Miroslav Bajgar

21.-22. října 2021

17. ZÁKAZNICKÝ DEN

NetDispatcher – Multitenantní NextGeneration firewall v Cloudu (Forcepoint)

Forcepoint v multitenantním prostředí

Miroslav Bajgar
Sales Engineer EEUR

Forcepoint

Jak funguje browser isolation

1. Malware embedded in active web-content →

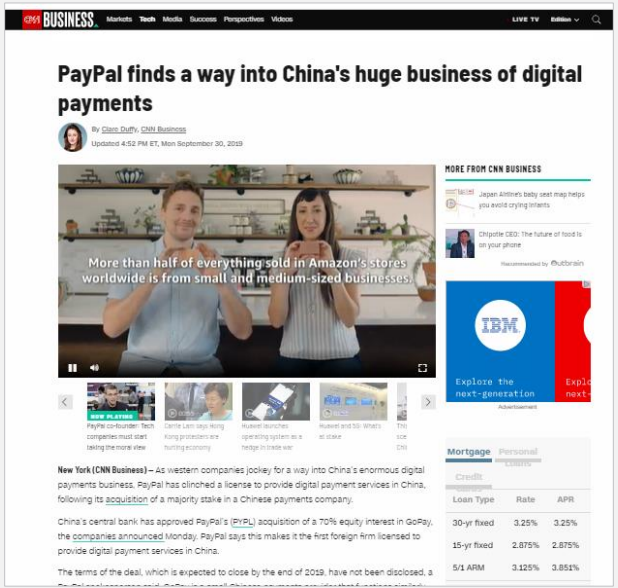
2. Ericom RBI executes content in an isolated container →

