Bezpečný svět
Security Fabric

Michal Plíhal

DX

is the integration of digital technology into all areas of a business, resulting in fundamental changes to how businesses operate and how they deliver value to customers.

[Digital Transformation]

FORTINET

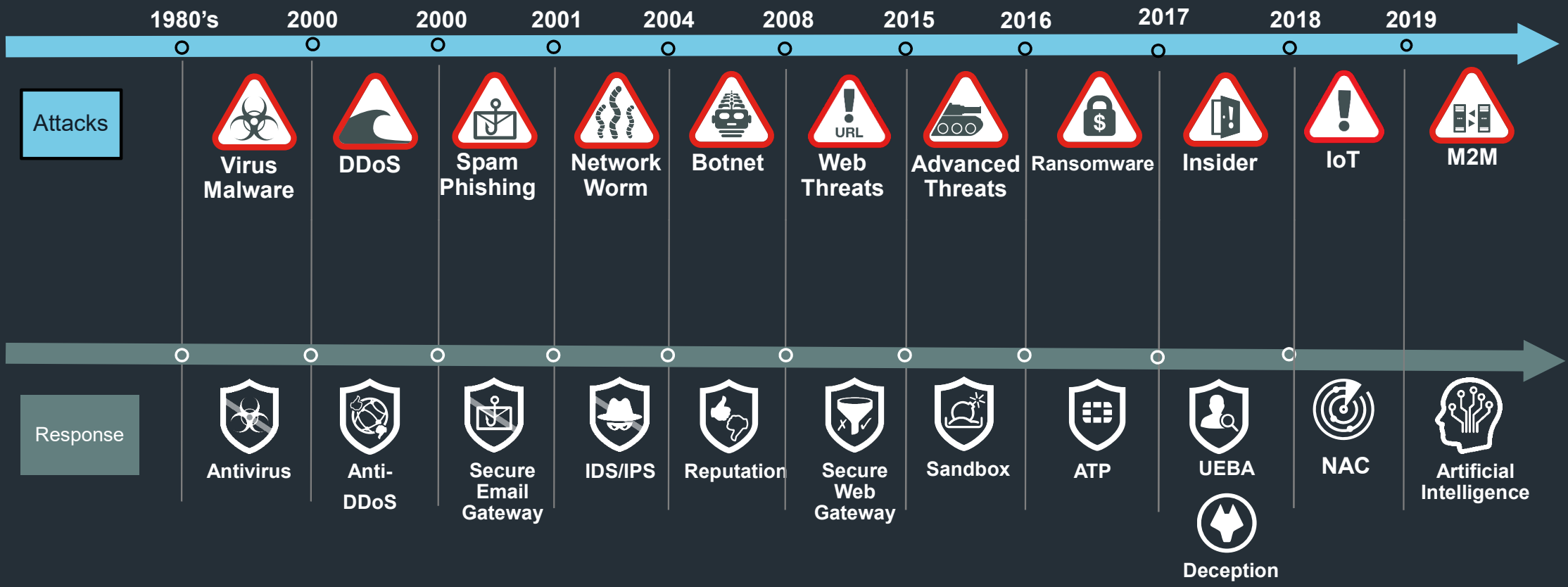
SX

is the integration of security into all areas of digital technology, resulting in a Security Architecture that provides a Continuous Trust Assessment.

[Security Transformation]

The Threat Landscape is Continually Changing

The expanding attack surface creates the opportunity today



Dealing with today's issues…

Areas of Greatest Concern for Security*

1. Cloud
2. Vulnerability in IT systems
3. Inside Threats
4. BYOD
5. IoT

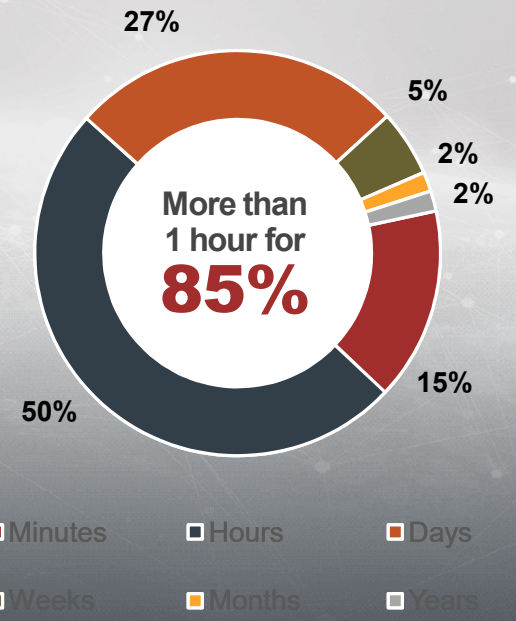
51%

OF ENTERPRISES BREACHED IN THE LAST 12 MONTHS*

3bn

NEW DEVICES PER YEAR THROUGH 2020

Time to Detect Breach*



FORTINET

* Source: Fortinet-sponsored Lightspeed GMI survey

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 3.0

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE)
A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení. stávajících souborů nebo změn konfigurace.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY),
včetně dynamických a jiných domén poskytovaných zdarma anonymním uživatelům internetu.

