Mohou pokročilé hrozby ovlivnit digitální transformaci e-governmentu?

Horymír Šíma, Fortinet

Network Security Leader

Fortinet is among the top 5 public cybersecurity companies in the world.

Its broad portfolio of solutions spans Network, Infrastructure, Cloud, and IoT Security.

$12B Mkt Cap

~$1.8B - 2018
(revenue)

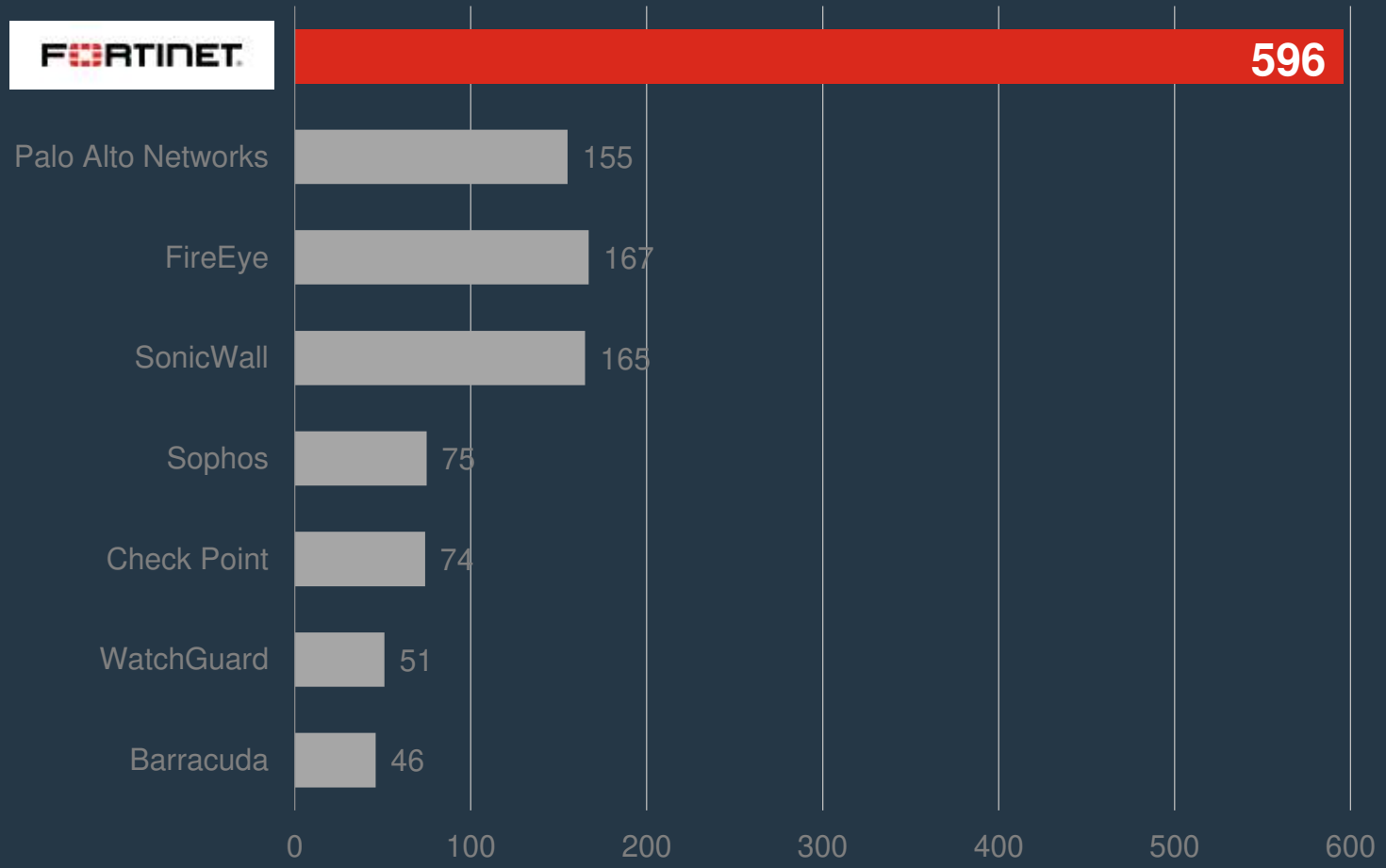
385,000+ Customers

4.4M+ Appliances Shipments Worldwide
(+30% units WW)

** As of Sept 30th 2018*

FORTINET

We Lead The Industry in Innovation



#1 Security Innovator

Competitor data based on patents issued as listed by the U.S. Patent and Trademark Office