3. Safe rendering information sent to endpoint →

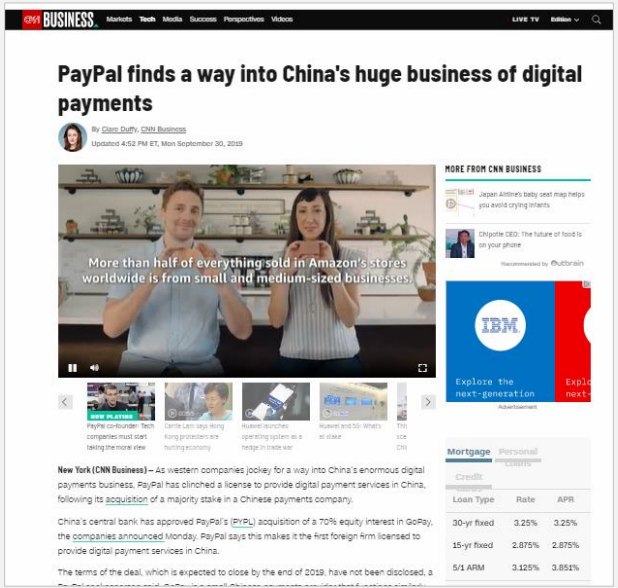
4. Standard browsing experience

Uživatel nevidí žádný rozdíl

Regular Browser

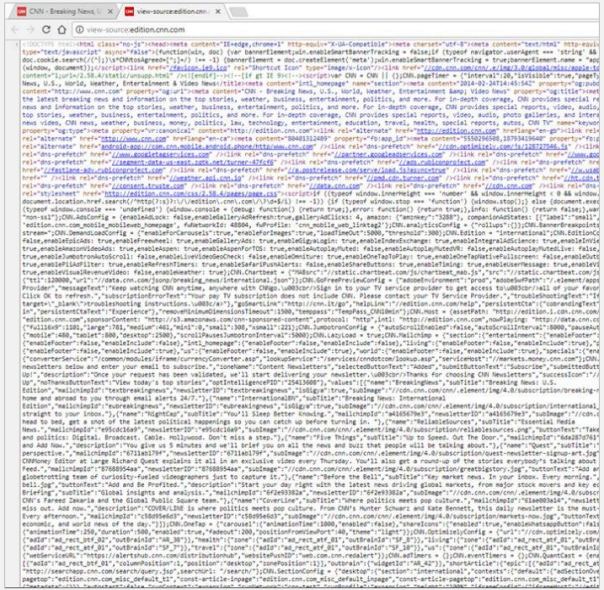


Remote Browser



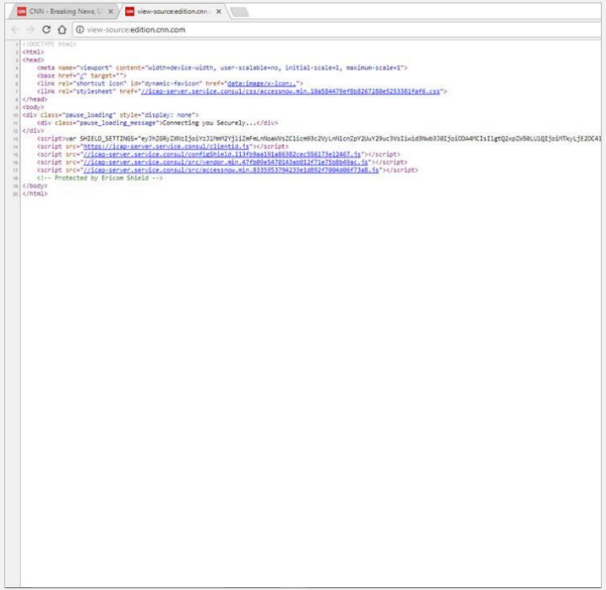
Bez rizikového kódu

Regular Browser



100s JavaScripts | Multiple CSS Scripts | Many External URLs

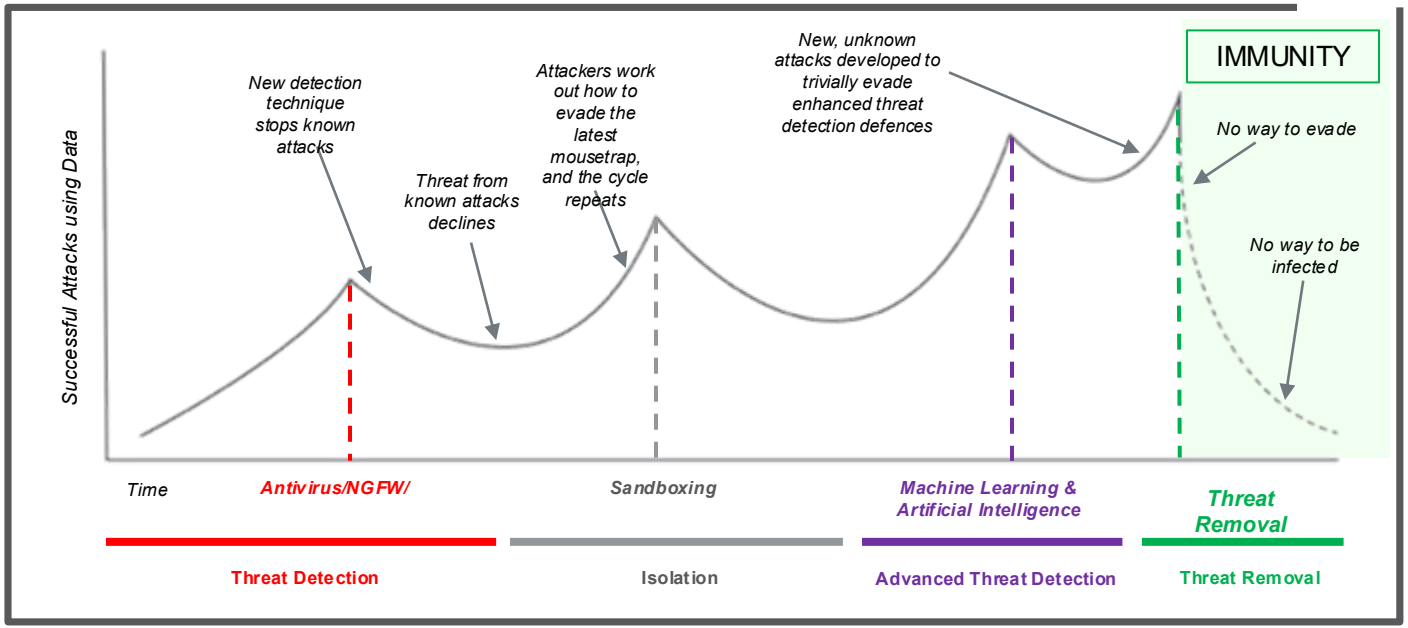
Remote Browser

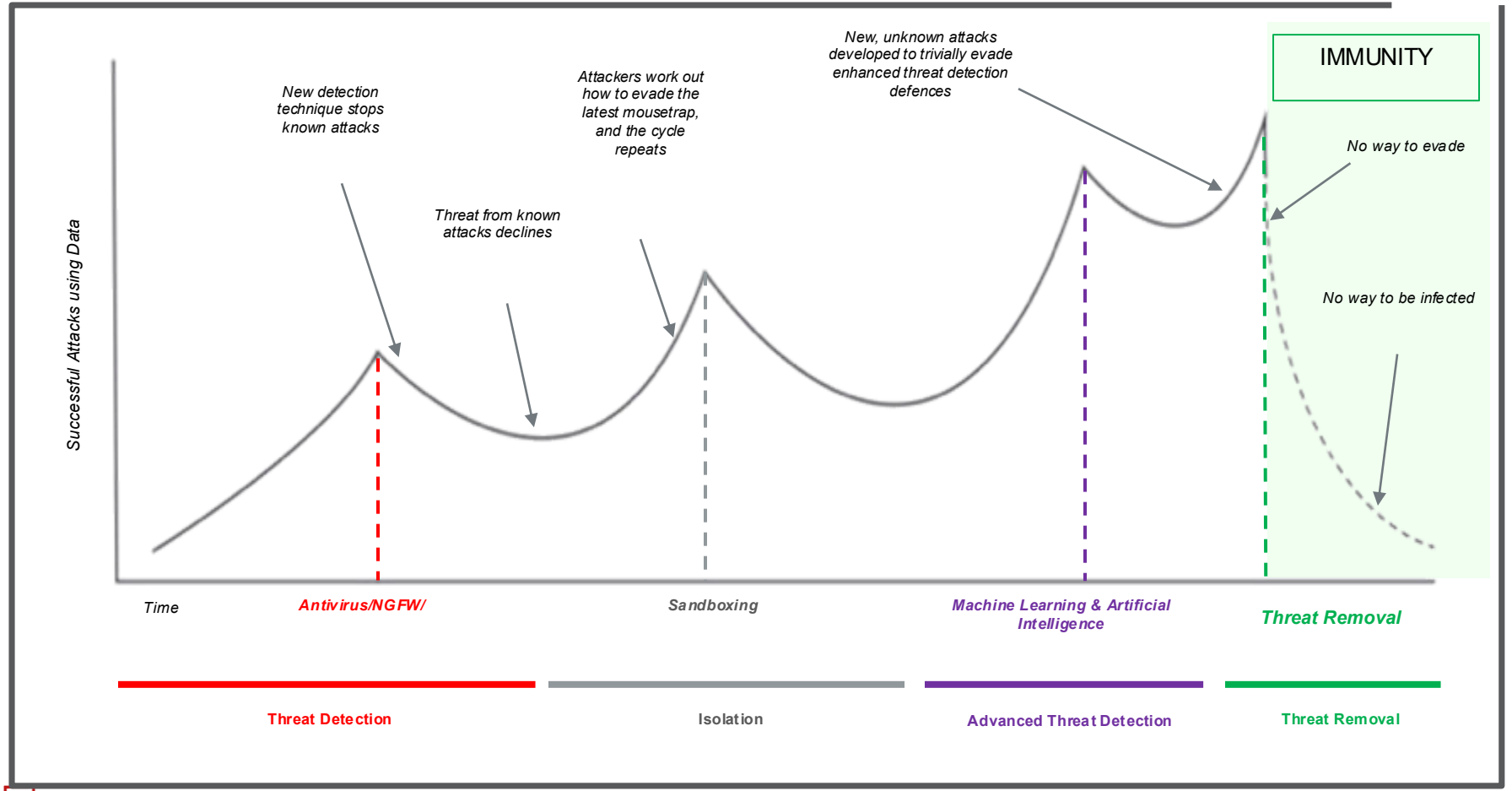


Couple of RBI JavaScripts | 0 CSS Scripts | 0 External URLs

Produkty založené na detekci selhávají v ochraně

- Detection and isolation technologies have a limited lifespan as attacks become increasingly evasive
- Better detection is a short-term solution, attackers will always develop evasion techniques that win
- Deep Secure's proprietary Threat Removal solution does not rely on detection - it uses a zero-trust approach to data to deliver digitally pure data and leave attackers with no opportunity to evade it




IMMUNITY
New, unknown attacks developed to trivially evade enhanced threat detection defences
Attackers work out how to evade the latest mousetrap, and the cycle repeats
New detection technique stops known attacks
Threat from known attacks declines
No way to evade
No way to be infected
Successful Attacks using Data