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ
z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHOZÍ E-MAILY
pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

FORTINET

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 3.0

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace. Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBU
prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

VYUŽIJTE APLIKAČNÍ FIREWALL
k blokování komunikace jiných než povolených aplikací (whitelisting) a blokování nestandardního provozu. V případě koncových stanic blokujte také spojení iniciovaná jinou stranou.

KONTROLUJTE POUŽÍVANÉ CERTIFIKÁTY
především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY
aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN
pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malé procento škodlivých domén.

NASAĎTE ANTI-DDOS TECHNOLOGIE,
které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasaďte na kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)
a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.

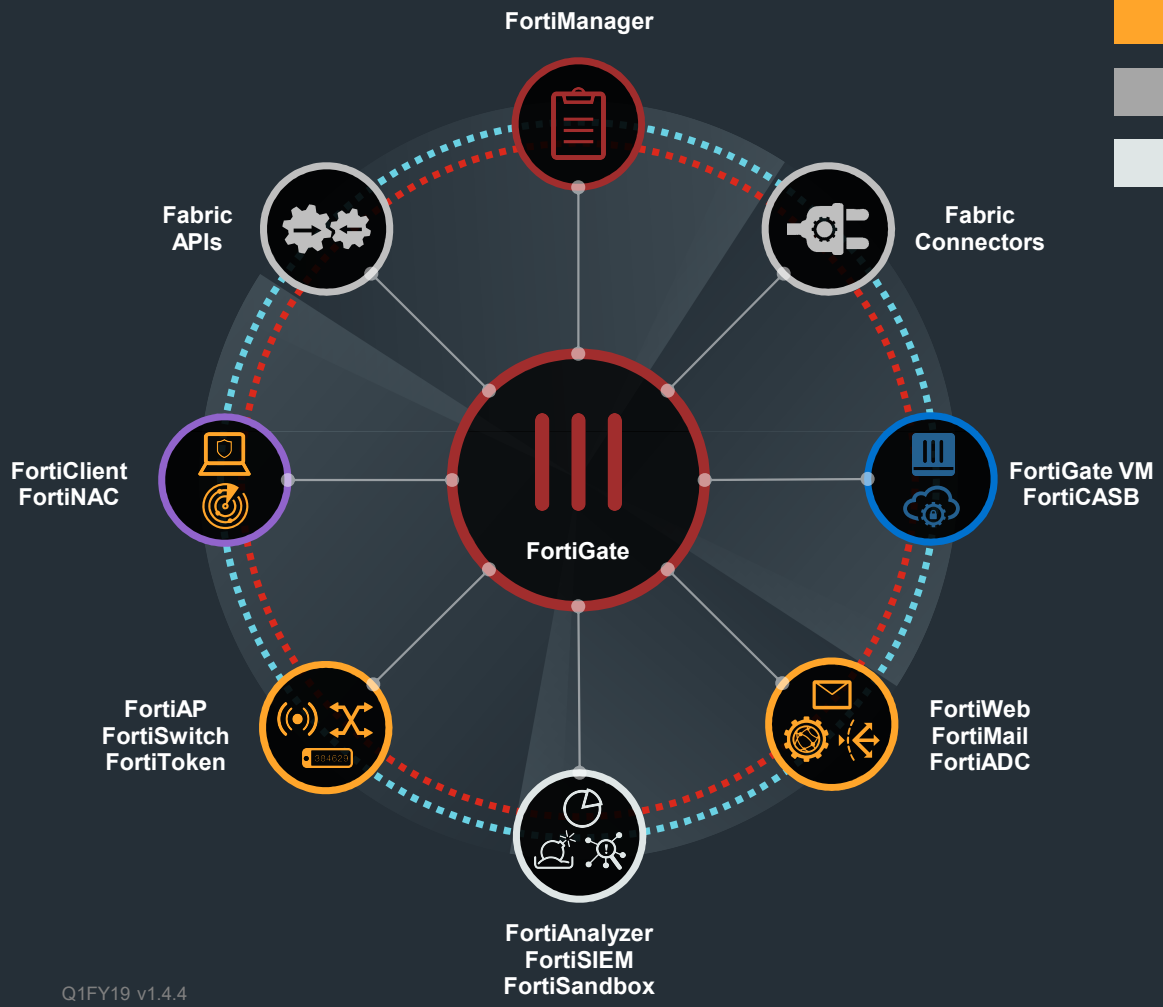
FORTINET

Fortinet Security Fabric

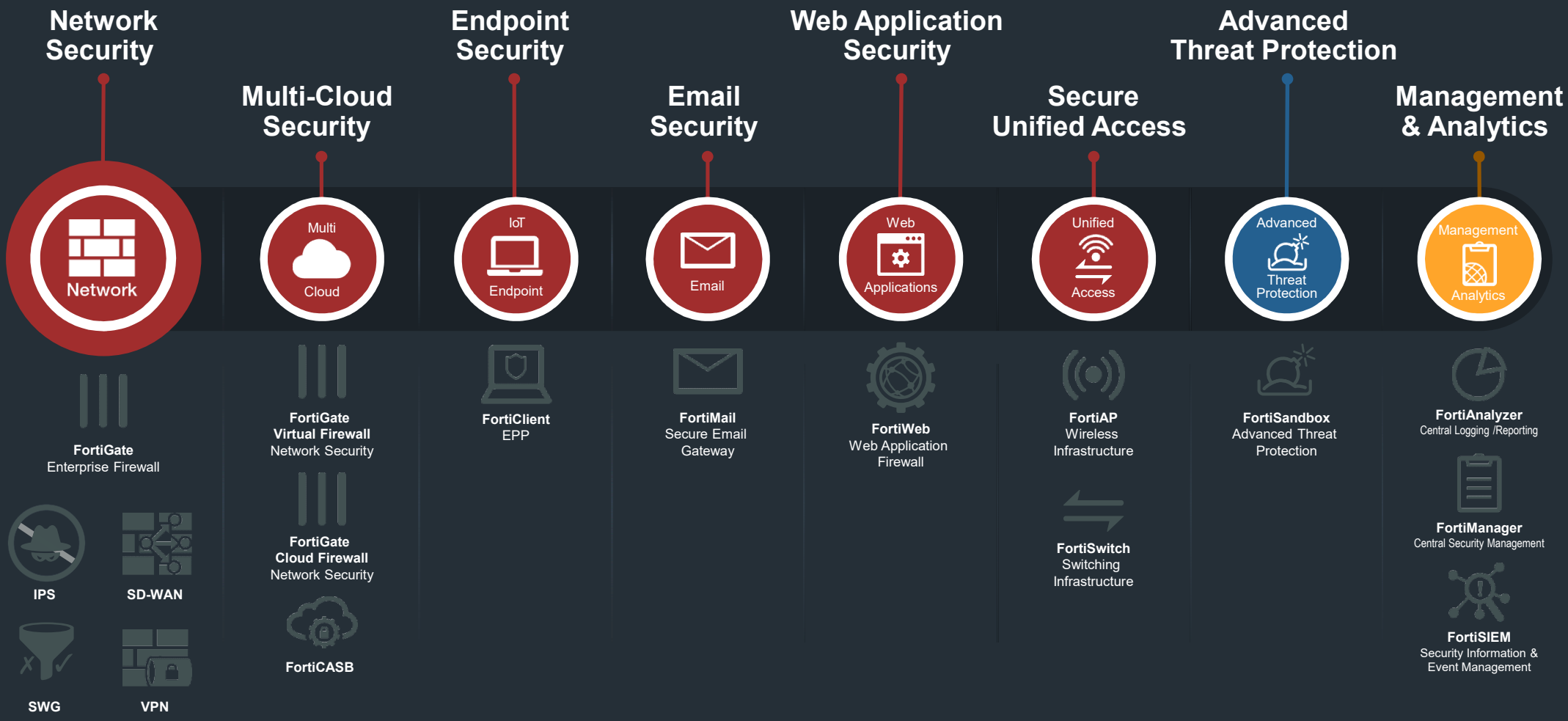
BROAD
Visibility of the entire digital attack surface

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

AUTOMATED
Operations, orchestration, and response



Fortinet End-to-End Solution



FORTINET

Fabric Ready Partners

CLOUD

- amazon web services™
- Google Cloud Platform
- ORACLE
- Microsoft Azure
- IBM

SDN

- BROCADE
- cisco
- nuagenetworks
- openstack
- NEC
- ARISTA
- vmware

ENDPOINT

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

MANAGEMENT

- algosec
- FIREMON
- servicenow
- tufin
- BACKBOX BACKUP RECOVERY AUTOMATION

Security/SIEM

- QUALYS CONTINUOUS SECURITY
- IBM Security
- Hewlett Packard Enterprise
- CYBERARK
- MICRO FOCUS
- cyglass
- WhiteHat SECURITY
- Phantom