566	U.S. Patents
30	International Patents
596	**Global Patents**

FORTINET

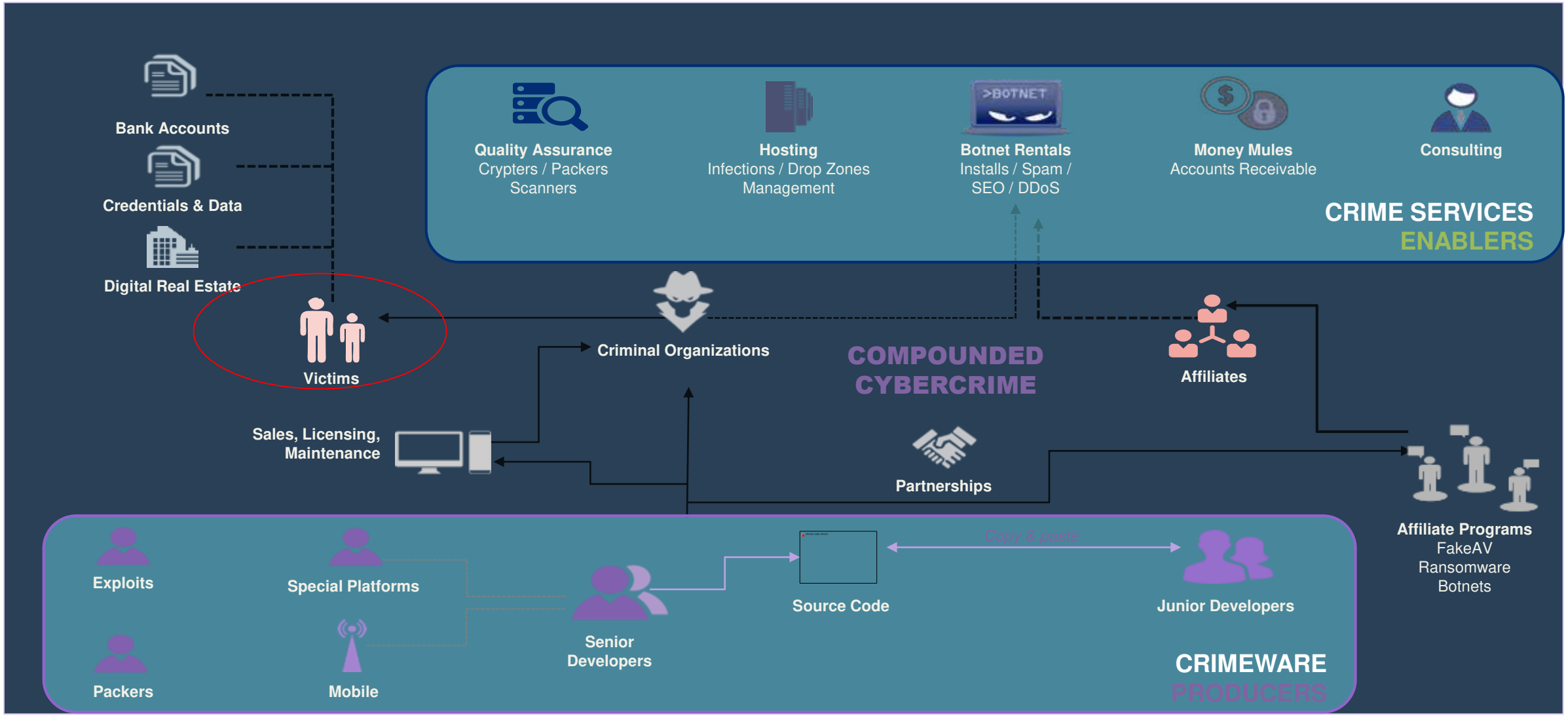
Jaká kybernetická rizika digitální transformace dnes hrozí?

Aktuální hrozby pro e-government.

Changes in Cyber Since 2007

	2007	2017
Threat Actors	<50	>1,000
Threat Types	<50	>1,000,000
Alerts/Day (Average Per Firm)	<1,000	>1,000,000
Security Vendors	<100	>2,300
VC Investments	<$500M	>$6B
Security Spending	<$3B	>$80B

Cybercrime Marketplace Ecosystem



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?

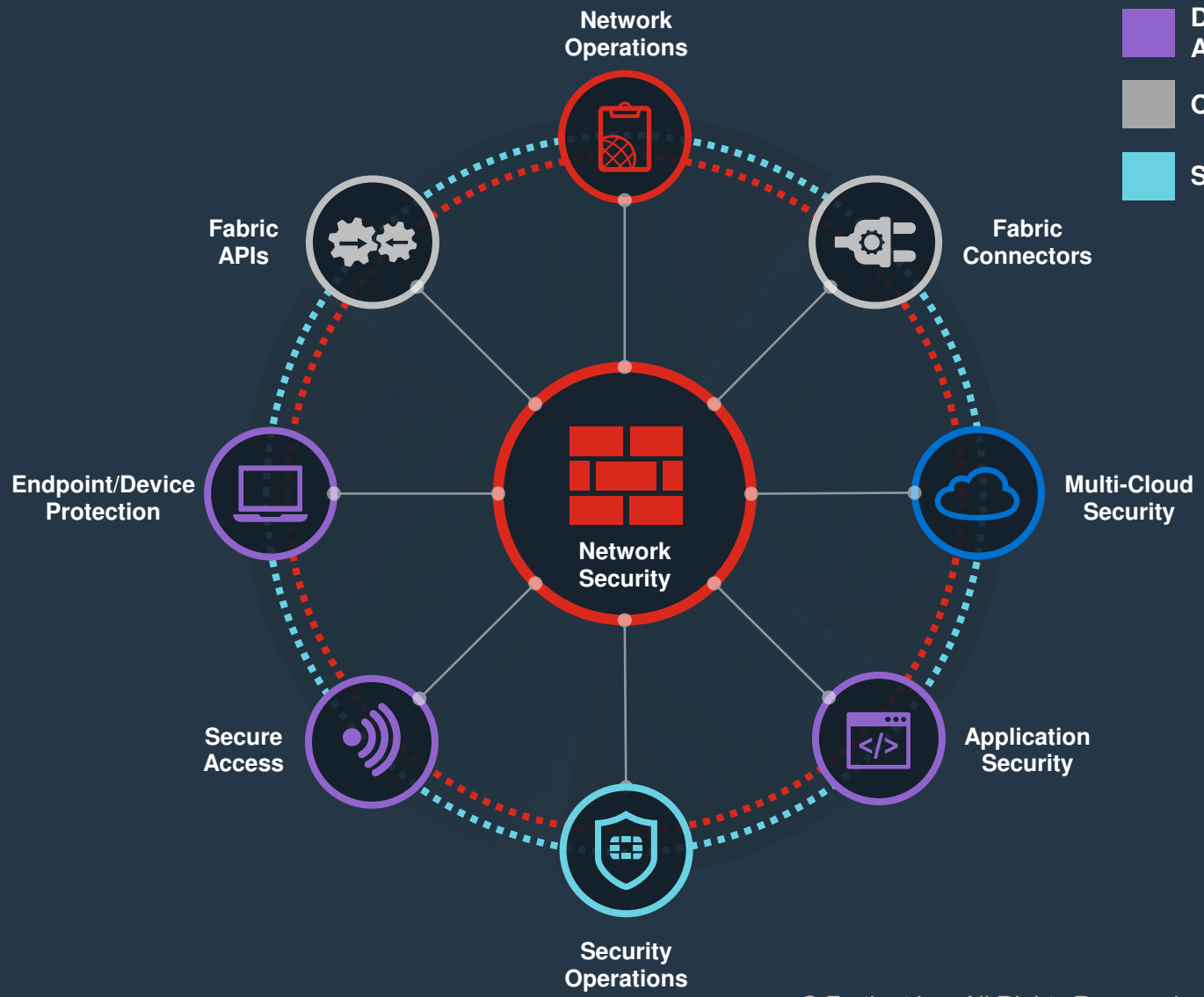
Představení funkčního systému pro optimální ochranu proti kybernetickým hrozbám (zejména pro ty, kteří ho ještě nemají nebo nevyužívají naplno).