Time
Antivirus/NGFW/
Sandboxing
Machine Learning & Artificial Intelligence
Threat Removal
Threat Detection
Isolation
Advanced Threat Detection
Threat Removal

Deep Secure Zero Trust Threat Removal Process - Secure by Design

EXTRAKCE

Take the business information from the data. Text, formatting, fonts, images, embedded content etc. Place it into an internal representation of the information. Simple structures which cannot contain code

OVĚŘENÍ

Verify that the internal format is what is expected. For critical systems, this can be done in hardware using FPGAs

REKONSTRUKCE

Create new data from the information. Always created in the same way and always safe

- Does not rely on detection – so no false positives
- Treats all data as potential malware (Zero Trust)
- Fast and always safe
- Complete Malware Immunity

Gartner: ***'Transforms neutralize all potentially malicious content, without requiring multi-AV and sandboxing.'***

DEEP SECURE

Gartner - Beyond Detection - Read the report here

Native Transformations:

FORMAT	EXTENSION
OFFICE PRODUCTIVITY	
Bitmap image	BMP
Microsoft Office X Doc	DOCX
Microsoft enhanced metafile	EMF+
Email message	EML
GIF image	GIF
HTML file	HTML
ICAL File	ICAL
JPEG 2000	JP2K
JPEG image	JPEG
MIME HTML Archive	MHT
Multipurpose Internet Mail Extensions	MIME
