Shields Up!
Cyber Security 101

Trusted Internet, New Boston, NH

BE ON THE LOOKOUT for a 2020 Red Toyota Highlander

License plate: TEXAS GER-515

- **Every license plate reader, traffic camera, and EZ Pass will be monitored for this car**
- **There might be an Amber, Silver, Other Alert issued**
- **If the car is spotted, it'll be tracked down and stopped by Police for questioning.**
- **The threat will be (hopefully) mitigated.**

We do this in cyber space.

We sell 24x7 monitoring and protection. When we see something on the property, we protect and defend it ourselves.

The ADT model, but for computers.

TRUSTED INTERNET

The Threats
(especially as a result of current circumstances)

- Opportunistic
- Targeted
- Collateral damage

Opportunistic – High Probability, Low to High impact

Ransomware!

Keystroke loggers

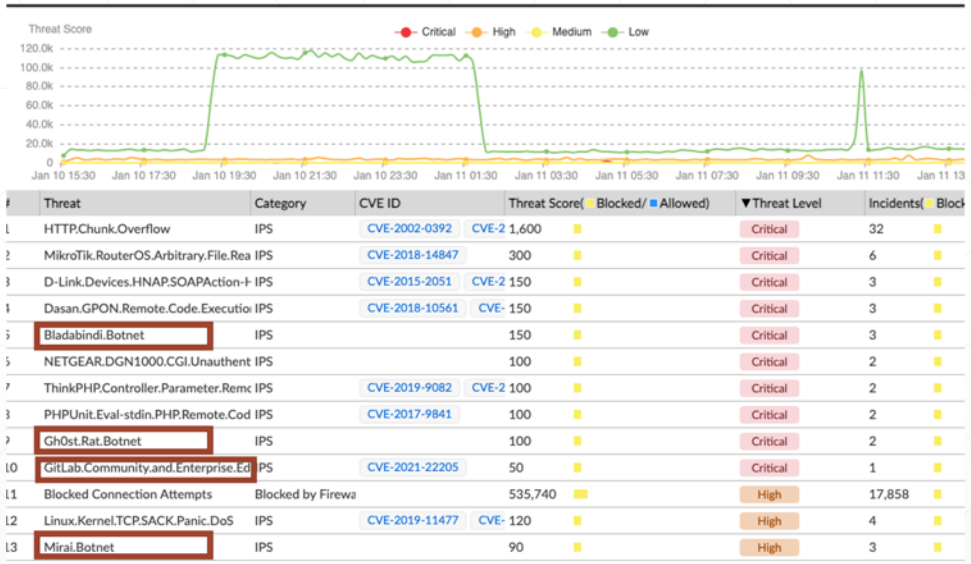
Password theft

Automated, high speed attacks

Motive? Protest, Financial Cyber Theft

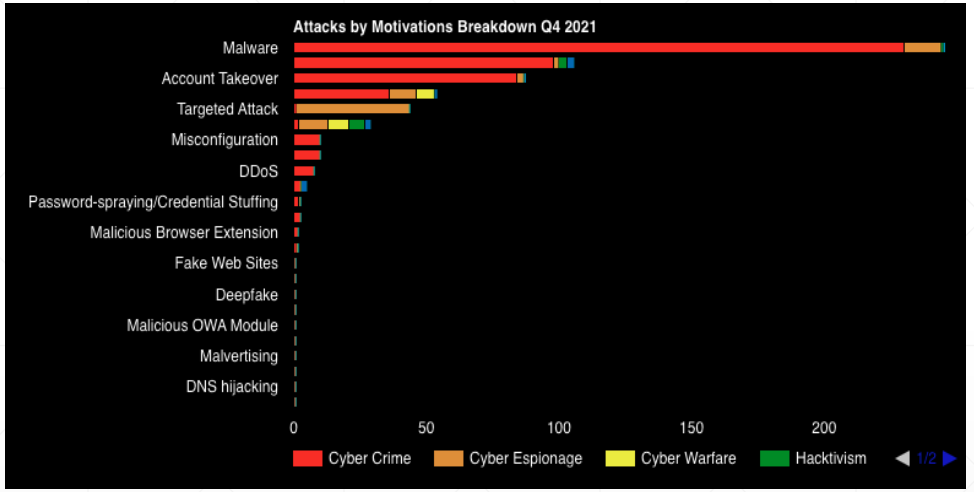
What does that look like?

High Speed automated attacks



#	Threat	Category	CVE ID	Threat Score(Blocked/ Allowed)	▼Threat Level	Incidents(Block
1	HTTP.Chunk.Overflow	IPS	CVE-2002-0392 CVE-2	1,600	Critical	32
2	MikroTik.RouterOS.Arbitrary.File.Rea	IPS	CVE-2018-14847	300	Critical	6
3	D-Link.Devices.HNAP.SOAPAction-H	IPS	CVE-2015-2051 CVE-2	150	Critical	3
4	Dasan.GPON.Remote.Code.Executio	IPS	CVE-2018-10561 CVE-	150	Critical	3
5	Bladabindi.Botnet	IPS		150	Critical	3
6	NETGEAR.DGN1000.CGI.Unauthent	IPS		100	Critical	2
7	ThinkPHP.Controller.Parameter.Remc	IPS	CVE-2019-9082 CVE-2	100	Critical	2
8	PHPUnit.Eval-stdin.PHP.Remote.Cod	IPS	CVE-2017-9841	100	Critical	2
9	Gh0st.Rat.Botnet	IPS		100	Critical	2
10	GitLab.Community.and.Enterprise.Ed	IPS	CVE-2021-22205	50	Critical	1
11	Blocked Connection Attempts	Blocked by Firewa		535,740	High	17,858
12	Linux.Kernel.TCP.SACK.Panic.DoS	IPS	CVE-2019-11477 CVE-	120	High	4
13	Mirai.Botnet	IPS		90	High	3

Malware, Ransomware. Account theft and targeted attacks



SOURCE: HACKMEGEDDON Q4, 2021

83
BREACHES TRACKED IN 2021

4.026B
RECORDS LEAKED IN 2021

2,443
EVENTS RECORDED IN 2021

Targeted - Low probability, high impact

- Ransomware (with BIG numbers)
- Identity theft or takeover
- Negative Press or Social Media

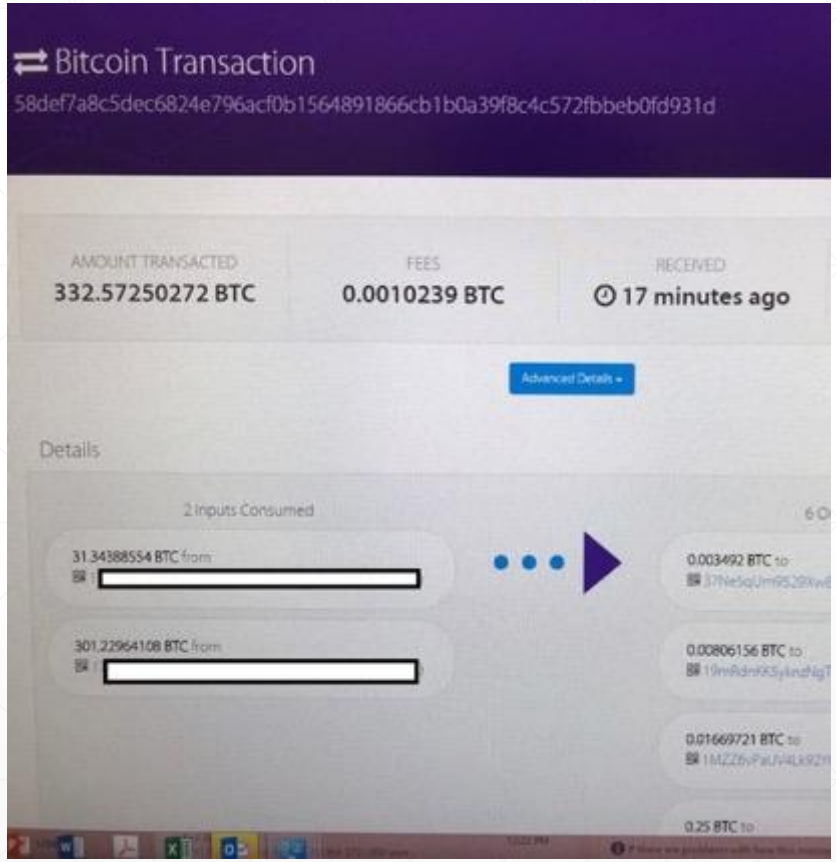
- Manual attacks, targeting specific people or companies

Targeted Ransomware

“Omega” – Houston, Tx

7500 employees, 1000 servers in over 40 locations encrypted, ransomed

- Trusted Internet brought in to interface with the board (after four days of business interruption at a cost of $25 mil per day).
- Trusted Internet took over incident response
- Paid $700,000 in Bitcoin Ransom
- Restored operations in <24 hours
- Reengineered security architecture