IOT/OT/NAC

- BRADFORD NETWORKS
- ForeScout
- NOZOMI NETWORKS
- Pulse Secure

IDENTITY

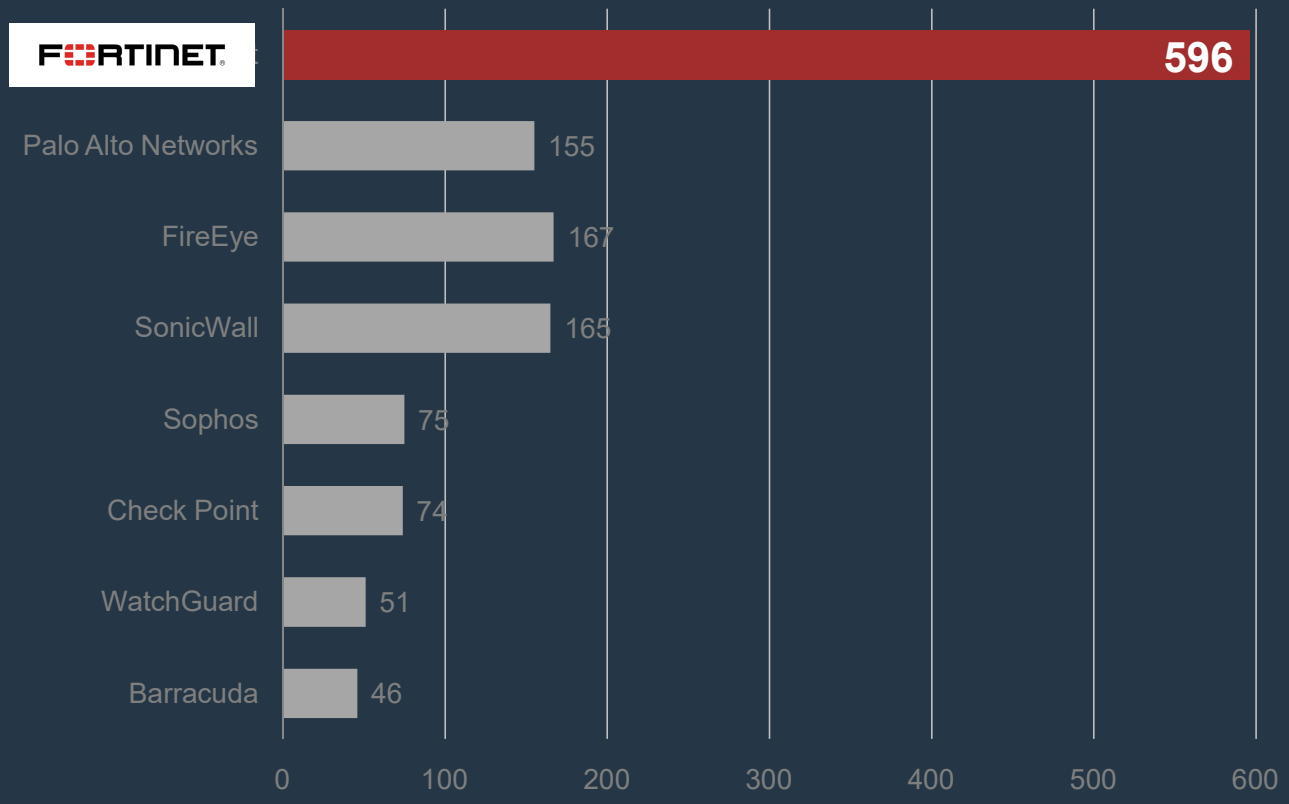
- Centrify
- CLOUDIFY
- CYBERARK

TECHNOLOGY

- ADVA Optical Networking
- HUGHES
- intel
- Sonus Cloud communications made smarter
- VERISIGN