Fortinet Security Fabric

BROAD
Visibility of the entire digital attack surface

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

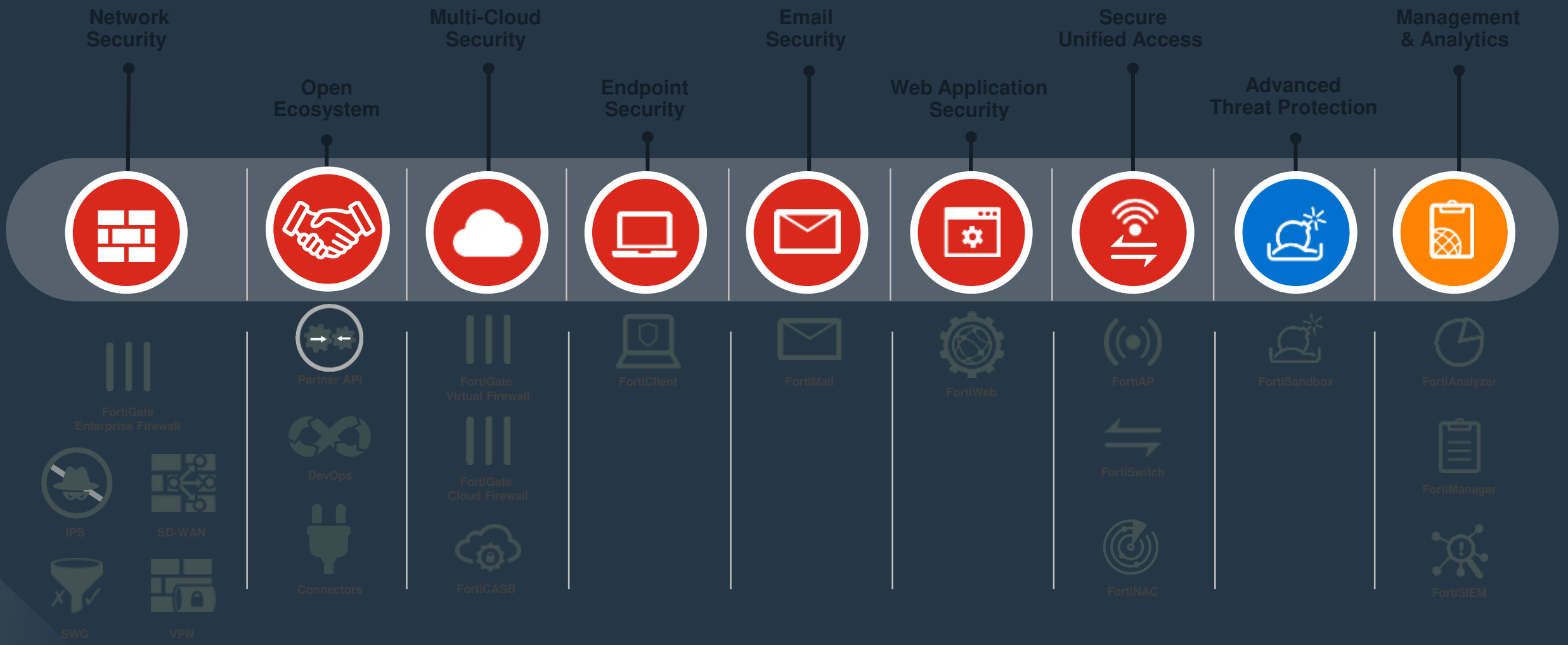
AUTOMATED
Operations, orchestration, and response



FORTINET

Q1FY19 v1.4.4

The Broadest Security Portfolio in the Industry



FORTINET

Fabric-Ready Ecosystem Partners Expand the Reach of the Fabric

MANAGEMENT

algosec, ARISTA, servicenow, tufin, cyber OBSERVER, cyglass, Phantom, HUGHES, FIREMON, BACKBOX, rubrik, CSPi

ENDPOINT

McAfee Together is power., Attivo NETWORKS, CARBON BLACK ARM YOUR ENDPOINTS, SentinelOne, Symantec., ziften

CLOUD/NFV/SDN

aws, Azure, Google Cloud, vmware, IBM Cloud, ORACLE, cisco, amdocs, NEC, BROCADE, Ubiqube, nuagenetworks, CLOUDIFY, silver peak, Hewlett Packard Enterprise