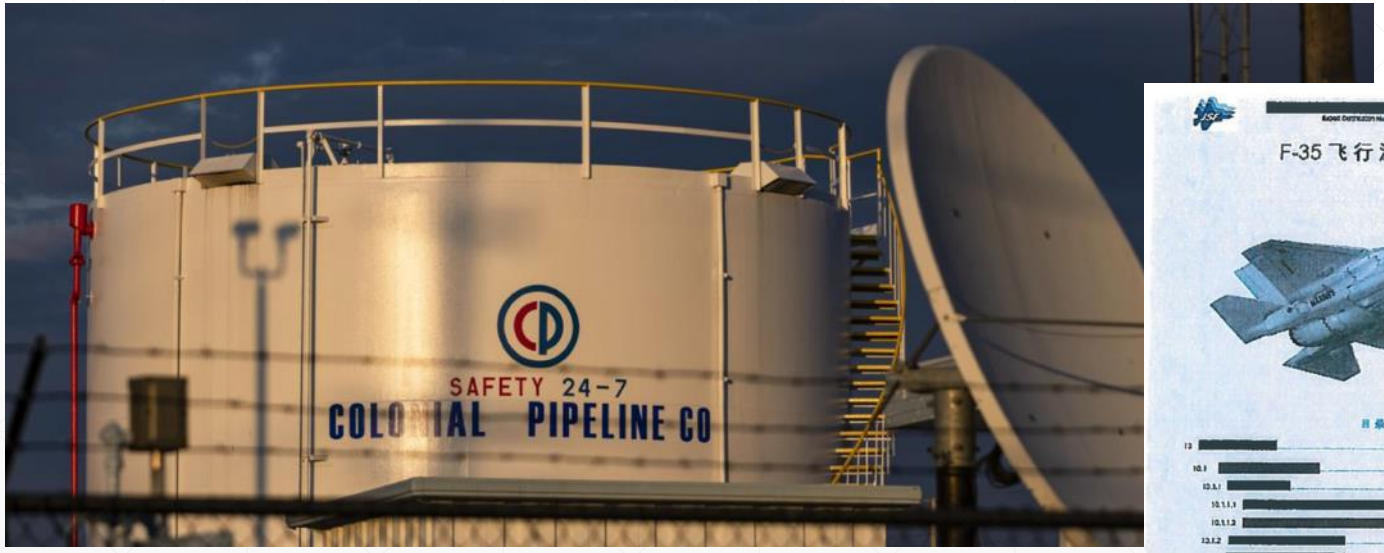


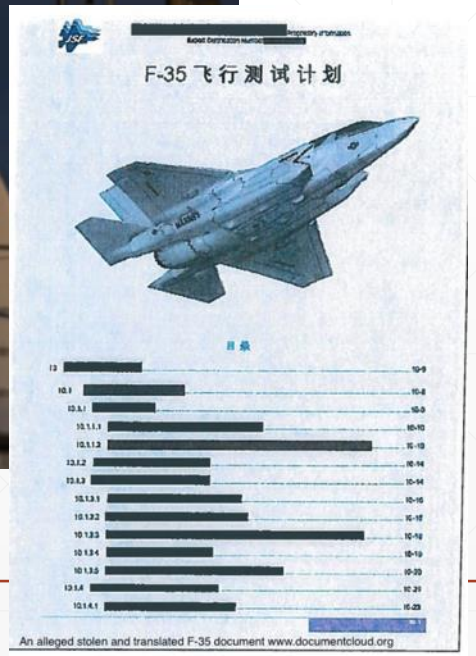
“Stutzman saved my Company!”

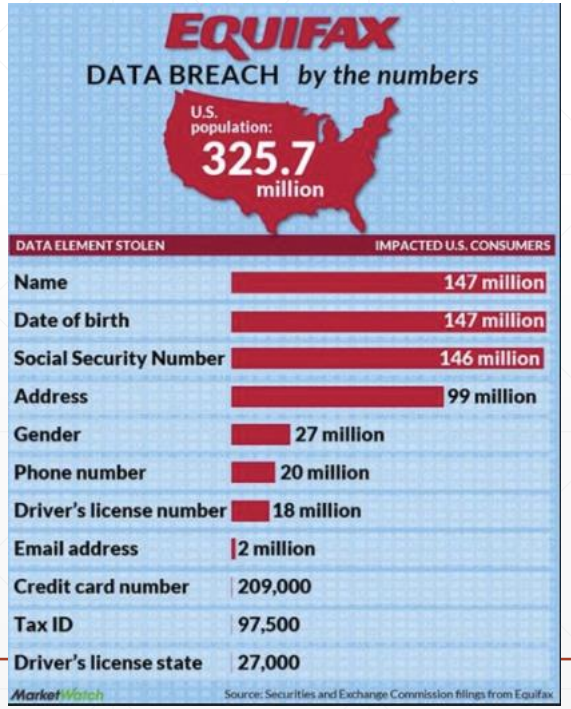
CEO “Omega”