FORTINET

We Lead The Industry in Innovation



#1 Security Innovator

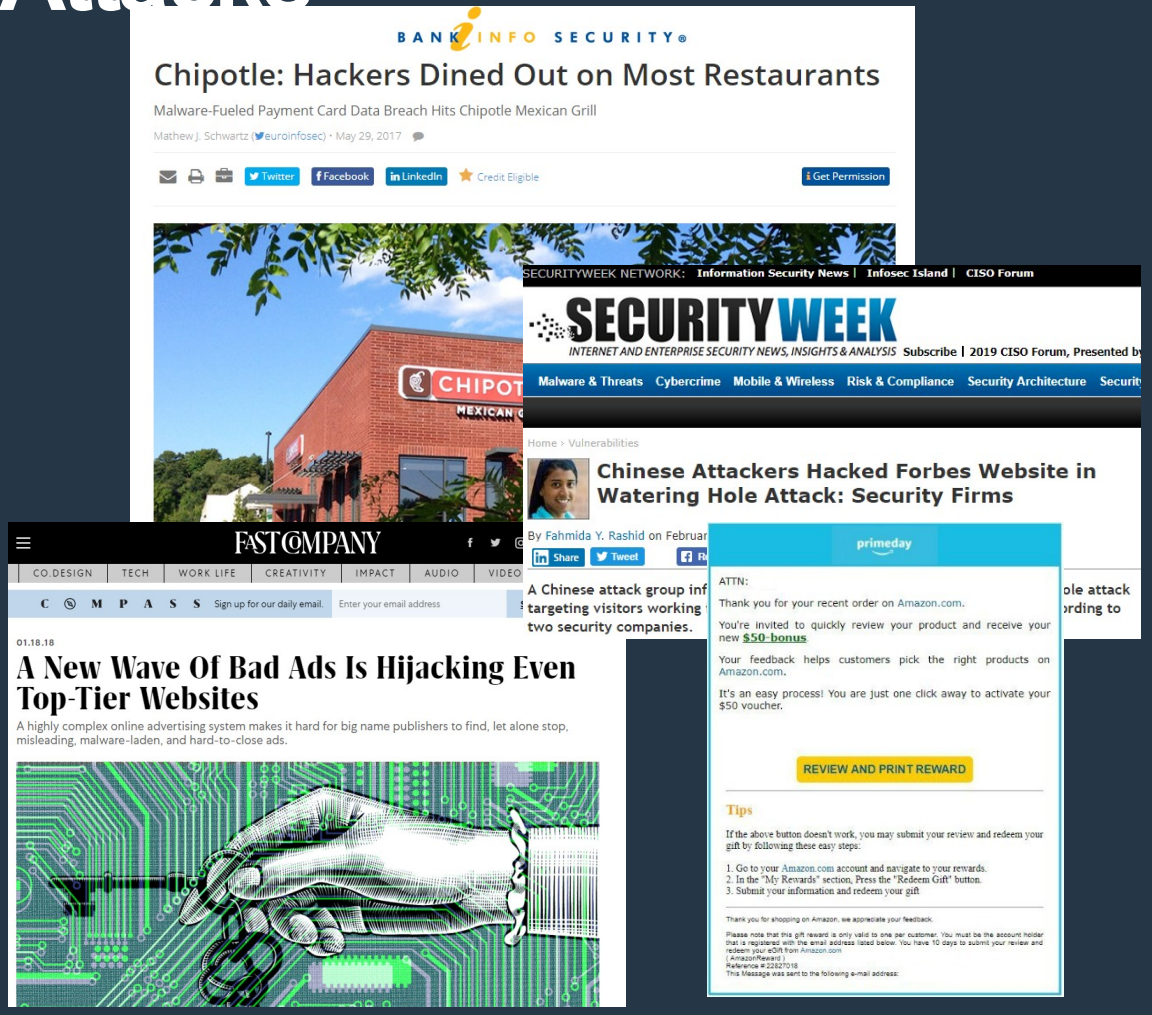
Competitor data based on patents issued as listed by the U.S. Patent and Trademark Office

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

FORTINET

Advanced Web Based Attacks

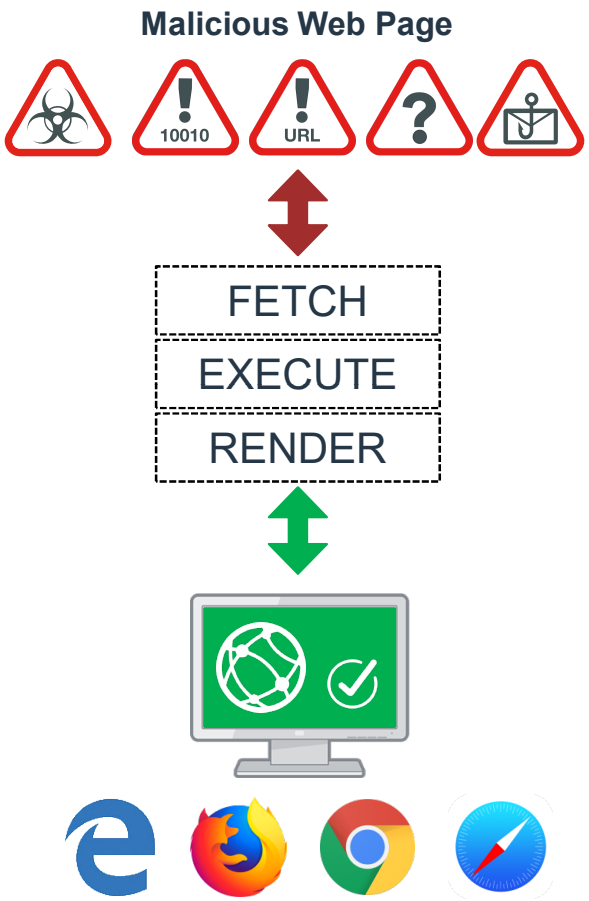
- Email (92.3%) and Web (6.3%) are the two main primary vectors for malware entering an organization.*
- 4% of people will click on a phishing email which is often used to gain a foothold in the network via malware or credential phishing.*
- Malware laden scripts and adverts mean malware can show up on the most popular and trusted websites