Adobe PDF	PDF
PNG image	PNG
Microsoft Office X PowerPoint	PPTX
Rich Text	RTF
Plain Text	TXT
TIFF image	TIFF
Microsoft Windows meta file	WMF
Microsoft Office X Excel	XLSX
Zip archive	ZIP
STRUCTURED DATA	
Comma separated values	CSV
JSON structured data	JSON
Google Protocol Buffers 3	Proto3
XML structured data	XML

With Translation Sidecar:

FORMAT	Original	Translated	Final
Legacy Microsoft Word	DOC	DOCX	DOC
Legacy Microsoft Powerpoint	PPT	PPTX	PPT
Legacy Microsoft Excel	XLS	XLSX	XLS
OpenDocument Text	ODT	DOCX	ODT
OpenDocument Spreadsheet	ODS	XLSX	ODS
OpenDocument Presentation	ODP	PPTX	ODP
Rich Text	RTF	DOCX	RTF
eXtensbile Paper Specification	XPS	PDF	XPS
EPUB book reader format	EPUB	PDF	EPUB
Mobipocket e-book format	MOBI	DOCX	
Computer Graphics Metafile	CGM	PDF	
Adobe Photoshop	PSD	PNG	PSD
Microsoft One Note	ONE	PDF	
AutoCAD Drawing	DWG	PDF	
Legacy AutoCAD Drawing	DXF	PDF	
Legacy Microsoft Visio	VSD	PDF	
Microsoft Visio	VSDX	PDF	
XLS Formatting Object	FO	PDF	
7Zip archive	7Zip	ZIP	7Zip
BZip2 Archive	BZip2	ZIP	BZip2
GZIP Archive	Gzip	ZIP	GZip
Z Archive	Z	ZIP	Z
TAR archive	TAR	ZIP	TAR
Microsoft CAB archive	CAB	ZIP	

The Translation Sidecar translates the *original* format into a natively supported file type (*translated*) and for some file types can translate to a *final* format afterwards.