What does a targeted attack look like? Typically

- Data Theft
- Espionage
- Ransomware

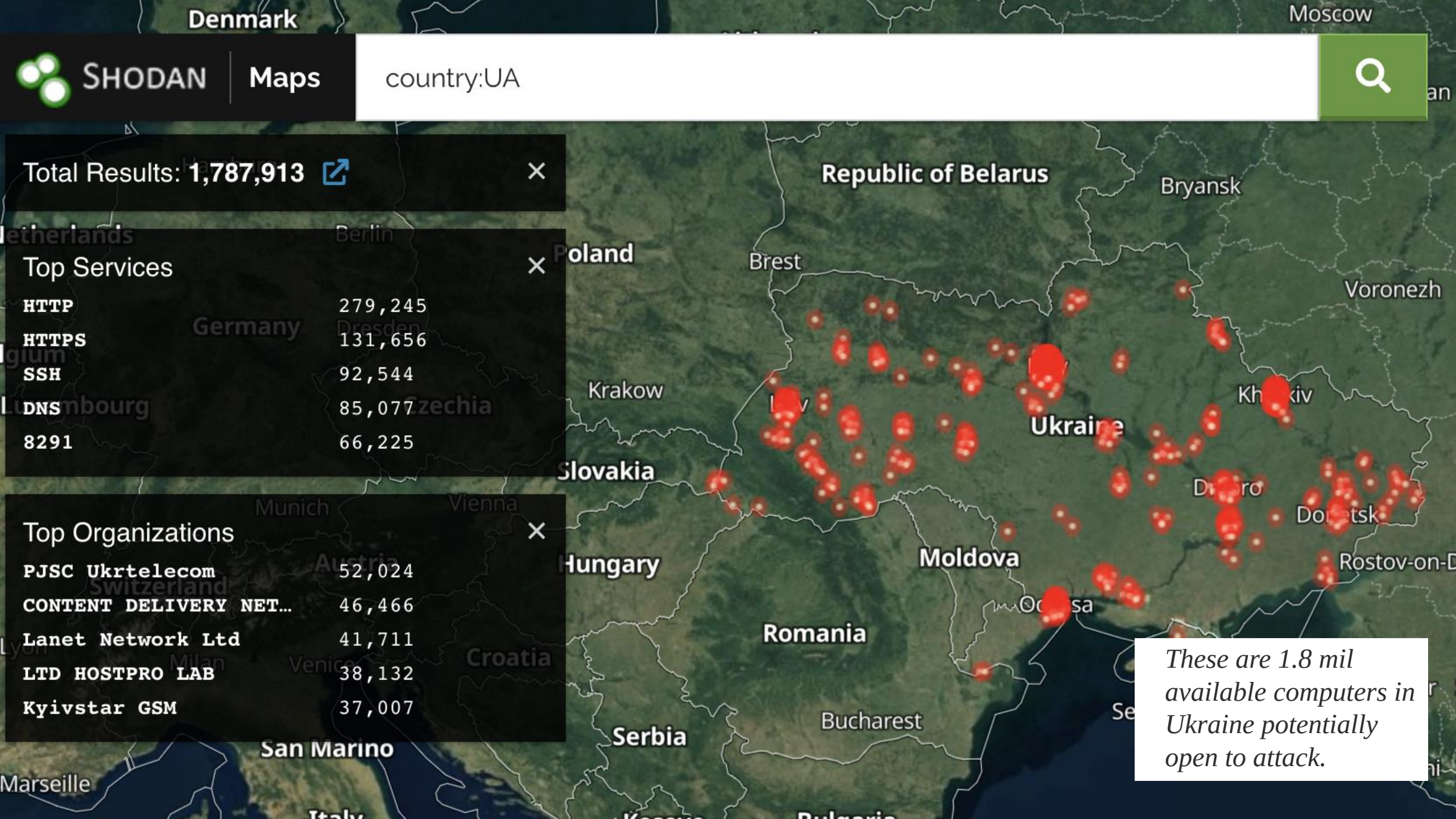


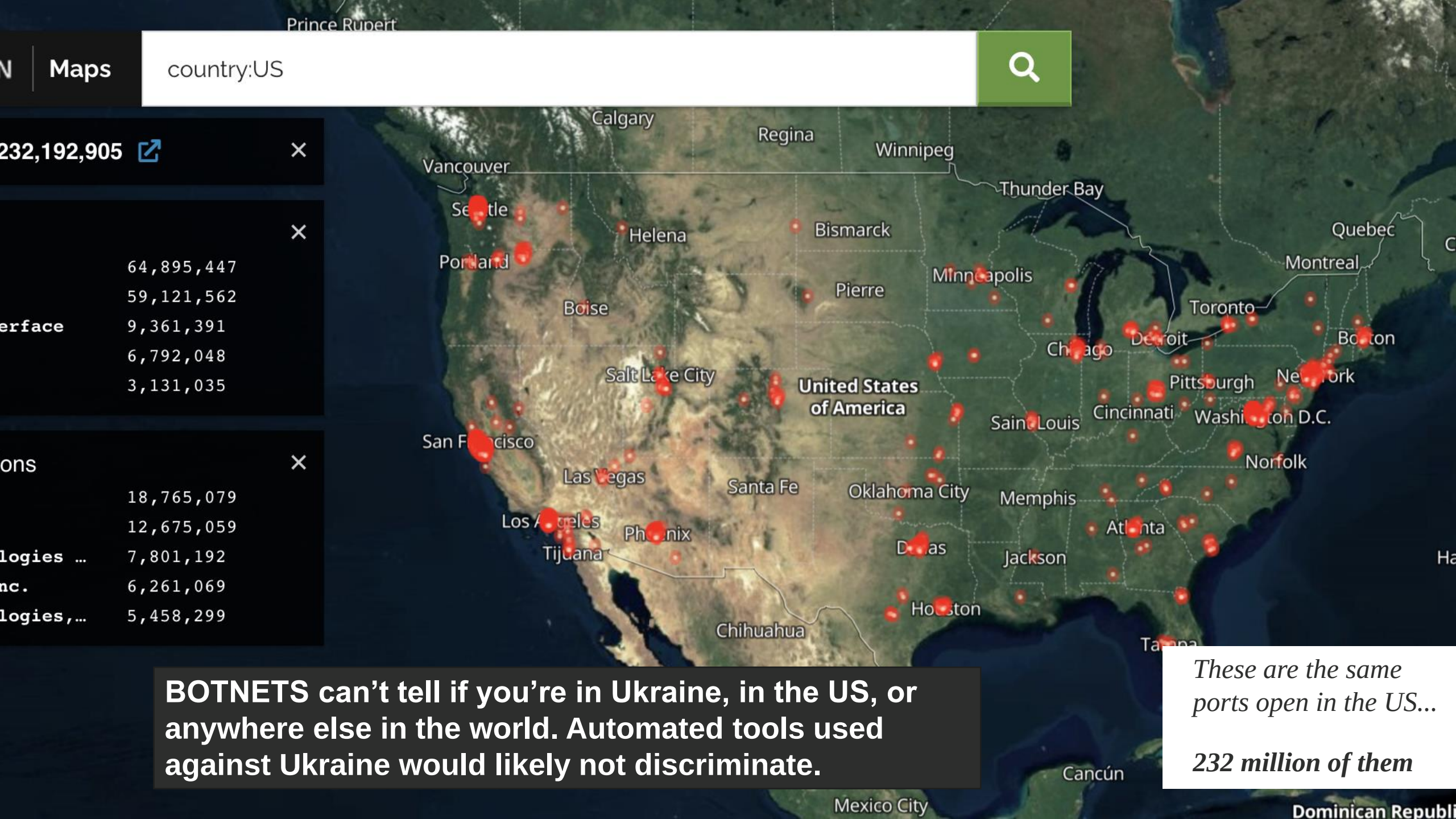




Collateral damage – (today) Medium Risk, Medium to High Impact

- Ransomware (without the abilty to recover)
  - MOTIVE? Financial Support
- Damaging malware (MS identified one in December)
- For Larger Banks and High Networth
  - Could be targeted.
  - Russian Oligarks are now sanctioned and assets frozen
  - Potically Exposed or High Networth personnel could be targeted
  - Motive? , Revenge, Financial Gain
- WannaCry, NotPetya, BadRabbit


SHODAN
Maps
country:UA
Total Results: 1,787,913
Top Services
HTTP 279,245
HTTPS 131,656
SSH 92,544
DNS 85,077
8291 66,225
Top Organizations
PJSC Ukrtelecom 52,024
CONTENT DELIVERY NET… 46,466
Lanet Network Ltd 41,711
LTD HOSTPRO LAB 38,132
Kyivstar GSM 37,007
Republic of Belarus
Bryansk
Brest
Voronezh
Krakow
Ukraine
Slovakia
Moldova
Hungary
Romania
Bucharest
Serbia
San Marino
Marseille
Rostov-on-D
These are 1.8 mil available computers in Ukraine potentially open to attack.



BOTNETS can't tell if you're in Ukraine, in the US, or anywhere else in the world. Automated tools used against Ukraine would likely not discriminate.

These are the same ports open in the US...

232 million of them

CEO, Trusted Internet, Virtual CISO® to a 7500-person oil and gas, the head coach of an NBA team, two NH Small Businesses (defense and financial), and a $3.5 billion Houston oil and gas company.

- Past positions include:
  - **DCISE Director at** DoD Cyber Crime Center
  - **Principal Engineer**, Carnegie Mellon, Software Engineering Institute
    - Some of my work continues to fund CMU/SEI for up to $40 mil per year.
    - Worked for Carnegie Mellon – Twice.
  - **Chief Information Security Officer** Northrop Grumman Electronics Sector
  - **Chief, Cyber Threat Analysis & Intelligence** Northrop Grumman Corporate
  - Cisco Systems, **Sr. Manager Global IT Risk Management**
  - **Navy Intelligence Officer**, Information Warfare (cyber)
- **Built and ran** DoD/DIB Information Sharing and Analysis Environment
- **Built and ran** Northrop Grumman's anti-cyber espionage team (to protect Northrop Grumman from Chinese spies (APT)).
  - Awarded Northrop Grumman Presidents Award for IT Innovation, 2008
  - Information Security Program of the year.
- **Built and ran** Cisco's global IT Risk Management practice. Authored risk and integration for Cisco's M&A processes.
- **Founding member**: Honeynet Project (the home to many of today's current security tools.

Certified Information System Security Professional (2002 – Pres), BS Excelsior College, MBA Worcester Polytechnic Institute, Senior Executive Fellow, Harvard Kennedy School

Veteran Led company

Jeff Stutzman
CISSP
Founder, CEO
Virtual CISO®

Previously:

- Wapack Labs
- DoD Cyber Crime Center (DCISE Dir)
- Carnegie Mellon Univ.
- CISO, NGES
- USN Intel
- USCG SYSADMIN

Jon Lance
COO, CFO

Previously:

- VP Operations, Global Guardian
- US Navy Pilot

Amanda Gorski
CISSP, VP, PMO, FSO
Virtual CISO®

Previously:

- US SOCOM
- GSEC LLC
- FSO, Nextech
- Raytheon Cyber

Nate Paddock
CISSP
Dir., Sec. Svcs, Virtual CISO®

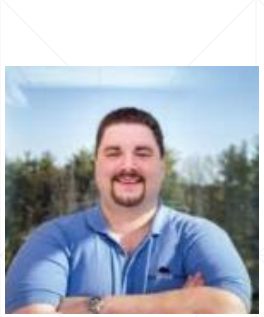
Previously:

- Dartmouth College
- Kearsarge Consulting
- USAF Security Operations Center

Sajjal Akram
CySA, NSE 5,
Dir., Security Ops Center

Previously:

- Senior Cyber Engineer, Ebryx PTC
- MS, BS, National University for Science and Technology



Mark Constantino
Dir., IT

Previously:

- President, MC Computer and CEO, MyCloudCure
- IT at Convenient MD
- IT at Dartmouth Hitchcock

Adam Lange
CISSP
Virtual CISO®
CMMC Specialist

Paul Wagner
CISSP
Virtual CISO®
CMMC Specialist

US Department of Labor Hire Vets "Platinum" Award Winner

Why Trusted Internet? Security Specialists, Experience, Education, Price

Formal Education, Experience

- Most IT companies use new graduates to run IT or manage an operations center
  - 83% of our team have Masters Degrees
- Deep bench in large enterprise companies
- Personality Diversity and Expert advise