VULNERABILITY/SIEM

QUALYS, IBM Security, WhiteHat SECURITY, MICRO FOCUS, splunk>

TECHNOLOGY

ADVA Optical Networking, intel, ribbon communications, VERISIGN

IOT/OT/NAC/IDENTITY

Centrify, CYBERARK, NOZOMI NETWORKS, CLAROTY, ForeScout, RAD, Pulse Secure

Fabric APIs

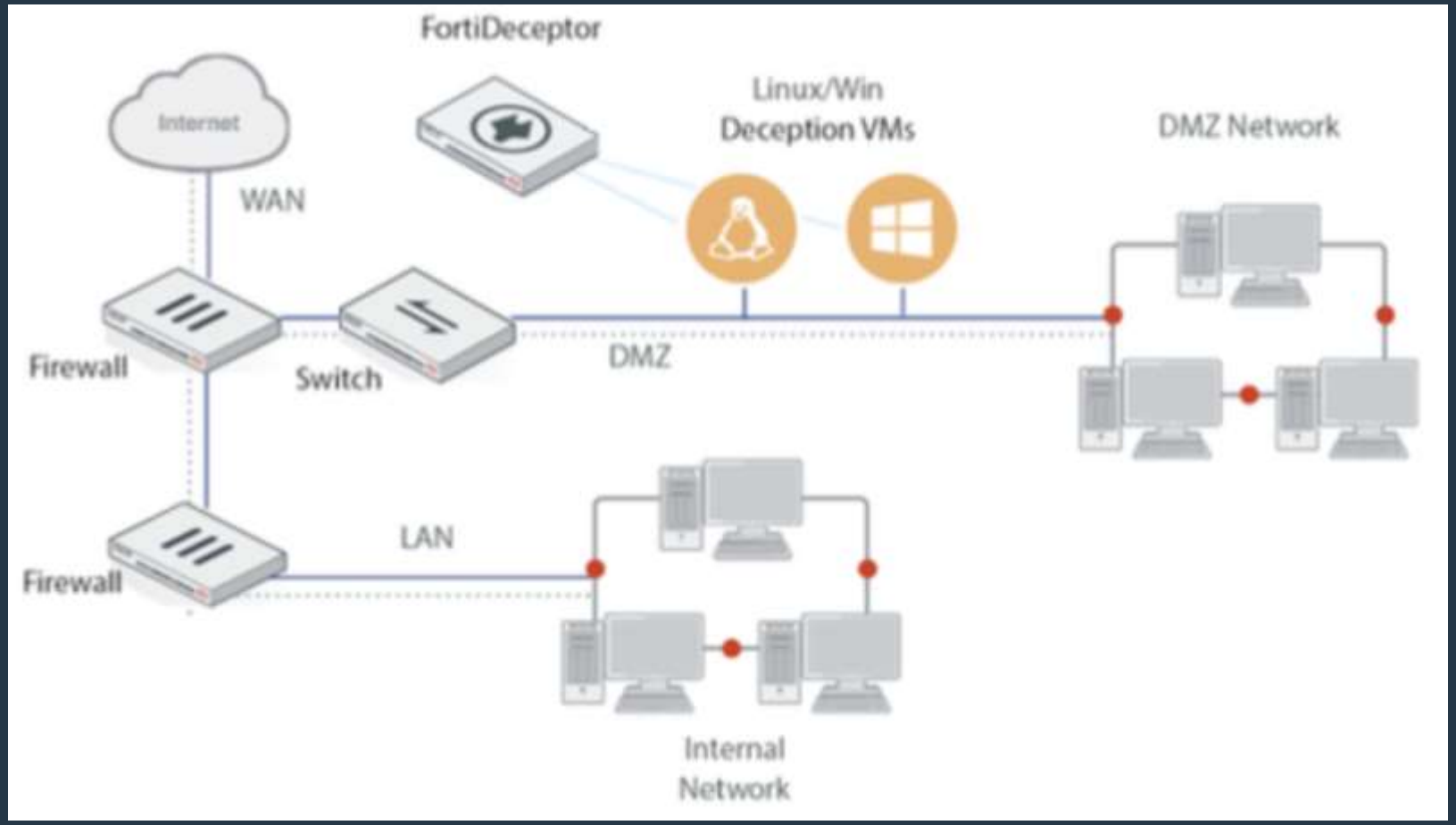
Fabric Connectors

FORTINET

Co můžeme udělat více než aplikovat sandboxing?

Mohou uživatelé využívat Internet opravdu bezpečně?