NSS Labs skóre 2012-2018

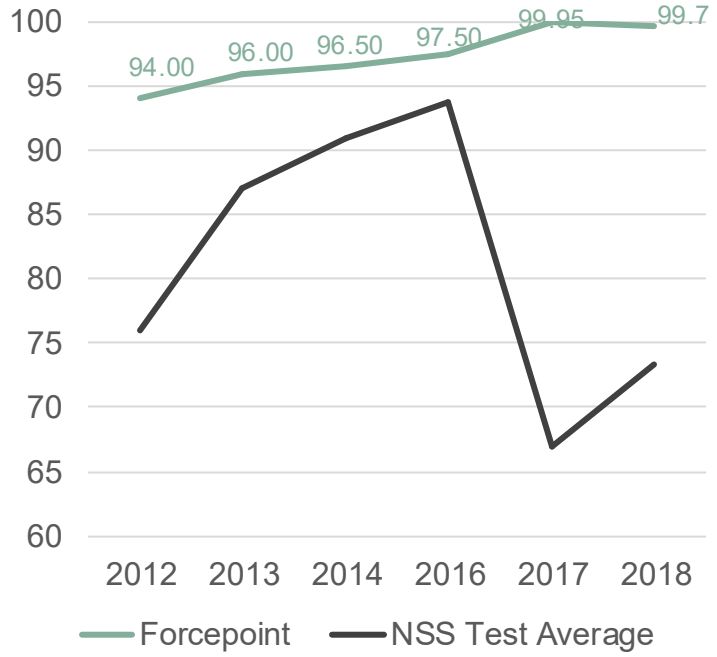
#1 Next Gen Firewall

#1 Next Gen IPS

#1 Breach Detection System*

Forcepoint NGFW 6x po sobě doporučený

zatímco



PaloAlto: Not Recommended 2017, 2016, 2014 on NSS Labs NGFW/NGIPS
Cisco: Not Recommended 2018, 2016, 2014, on NSS Labs NGFW/NGIPS
Fortinet: Not Recommended 2016, 2013 NGIPS, 2012 NGFW and bad score on NGFW 2017
Checkpoint: Not Recommended 2018 NGIPS, and bad score on NGFW 2017