FORTINET

* Source: Verizon Data Breach Report 2018

FortiIsolator - Zero Trust Web Browsing



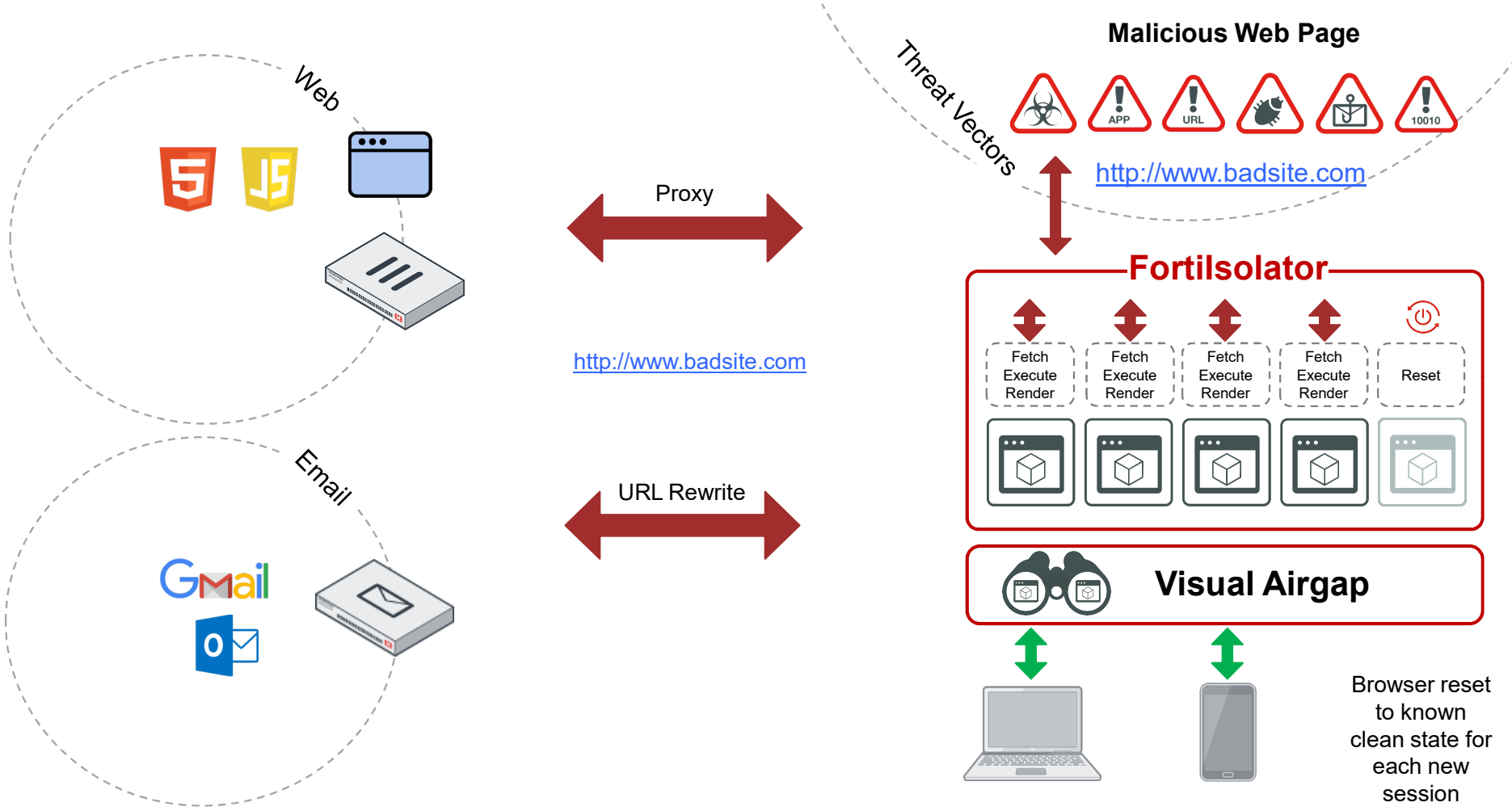
Clientless remote browser isolation

- Works with any modern HTML5 capable browser

Mitigate against web based threats whilst retaining productivity

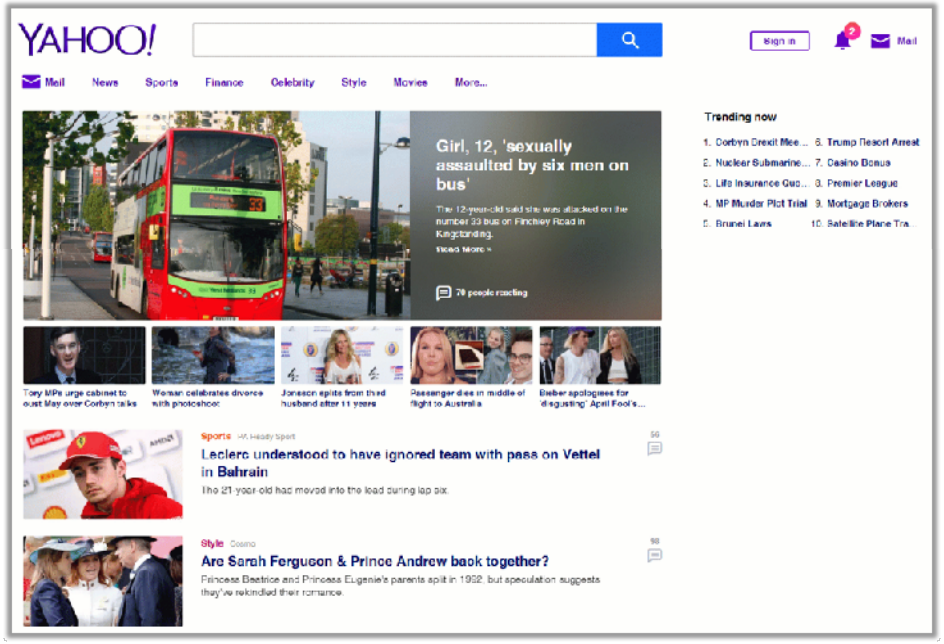
- No third party code ever runs on the local machine
- Browser session runs in clean remote container
- Rendered page image displayed to client
- Supports web page interactivity e.g. links, forms, video, audio