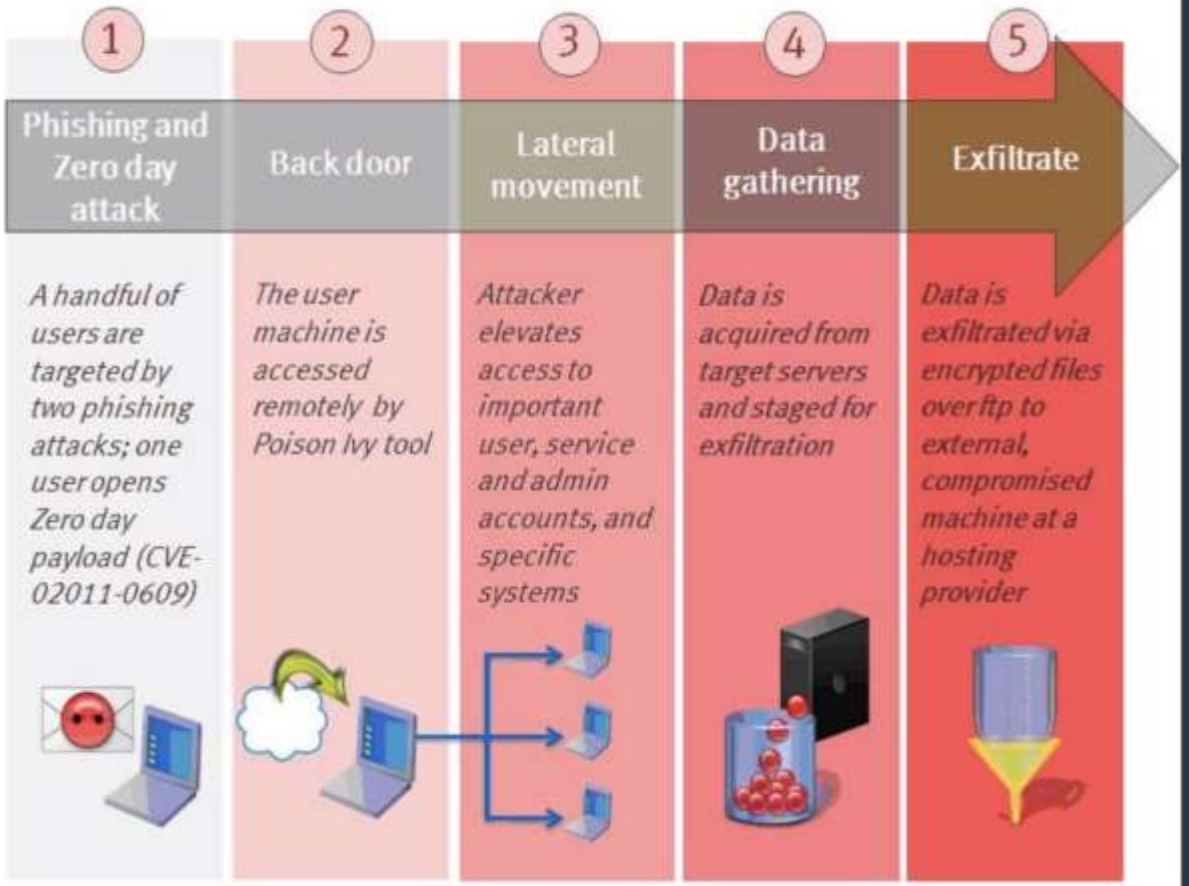
Forti Deceptor *in DMZ mode*



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 receives 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



Forti Deceptor

FORTIDECEPTOR HIGHLIGHTS

DECEIVE

- Utilize deception technology
- Manage, update, view and scale decoys and deception tokens at a centralize 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