NSS Labs NGFW 2019

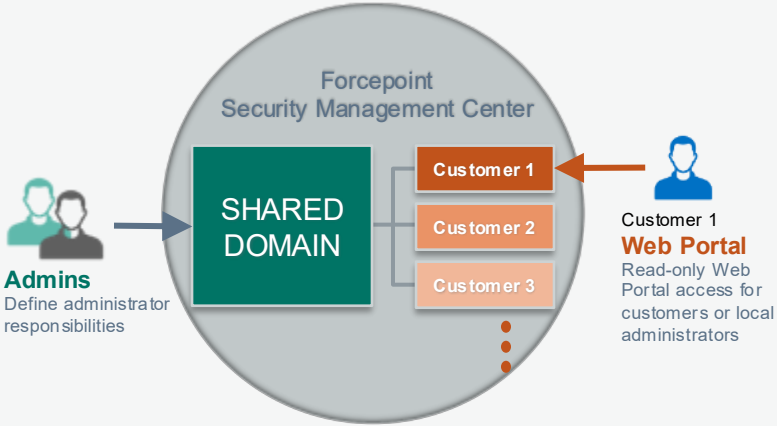
Historie pokrytí známých zranitelností

Product/Year	Barracuda Networks	Check Point	Forcepoint	Fortinet	Huawei	Palo Alto Networks	SonicWall	Sophos	Versa Networks	WatchGuard	Vendor A	Vendor B
2008	94.0%	100.0%	100.0%	99.7%	99.1%	100.0%	99.4%	96.8%	100.0%	98.4%	100.0%	99.1%
2009	93.0%	98.9%	100.0%	100.0%	97.3%	100.0%	98.9%	98.9%	99.5%	97.3%	99.5%	99.5%
2010	90.5%	100.0%	100.0%	100.0%	93.9%	100.0%	98.8%	90.5%	98.5%	96.3%	99.7%	99.4%
2011	90.7%	99.2%	100.0%	100.0%	84.7%	100.0%	100.0%	80.5%	98.3%	96.6%	99.2%	100.0%
2012	94.1%	99.5%	100.0%	100.0%	93.1%	100.0%	99.5%	89.7%	100.0%	99.0%	100.0%	99.0%
2013	100.0%	100.0%	100.0%	100.0%	98.8%	100.0%	100.0%	89.2%	100.0%	100.0%	100.0%	100.0%
2014	98.9%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	97.8%	100.0%	100.0%
2015	87.5%	100.0%	100.0%	99.0%	100.0%	100.0%	99.0%	97.9%	100.0%	96.9%	99.0%	97.9%
2016	97.1%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	99.6%	98.9%	94.2%	98.9%	99.6%
2017	91.1%	100.0%	100.0%	98.2%	96.4%	100.0%	100.0%	98.2%	98.2%	87.5%	94.6%	100.0%
2018	94.6%	97.3%	100.0%	100.0%	100.0%	97.3%	97.2%	88.9%	91.9%	91.7%	91.9%	97.2%
TOTAL	93.6%	99.7%	100.0%	99.8%	96.5%	99.9%	99.4%	94.2%	99.2%	96.7%	99.3%	99.3%

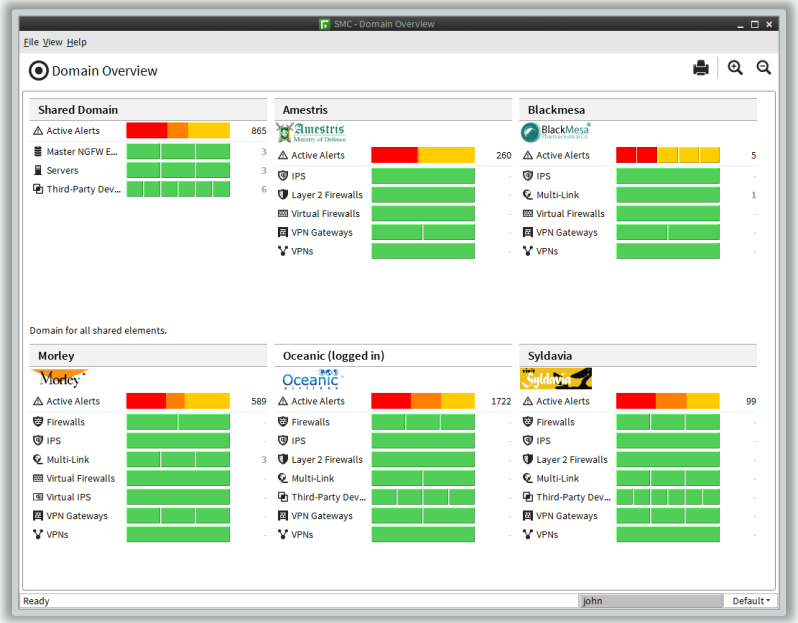
Multi-Tenant / Multi-Domain

Compartmentalize Distributed Security

- All elements are stored in the same Management Server Database
- Domains are totally isolated from each other
- All Domains inherit elements from Shared Domain