Product Overview

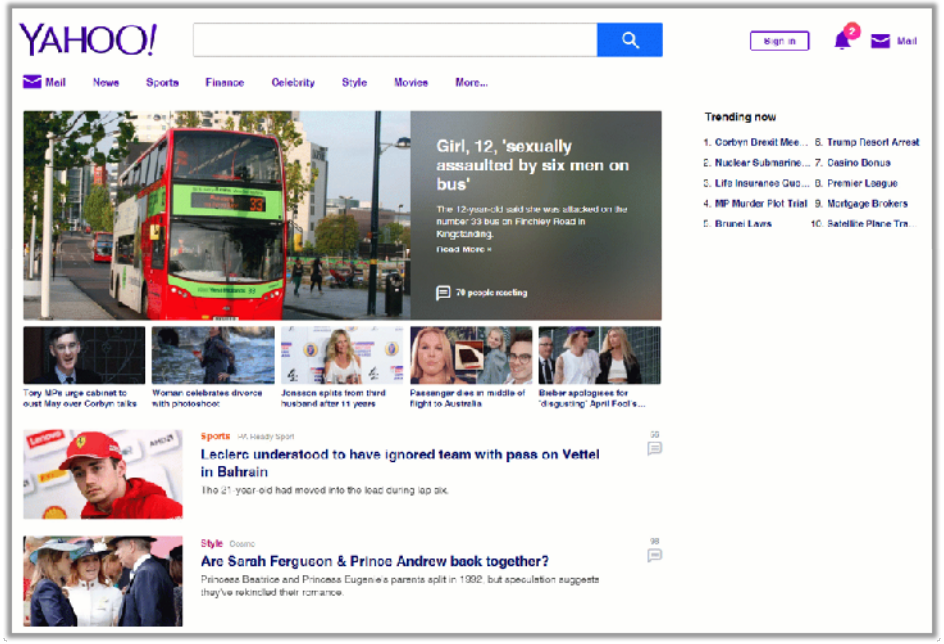


Safe Content Rendering

Directly accessed using Chrome



Accessed via Fortilsolator using Chrome



Safe Content Rendering

Directly accessed using Chrome

20+ Scripts

3rd party scripts & content from iFrame

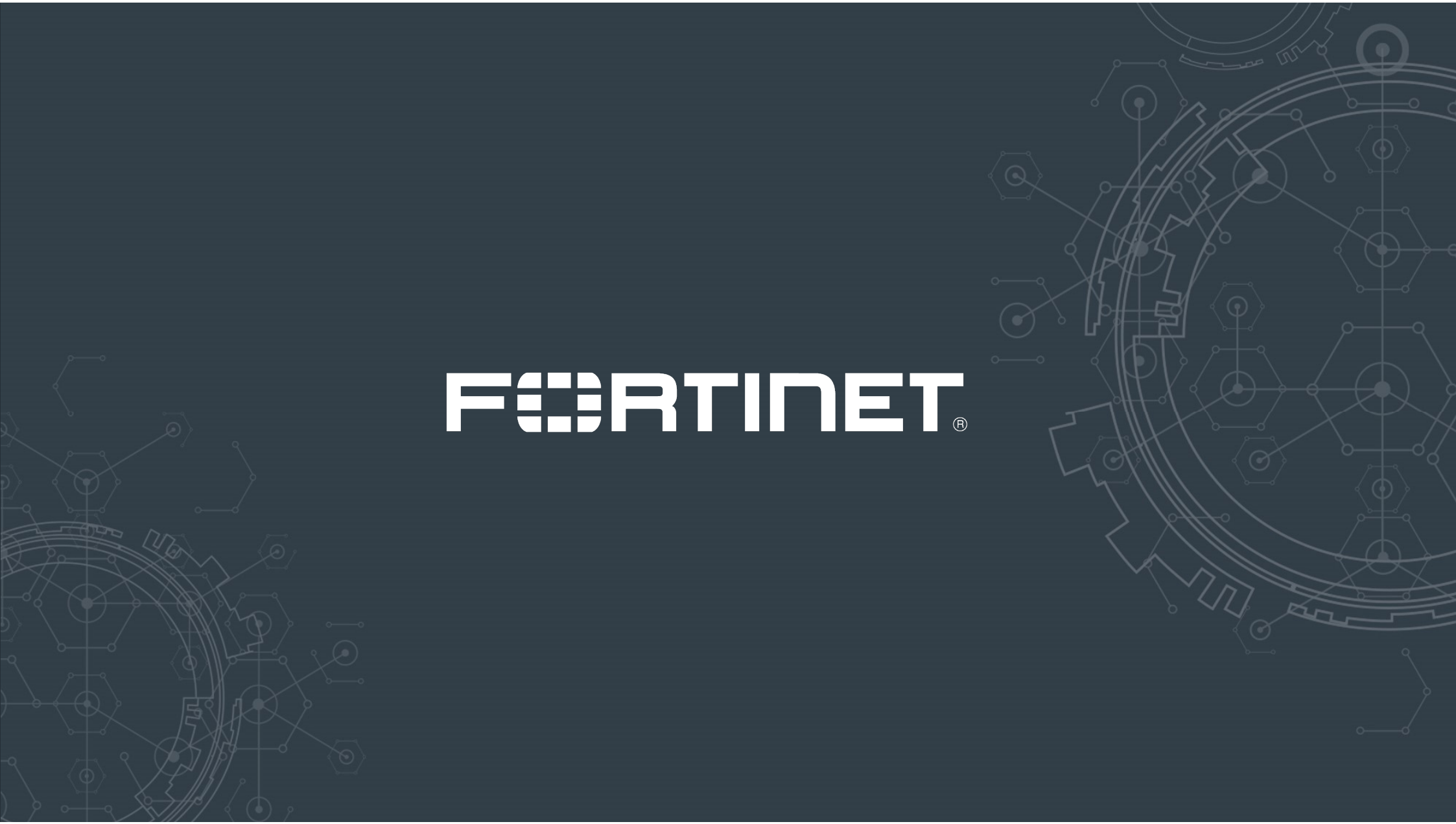
Tracking cookies & scripts

Accessed via FortiIsolator using Chrome

2 FortiIsolator Scripts

```
<!doctype html>
<html style="overflow: hidden;">
▼<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width">
    <link rel="stylesheet" href="https://10.1.0.1:8887/ftnt.css">
    <script src="https://10.1.0.1:8887/jquery.js"></script>
    <script src="https://10.1.0.1:8887/ftnt.js"></script>
    <title>Yahoo</title>
  </head>
▼<body>
  ▶<script>…</script> == $0
    <div id="statusDiv" hidden="hidden"></div>
    <canvas id="mainCanvas" width="150" height="979" style="cursor: default;">
    <canvas id="popupCanvas">
  </body>
</html>
```

No external scripts, iFrames, imports


FORTINET