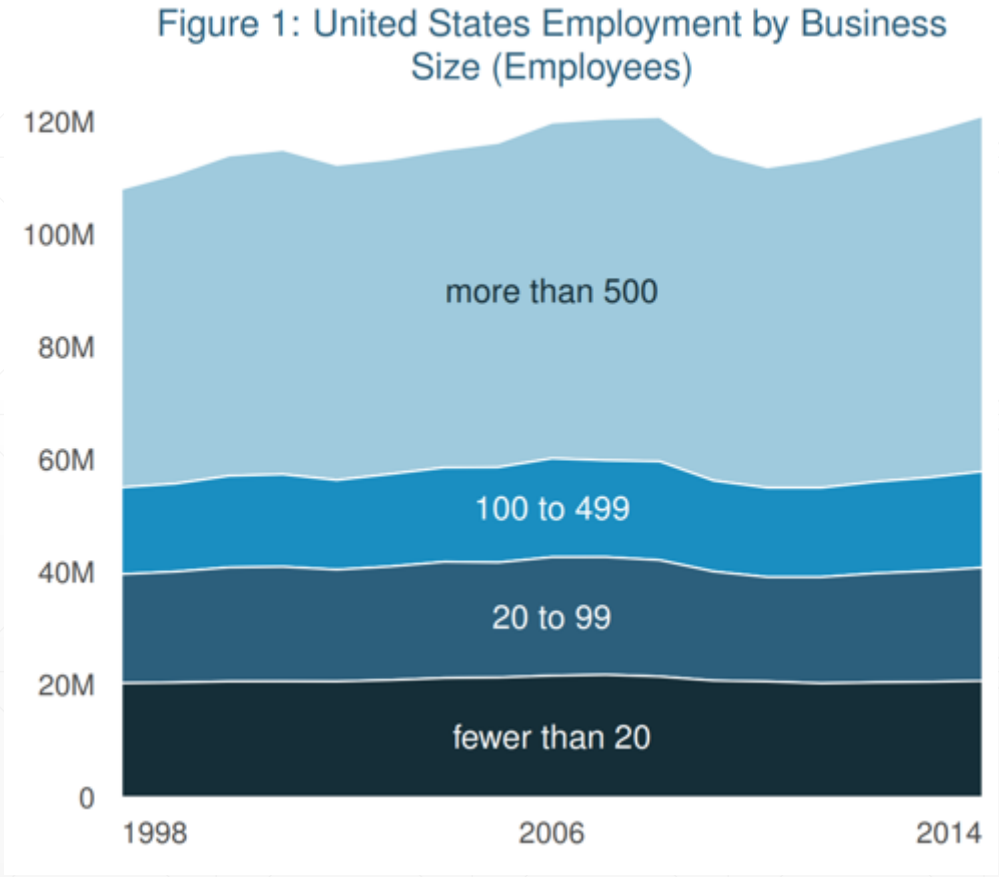
Professional Certifications

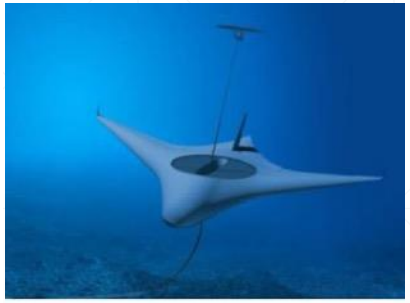
- 39 Certificates, including
  - 9 CISSPs
  - 1 CISA
  - **6 NSE 4**
  - **9 NSE 5**
  - **1 NSE 7**
  - IT Audit, ISO 27001, Cisco, **Fortinet**

Priced at approximately 40% of current market rates.

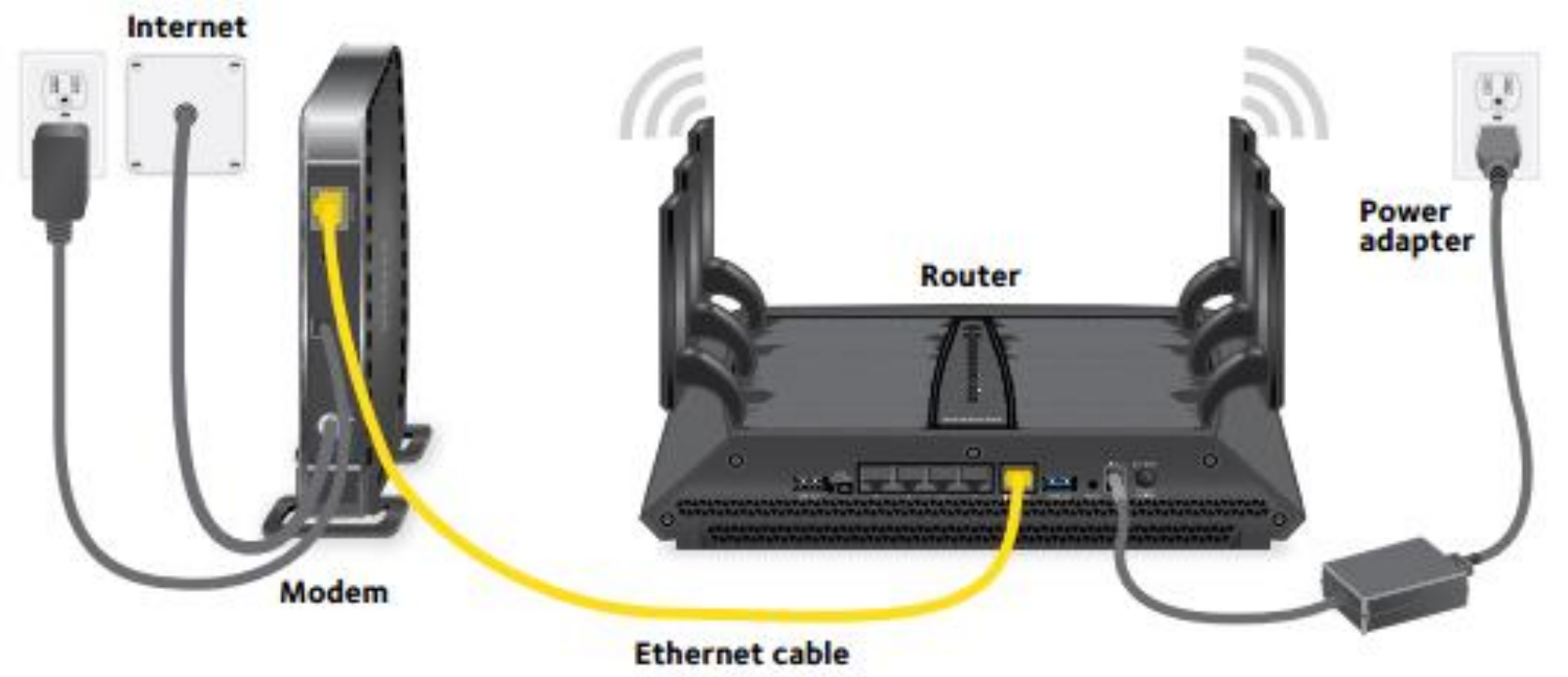
Our clients? High and Ultra High Net worth Families and their companies

- **Approximately 125 current customers**
- **Smallest: 1. Largest: 3500**
- Families, Manufacturing, Oil and Gas, Defense, Finance, Internet, Exec Homes, Family Offices





This is what we normally see

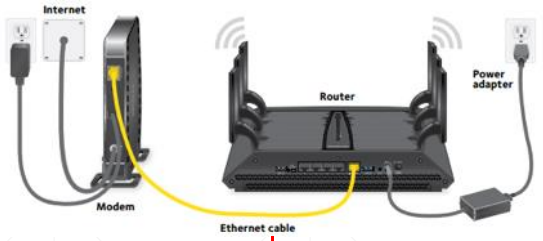


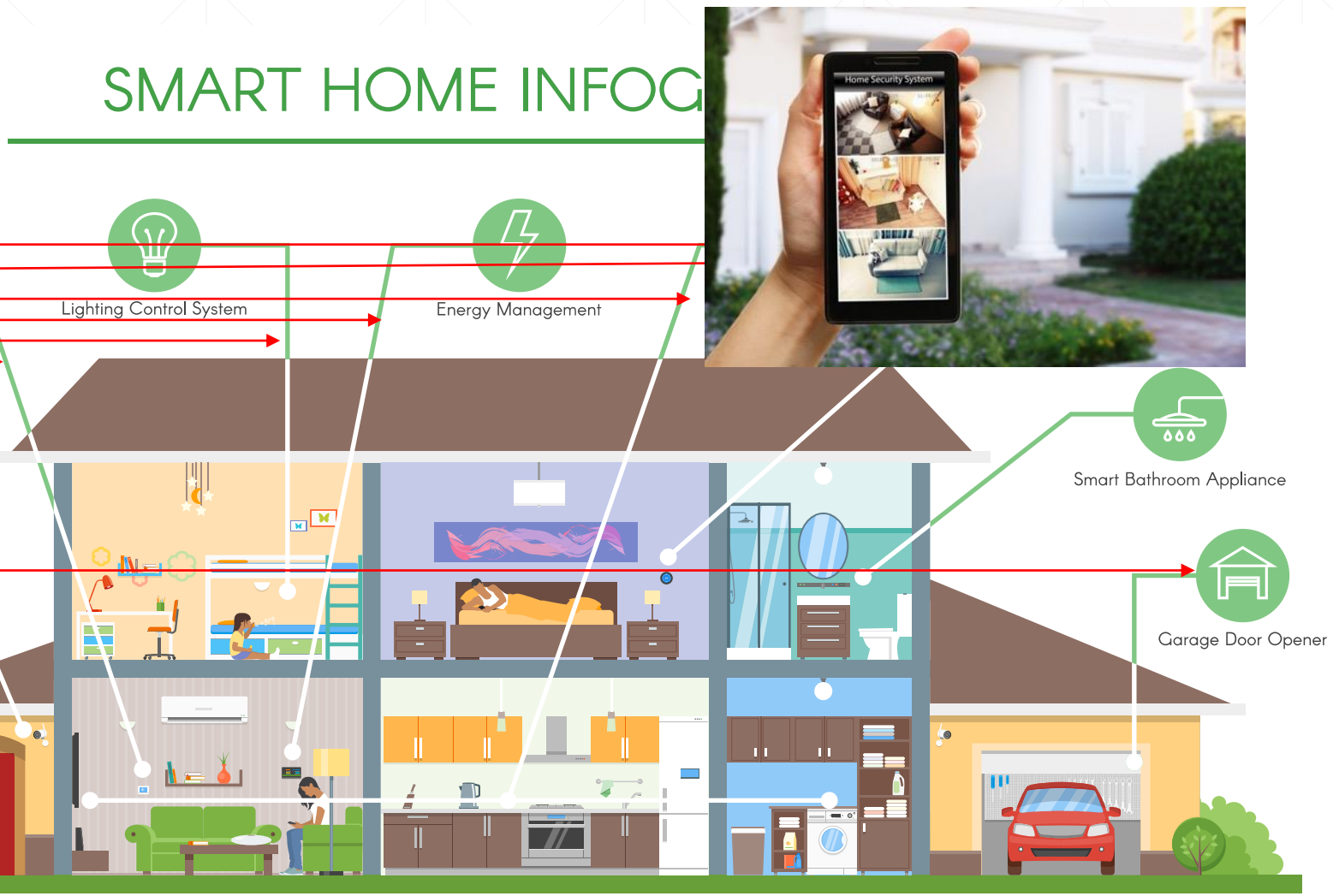
This architecture is unprotected.