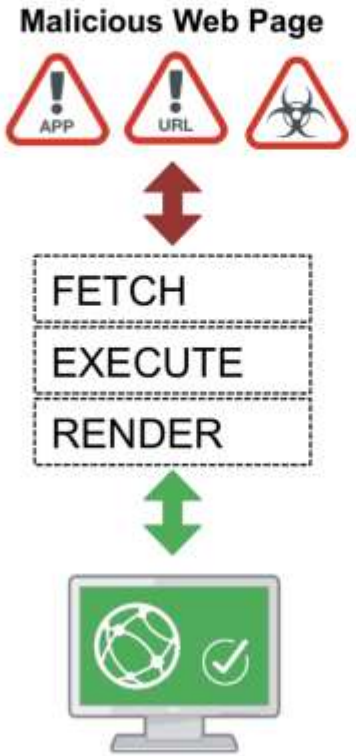
FABRIC

- 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

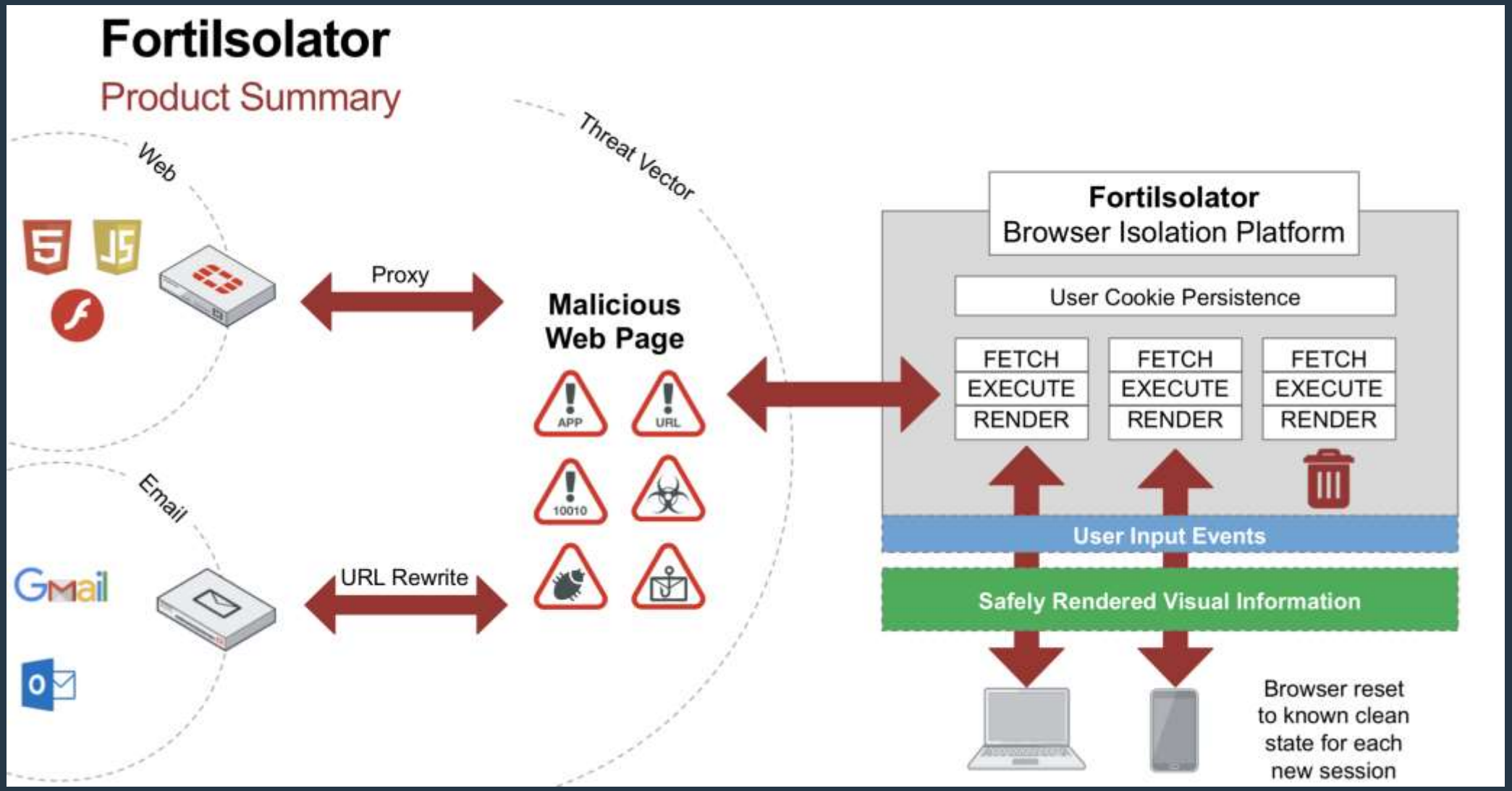
FortiIsolator

Product Summary



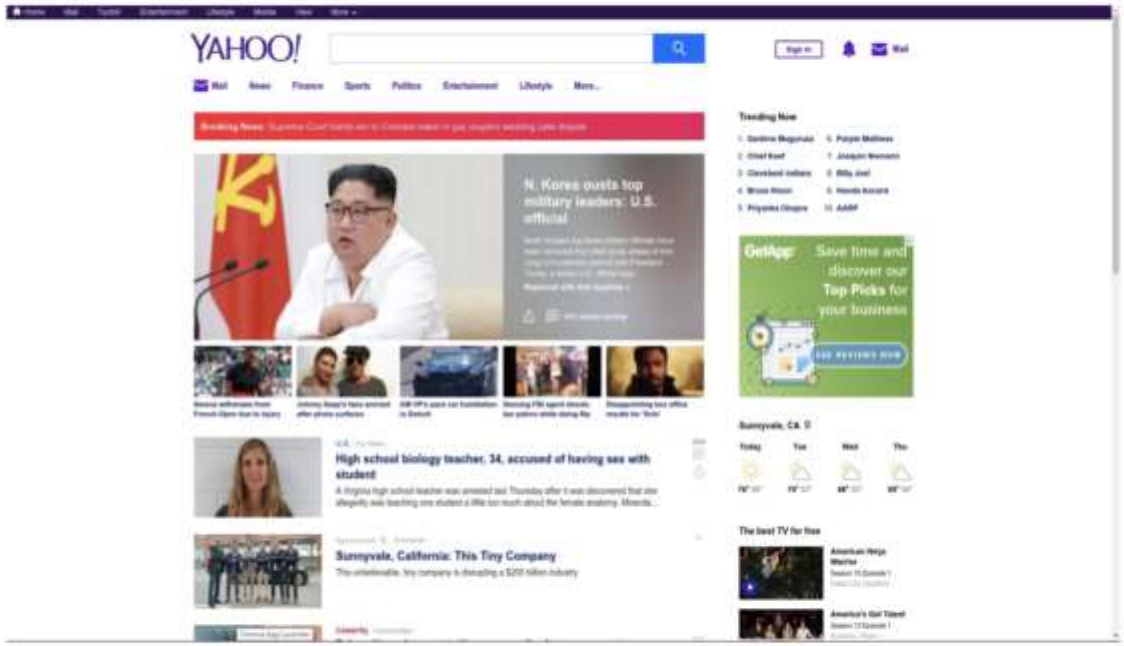
- Clientless remote browser isolation
  - » Works with any modern HTML5 capable browser
- Mitigate against web based threats whilst retaining productivity
  - » No server side code runs on the local machine
  - » Browser session runs in clean remote container
  - » Rendered page image displayed to client
  - » Supports web page interactivity e.g. links, forms, video, audio