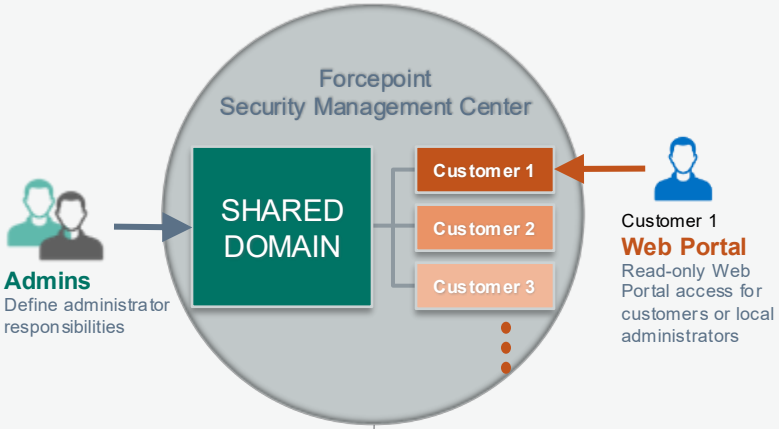
Region, Business Unit or Security Domains

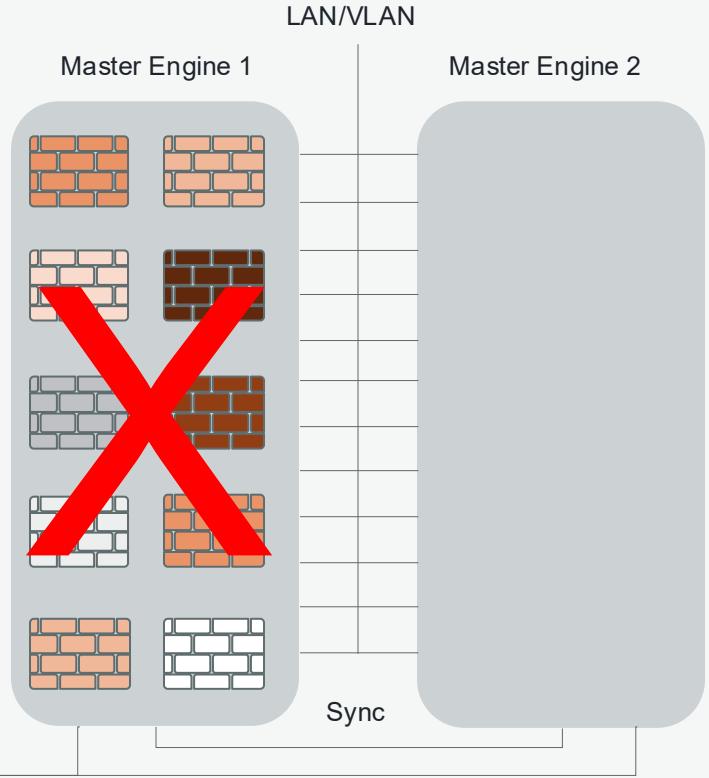


Virtuální firewally

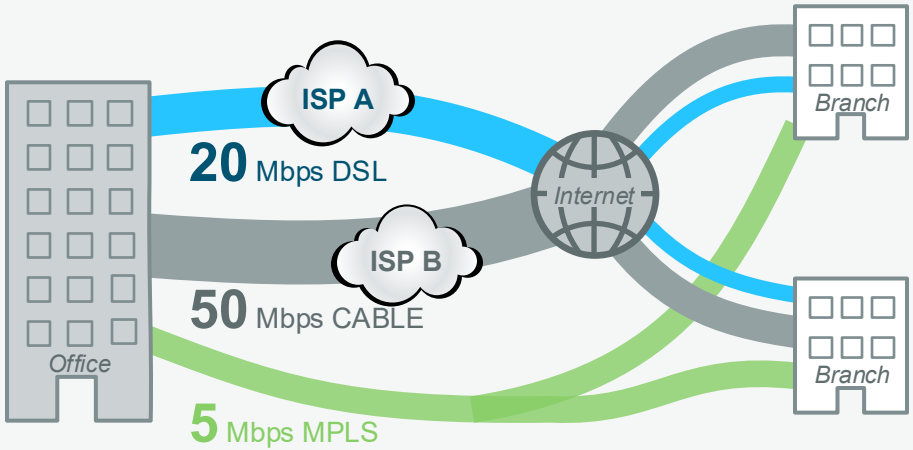
Až 250 virtuálních FW na jeden box

Může být přiřazeno na 200 domén (zákazníků)





