input Events

Safely Rendered Visual Information

User Cookie Persistence

FETCH
EXECUTE
RENDER

FETCH
EXECUTE
RENDER

FETCH
EXECUTE
RENDER

Browser reset to known clean state for each new session

© Fortinet Inc. All Rights Reserved.
Forti ISOLATOR