Forti ISOLATOR

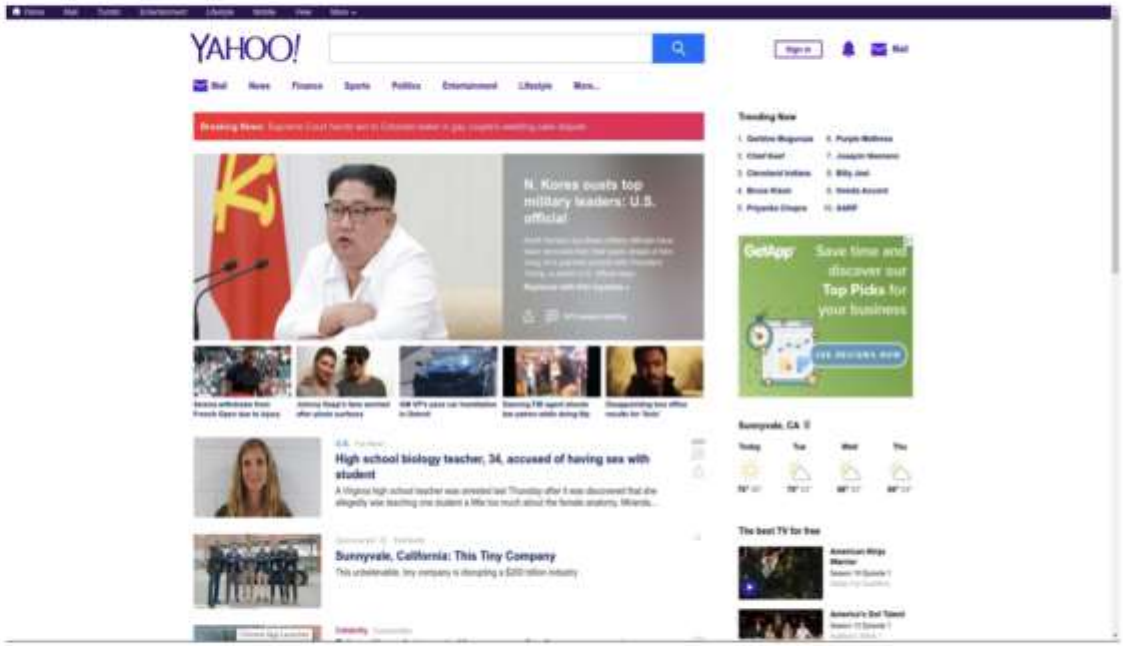


Forti ISOLATOR

Direct Access



FortiIsolator



Forti ISOLATOR

Direct Access

```html
<!DOCTYPE html>
<html id="atomic" lang="en-US" class="atomic my3columns ua-wk ua-win ua-10.0 ua-wk537  l-out Pos-r
https fp fp-v2 rc1 fp-default mini-uh-on viewer-right two-col ntk-wide ltr desktop Desktop bkt201
JsEnabled jsenabled Billboard hide-Adnorth  css-filters yui3-js-enabled stencil-js stencil-canvas
stencil-no-touch stencil-csstransforms3d stencil-csstransitions stencil-svg stencil-fullscreen
stencil-no-overflowscrolling stencil-plugin-sticker stencil-plugin-imageloader stencil-plugin-
selectbox stencil-plugin-source stencil-plugin-tooltip stencil-plugin-fx stencil-plugin-toggle Sticky-
off">
  ▶<head>…</head>
  ▼<body class="my3columns ua-wk ua-win ua-10.0 ua-wk537 l-out Pos-r https fp fp-v2 rc1 fp-default
  mini-uh-on viewer-right two-col ntk-wide ltr stream-dense rspblbrd-ad display-push-promos" dir="ltr"
  id="yui_3_18_0_3_1528123324224_104">
    ▶<iframe width="0" height="0" name="__cmpLocator" style="display: none;">…</iframe>
     <noscript></noscript>
    ▶<div id="darla-assets-js-top">…</div>
    ▶<script type="text/javascript">…</script>
    ▶<div id="UH">…</div>
     <!-- Header -->
    ▶<div id="Stencil">…</div>
…   ▶<div id="Masterwrap" class="slider js-viewer-pagewrapper">…</div> == $0
    ▶<div id="darla-assets-bottom">…</div>
     <input type="hidden" id="afhistorystate">
     <script type="text/javascript" src="https://mbp.yimg.com/sy/zz/combo?yui:/3.18.0/yui/yui-
     min.js"></script>
    ▶<div id="darla_csc_holder" class="darla" style="display: none;">…</div>
     <div id="yui3-css-stamp" style="position: absolute !important; visibility: hidden !important"
     class></div>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/ss/rapid-3.42.4.js"></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/aperollup-min-
     8e0fae4b_desktop_advance.js"></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-stream-atomic-
     2.0.1607/r-min.js" async defer></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-mega-header-
     1.0.672/r-min.js" async defer></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-viewer-0.1.2757/
     r-min.js" async defer></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-specialevent-
     0.0.52/r-min.js" async defer></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-amplify-hoset-
     1.0.30/r-min.js" async defer></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-breakingnews-
     atomic-0.0.58/r-min.js" async defer></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-yahooview-
     0.0.20/r-min.js" async defer></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-astro-atomic-
     0.0.21/r-min.js" async defer></script>
     <script type="text/javascript" src="https://mbp.yimg.com/sy/os/mit/td/td-applet-portfolios-
     0.1.503/r-min.js" async defer></script>
    ▶<script>…</script>
```