It causes bad things to happen.

If you can see your home, office, or computer remotely on your phone.. Others may also.

TRUSTED INTERNET®





Executive Home Compromise

Word of mouth is our best advertising.

This client referred us to her CEO resulting in signed new sales.

Orange County, CA

- Company partner and Number two sales producer hacked
- **$82,000 stolen from her bank accounts between Feb and Mar 2019**
- She was hacked through her home wireless router. Company got hacked through her.
- Responded in <12 hours
- Secured the home
- Contacted banks, credit card companies, more. Locked down accounts.
- Virtual CISO assigned. Money restored through Insurance.

During the Ukrainian Presidential Election (2014):

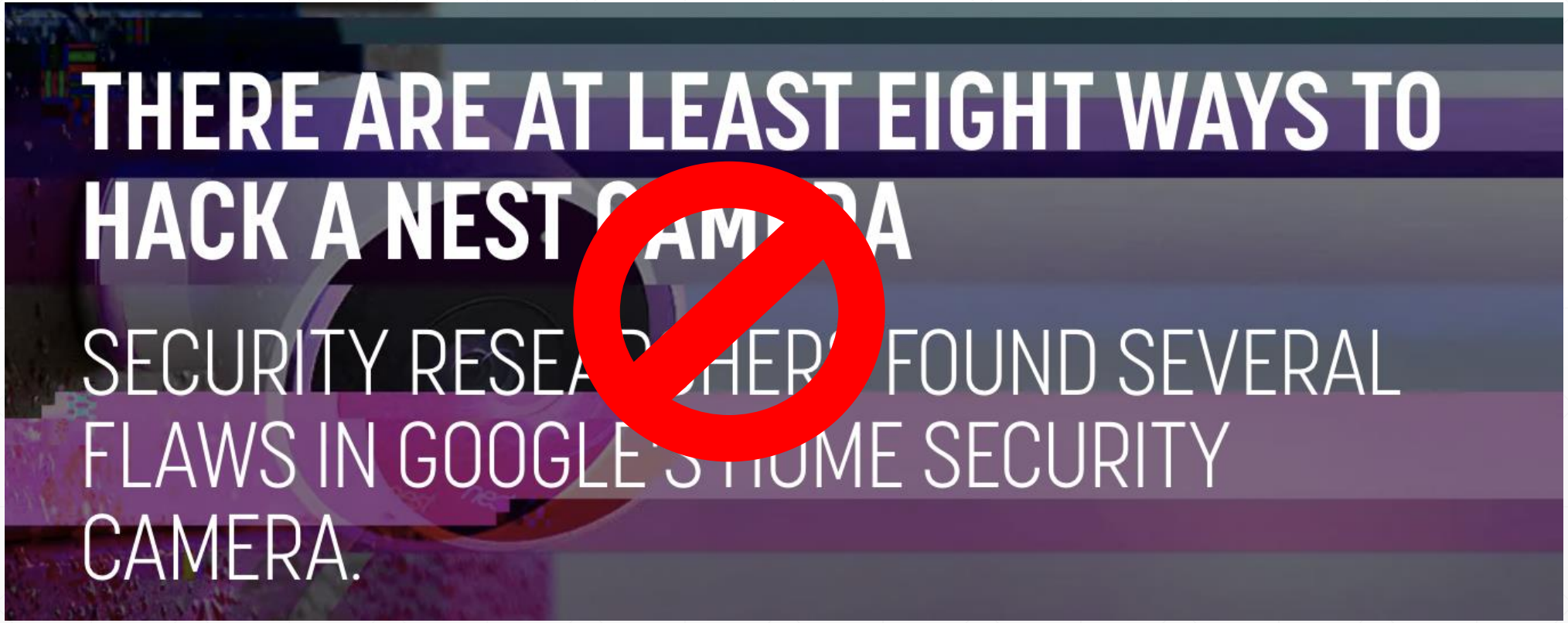
- Smart TV's used to collect intelligence
- Traffic cameras used to monitor movement
- Cellular was denied service
- Texting used for propaganda and psychological operations

Ukraine election narrowly avoided 'wanton destruction' from hackers

SOURCE: Christian Science Monitor, *June 17, 2014*

TRUSTED INTERNET®

“Don’t forget to grab your purse.”



You need to design a Defense in Depth Strategy Fast.

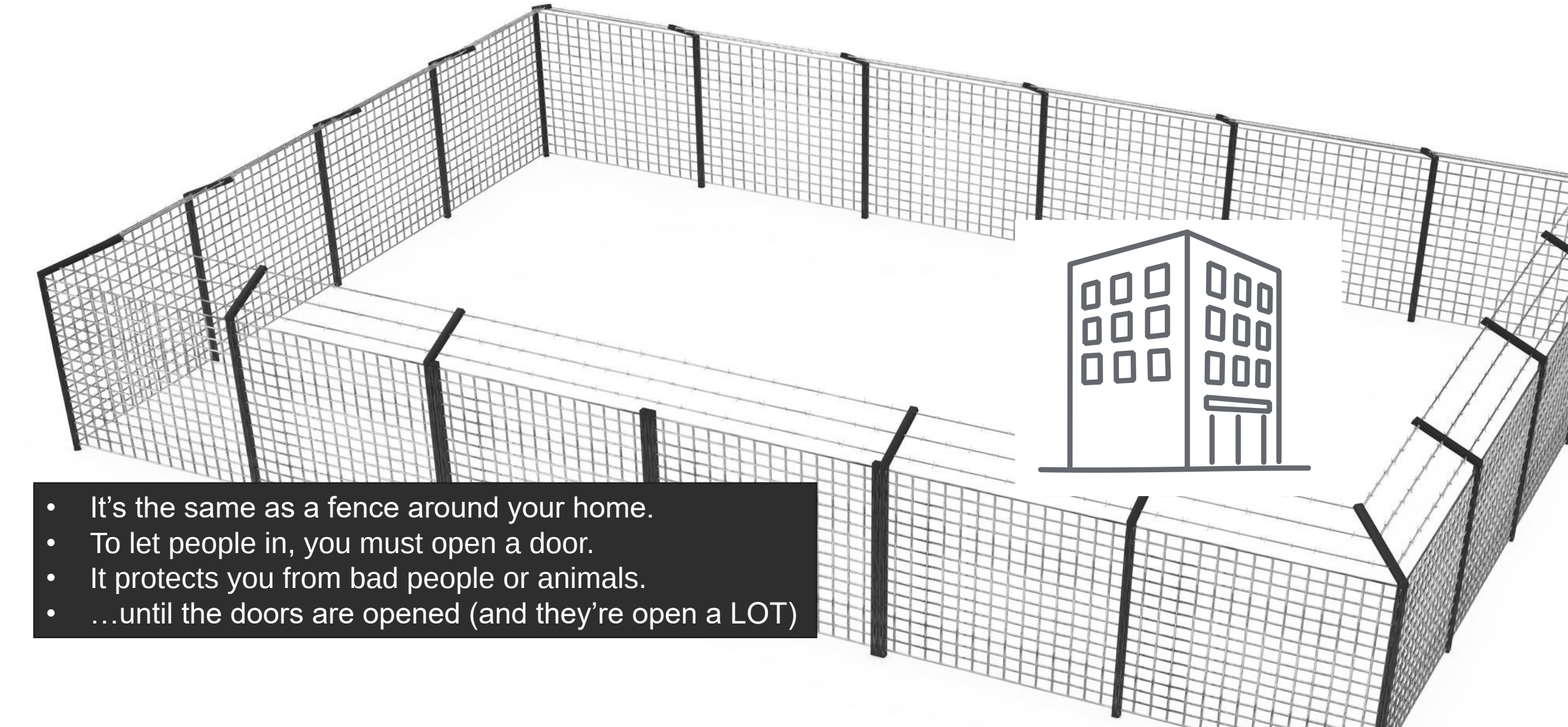
Cyber Security 101

Now.. The good stuff…

Your mission: PROTECT THIS HOUSE!