Multi-Link™ konektivita



Kombinovaných **75** Mbps se zálohou a levněji

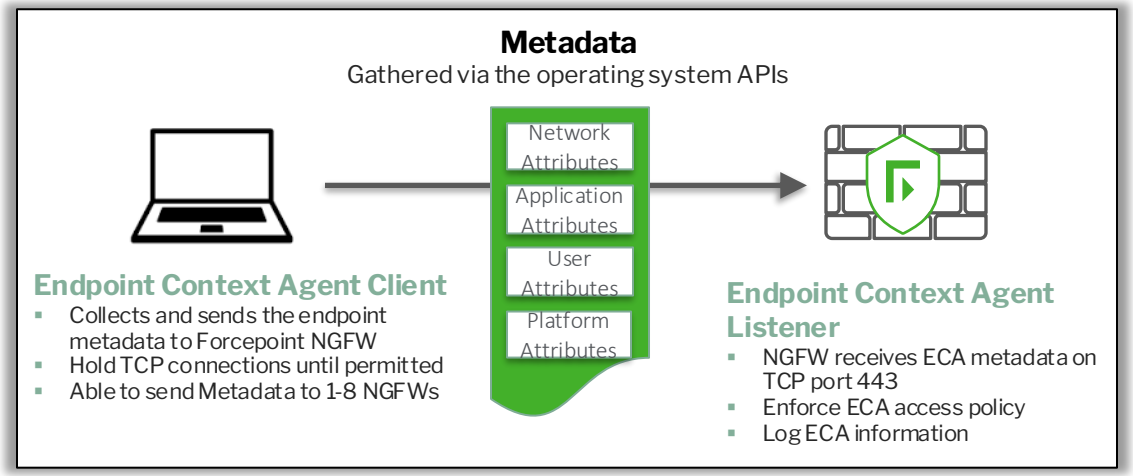
Možné míchat ISP a MPLS linky

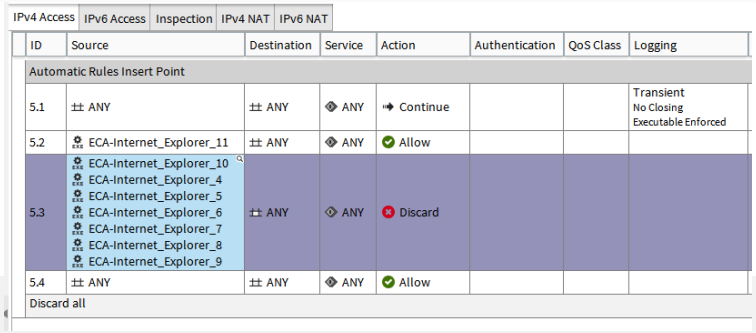
- Bandwidth & Quality of Service (QoS) controls
- Site-to-site VPNs

Možnost řídit >2500 firewallů v jednom

- Networking & security policies together
- In-house or MSSP

Endpoint Context Agent (ECA)





CATEGORY	METADATA
Application Attributes	Executable binary name read from the signed executable file (String)
	Executable checksum(SHA-256/MD5)
	Executable product name (String)
	Executable version (String)
	Fingerprint of the signer certificate or public key
	Signature check result from OS (OK, not OK or not checked)
	Signer name (String)
Platform Attributes	AV status
	BIOS serial number
	Endpoint load (CPU, memory, disk)
	Full computer name
	Listening sockets, their interfaces and ports
	Local FW settings
	OS updates
	OS version
	User login/logout event
User Attributes	User Domain Name (String)
	User Group Information (String Array)
	User ID (String)
	User Type

Forcepoint NGFW cloud služby

URL Filtering

- Powered by Forcepoint ThreatSeeker Intelligence
- Extensive categorization of domains (Banking, etc.)
- Filter by category, not hardcoded URLs
- Easy to use directly from access policies

Advanced Malware Detection (Sandbox)

- Cloud Service or on-premises appliance
- Full System Emulation delivers highest efficacy
- Also used with Forcepoint CASB, Web & Email Security

Q&A

Forcepoint