FortiIsolator

```html
<!DOCTYPE html>
<html style="overflow: hidden;">
▶<head>…</head>
▼<body>
  ▶<script>…</script>
…   <canvas id="mainCanvas" width="1008" height="984" style="cursor: default;"> == $0
    <canvas id="popupCanvas">
    <span style="border-radius: 3px; text-indent: 20px; width: auto; padding: 0px 4px 0px 0px; text-
    align: center; font-style: normal; font-variant: normal; font-weight: bold; font-stretch: normal;
    font-size: 11px; line-height: 20px; font-family: "Helvetica Neue", Helvetica, sans-serif; color:
    rgb(255, 255, 255); background: url("data:image/svg+xml;
    base64,PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIGhlaWdodD0iMzBweCIgd2lkdGg9IjMwcHgiIHZp
    ZXdCb3g9Ii0xIC0xIDMxIDMxIj48Zz48cGF0aCBkPSJNMjkuNDQ5LDE0LjY2MiBDMjkuNDQ5LDIyLjcyMiAyMi44NjgsMjkuMjU
    2IDE0Ljc1LDI5LjI1NiBDNi42MzIsMjkuMjU2IDAuMDUxLDIyLjcyMiAwLjA1MSwxNC42NjIgQzAuMDUxLDYuNjAxIDYuNjMyLD
    AuMDY3IDE0Ljc1LDAuMDY3IEMyMi44NjgsMC4wNjcgMjkuNDQ5LDYuNjAxIDI5LjQ0OSwxNC42NjIiIGZpbGw9IiNmZmYiIHN0c
    m9rZT0iI2ZmZiIgc3Ryb2tlLXdpZHRoPSIxIj48L3BhdGg+PHBhdGggZD0iTTE0LjczMywxLjY4NiBDNy41MTYsMS42ODYgMS42
    NjUsNy40OTUgMS42NjUsMTQuNjYyIEMxLjY2NSwyMC4xNTkgNS4xMDksMjQuODU0IDkuOTcsMjYuNzQ0IEM5Ljg1NiwyNS43MTg
    gOS43NTMsMjQuMTQzIDEwLjAxNiwyMy4wMjIgQzEwLjI1MywyMi4wMSAxMS41NDgsMTYuNTcyIDExLjU0OCwxNi41NzIgQzExLj
    U0OCwxNi41NzIgMTEuMTU3LDE1Ljc5NSAxMS4xNTcsMTQuNjQ2IEMxMS4xNTcsMTIuODQyIDEyLjIxMSwxMS40OTUgMTMuNTIyL
    DExLjQ5NSBDMTQuNjM3LDExLjQ5NSAxNS4xNzUsMTIuMzI2IDE1LjE3NSwxMy4zMjMgQzE1LjE3NSwxNC40MzYgMTQuNDYyLDE2
    LjEgMTQuMDkzLDE3LjY0MyBDMTMuNzg1LDE4LjkzNSAxNC43NDUsMTkuOTg4IDE2LjAyOCwxOS45ODggQzE4LjM1MSwxOS45ODg
    gMjAuMTM2LDE3LjU1NiAyMC4xMzYsMTQuMDQ2IEMyMC4xMzYsMTAuOTM5IDE3Ljg4OCw4Ljc2NyAxNC42NzgsOC43NjcgQzEwLj
    k1OSw4Ljc2NyA4Ljc3NywxMS41MzYgOC43NzcsMTQuMzk4IEM4Ljc3NywxNS41MTMgOS4yMSwxNi43MDkgOS43NDksMTcuMzU5I
    EM5Ljg1NiwxNy40ODggOS44NzIsMTcuNiA5Ljg0LDE3LjczMSBDOS43NDEsMTguMTQxIDkuNTIsMTkuMDIzIDkuNDc3LDE5LjIw
    MyBDOS40MiwxOS40NCA5LjI4OCwxOS40OTEgOS4wNCwxOS4zNzYgQzcuNDA4LDE4LjYyMiA2LjM4NywxNi4yNTIgNi4zODcsMTQ
    uMzQ5IEM2LjM4NywxMC4yNTYgOS4zODMsNi40OTcgMTUuMDIyLDYuNDk3IEMxOS41NTUsNi40OTcgMjMuMDc4LDkuNzA1IDIzLj
    A3OCwxMy45OTEgQzIzLjA3OCwxOC40NjMgMjAuMjM5LDIyLjA2MiAxNi4yOTcsMjIuMDYyIEMxNC45NzMsMjIuMDYyIDEzLjcyO
    CwyMS4zNzkgMTMuMzAyLDIwLjU3MiBDMTMuMzAyLDIwLjU3MiAxMi42NDcsMjMuMDUgMTIuNDg4LDIzLjY1NyBDMTIuMTkzLDI0
    Ljc4NCAxMS40OTYsMjYuMTk2IDEwLjg2MywyNy4wNTggQzEyLjA4NiwyNy40MzQgMTMuMzg2LDI3LjYzNyAxNC43MzMsMjcuNjM
    3IEMyMS45NSwyNy42MzcgMjcuODAxLDIxLjgyOCAyNy44MDEsMTQuNjYyIEMyNy44MDEsNy40OTUgMjEuOTUsMS42ODYgMTQuNz
    MzLDEuNjg2IiBmaWxsPSIjYmQwODFjIj48L3BhdGg+PC9nPjwvc3ZnPg==") 3px 50% / 14px 14px no-repeat rgb(189,
    8, 28); position: absolute; opacity: 1; z-index: 8675309; display: none; cursor: pointer; border:
    none; -webkit-font-smoothing: antialiased;">Save</span>
    <span style="width: 24px; height: 24px; background: url("data:image/svg+xml;
    base64,PD94bWwgdmVyc2lvbj0iMS4wIiA/
    Pjxzdmcgd2lkdGg9IjI0cHgiIGhlaWdodD0iMjRweCIgdmlld0JveD0iMCAwIDI0IDI0IiB2ZXJzaW9uPSIxLjEiIHhtbG5zPSJ
    odHRwOi8vd3d3LnczLm9yZy8yMDAwL3N2ZyIgeG1sbnM6eGxpbms9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkveGxpbmsiPjxkZW
    ZzPjxtYXNrIG1kPSJtIj48cmVjdCBmaWxsPSIjZmZmIiB4PSIwIiB5PSIwIiB3aWR0aD0iMjQiIGhlaWdodD0iMjQiIHJ4PSI2I
    iByeT0iNiIvPjxyZWN0IGZpbGw9IiMwMDAiIHg9IjUiIHk9IjUiIHdpZHRoPSIxNCIgaGVpZ2h0PSIxNCIgcng9IjEiIHJ5PSIx
    Ii8+PHJ1Y3QgZmlsbD0iIzAwMCIgeD0iMTAiIHk9IjAiIHdpZHRoPSI0IiBoZWlnaHQ9IjI0Ii8+PHJ1Y3QgZmlsbD0iIzAwMCI
    geD0iMCIgeT0iMTAiIHdpZHRoPSIyNCIgaGVpZ2h0PSI0Ii8+PC9tYXNrPjwvZGVmcz48cmVjdCB4PSIwIiB5PSIwIiB3aWR0aD
    0iMjQiIGhlaWdodD0iMjQiIGZpbGw9IiNmZmYiIG1hc2s9InVybCgjbSkiLz48L3N2Zz4=") 50% 50% / 14px 14px no-
    repeat rgba(0, 0, 0, 0.4); position: absolute; opacity: 1; z-index: 8675309; display: none; cursor:
    pointer; border: none; border-radius: 12px;"></span>
  </body>
</html>
```


FORTINET