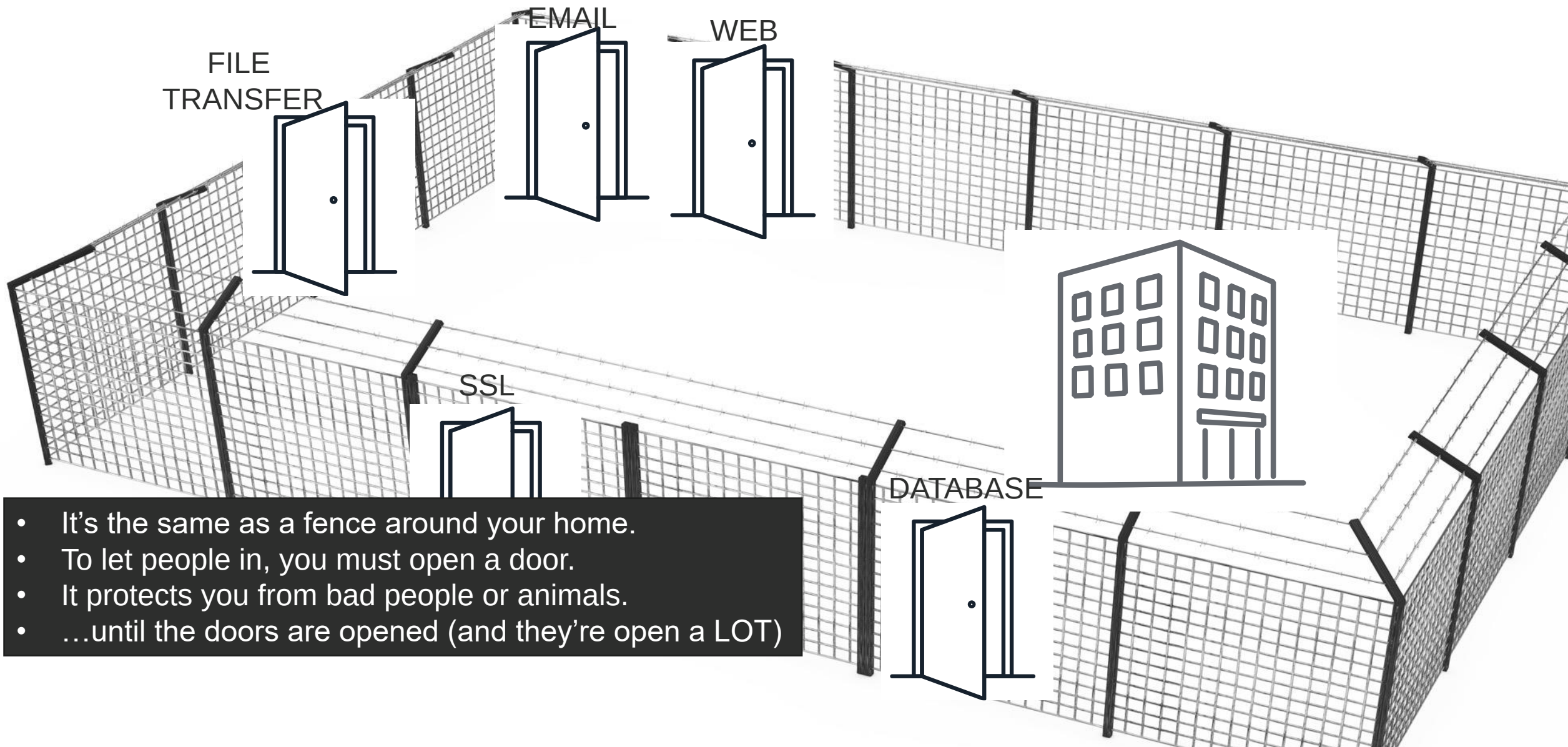
- **From…**
  - Ransomware
  - Email based attacks (phishing, spam, BES)
  - Automated, high-speed BotNets
  - Espionage
  - Keystroke loggers
  - Others??

This is a **Firewall**.



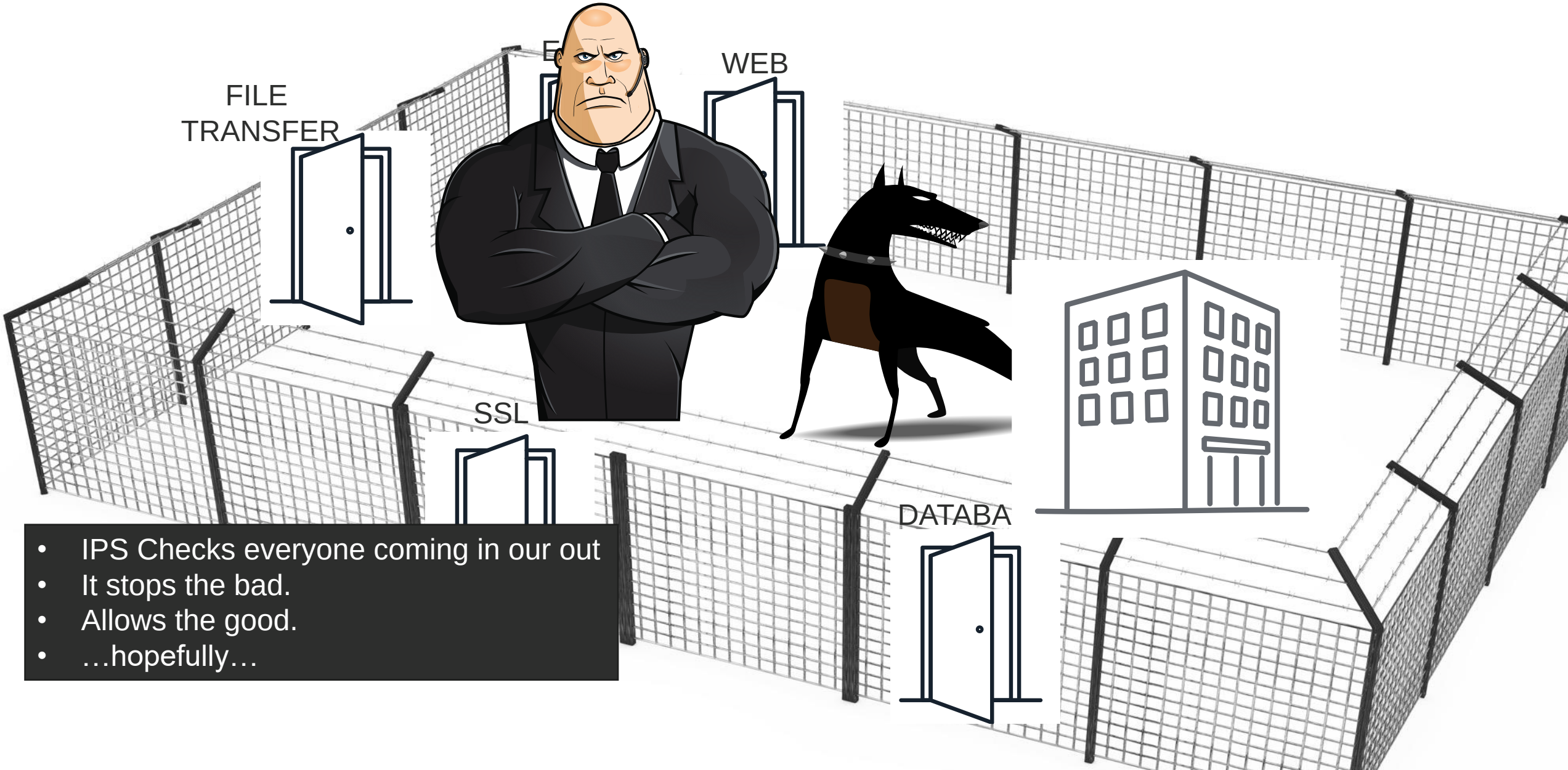
- It’s the same as a fence around your home.
- To let people in, you must open a door.
- It protects you from bad people or animals.
- …until the doors are opened (and they’re open a LOT)

This is a **Firewall**.



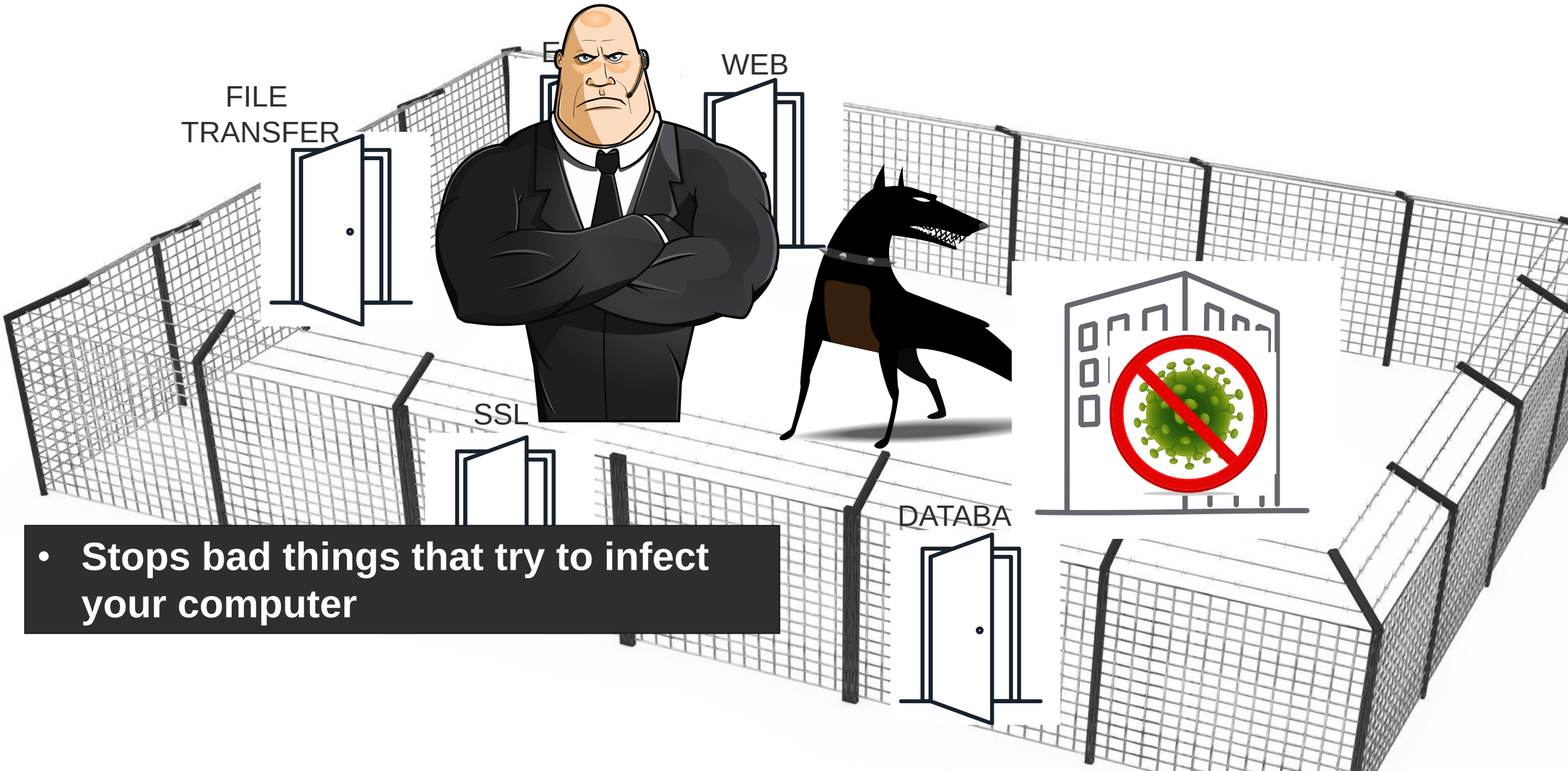
- It’s the same as a fence around your home.
- To let people in, you must open a door.
- It protects you from bad people or animals.
- …until the doors are opened (and they’re open a LOT)

This is an Intrusion Prevention System (IPS)



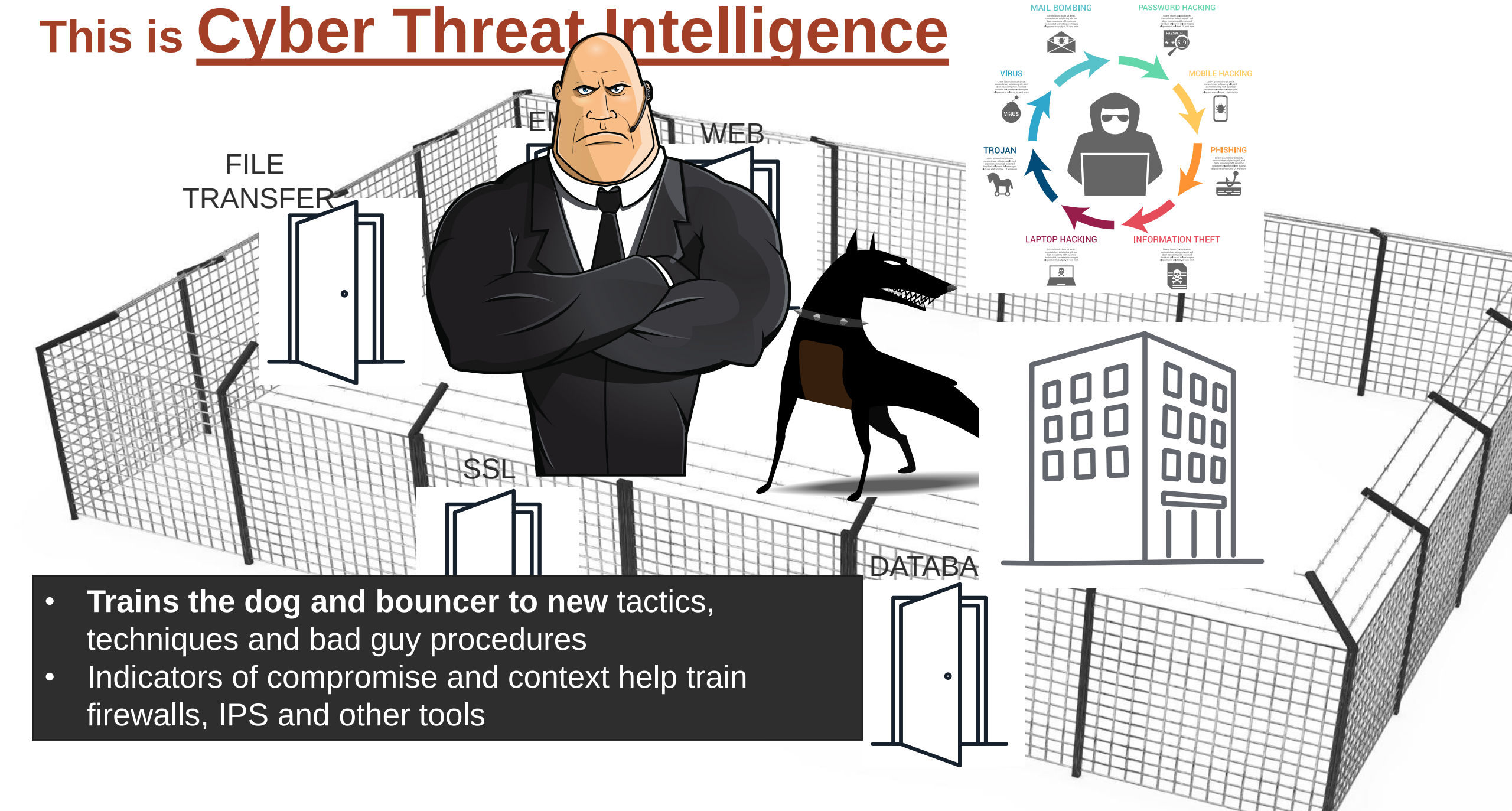
- IPS Checks everyone coming in our out
- It stops the bad.
- Allows the good.
- …hopefully…

This is ANTI-VIRUS.



- **Stops bad things that try to infect your computer**

This is Cyber Threat Intelligence



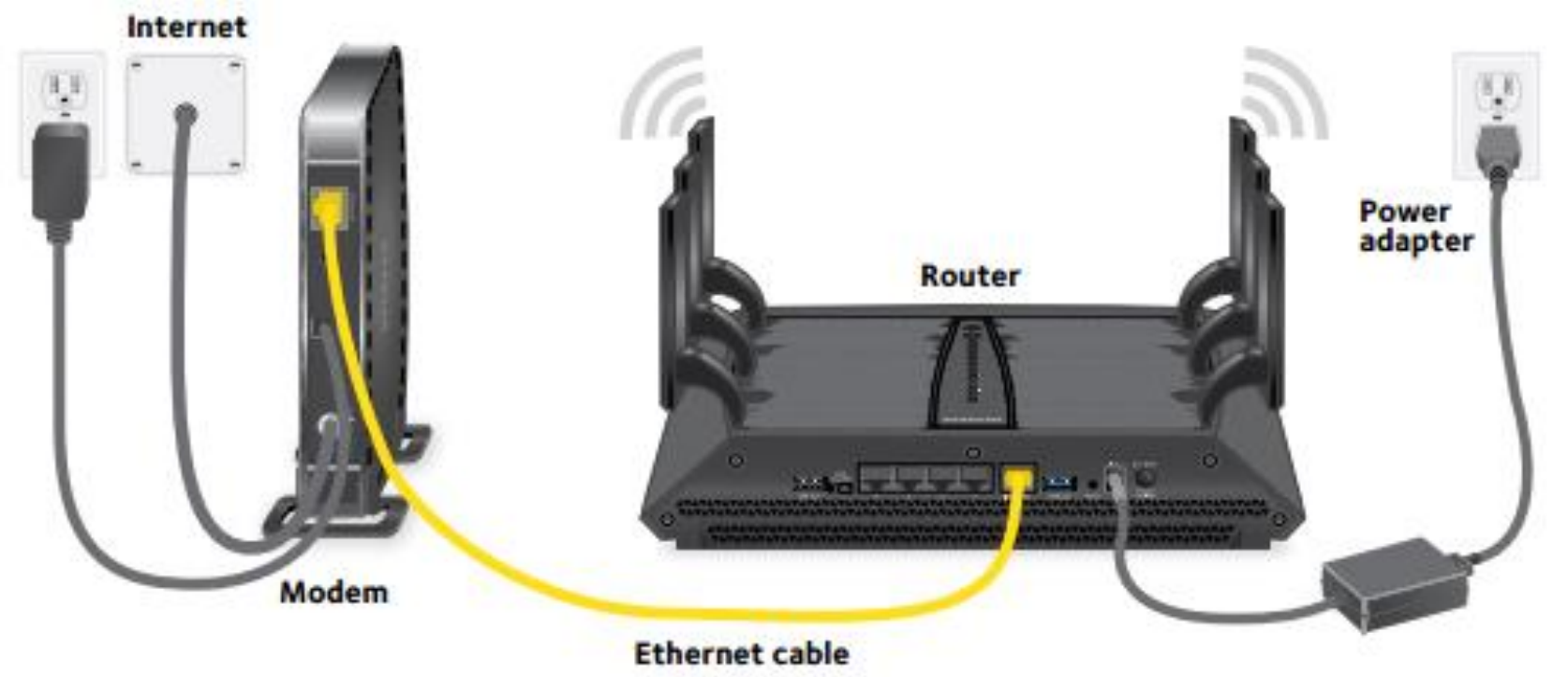
- **Trains the dog and bouncer to new** tactics, techniques and bad guy procedures
- Indicators of compromise and context help train firewalls, IPS and other tools

And.. Email? Systems in the cloud?

- It’s no different.
- Tools like Avanon, Proofpoint, Mimecast and others read your email before you see it, to filter out fake or malicious emails before they get to you.

Here’s what it looks like in real life

This is what we normally see

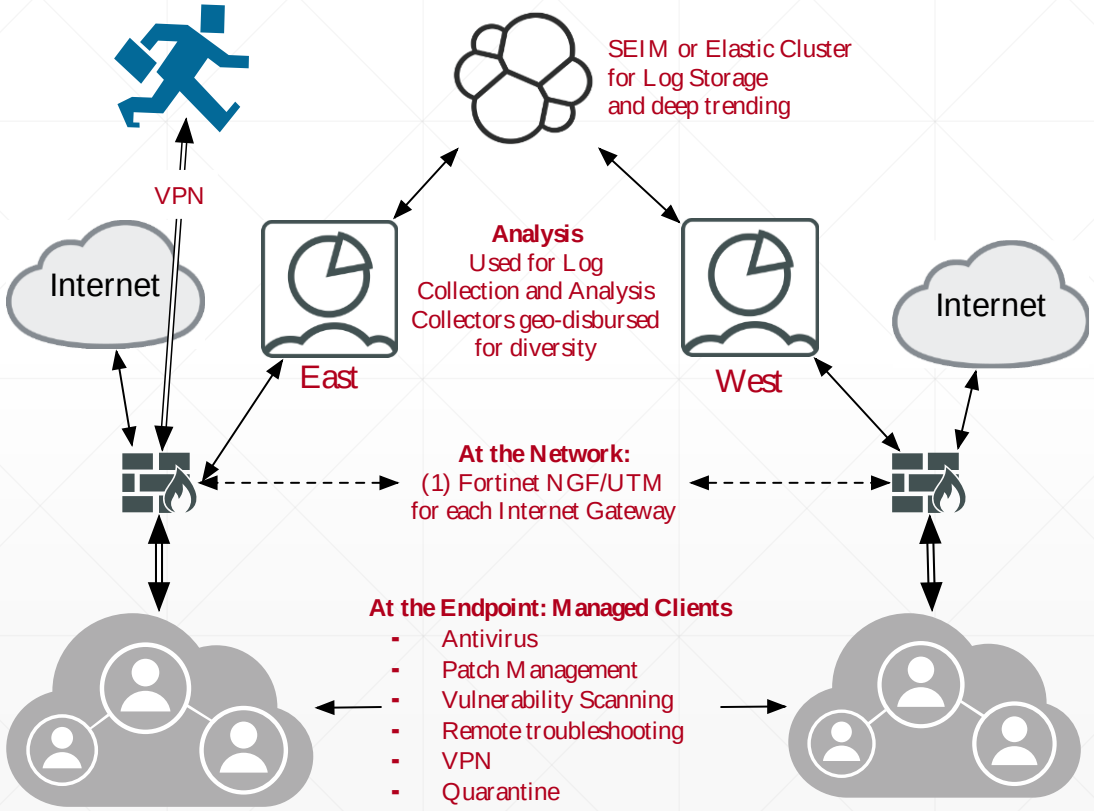


This architecture is unprotected.

It causes bad things to happen.

Baseline Reference Architecture

This is what we install and/or model against during crisis or pre-crisis.

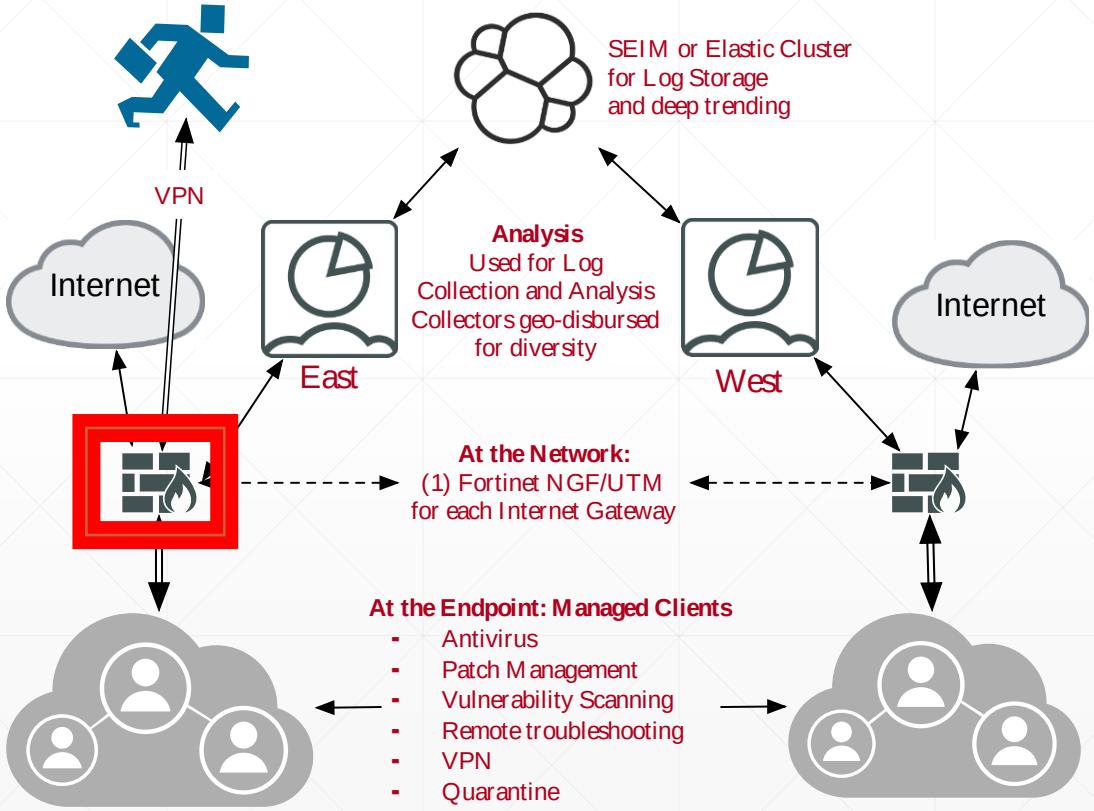


Insurance companies (and CEOs) love our Trusted Internet Reference Architecture…

"My Insurance premium savings paid for all of the work Stutzman and his team did!"

CEO "Omega"

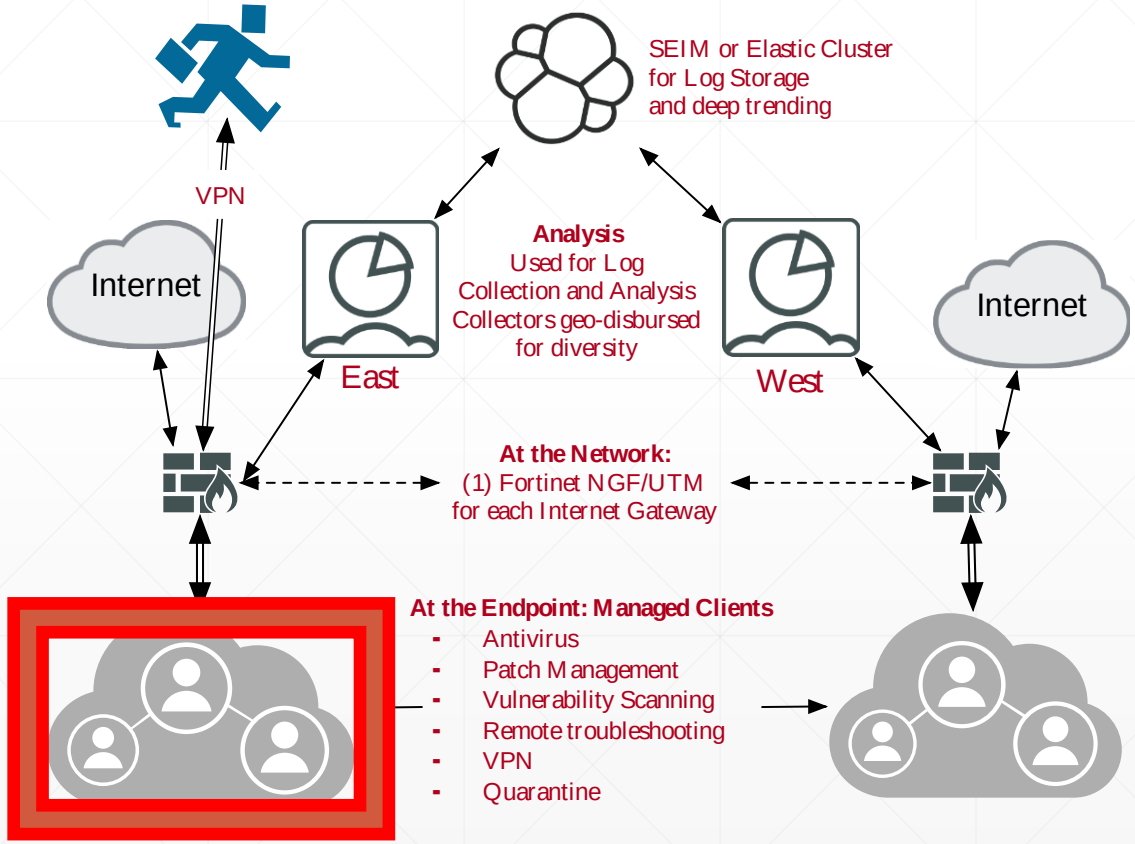
Next Generation Firewall – Placed behind your Internet Connection (i.e. Comcast Modem or Border Router)



Next Generation Firewall (the fence)

- Intrusion Prevention System (the bouncer and dog)
- Anti-virus (removes malware before it comes in or leaves)
- DNS monitoring
- Cyber Threat Intelligence
- More!!!

On the computer? Anti-Virus, Anti-evasion



FortiClient

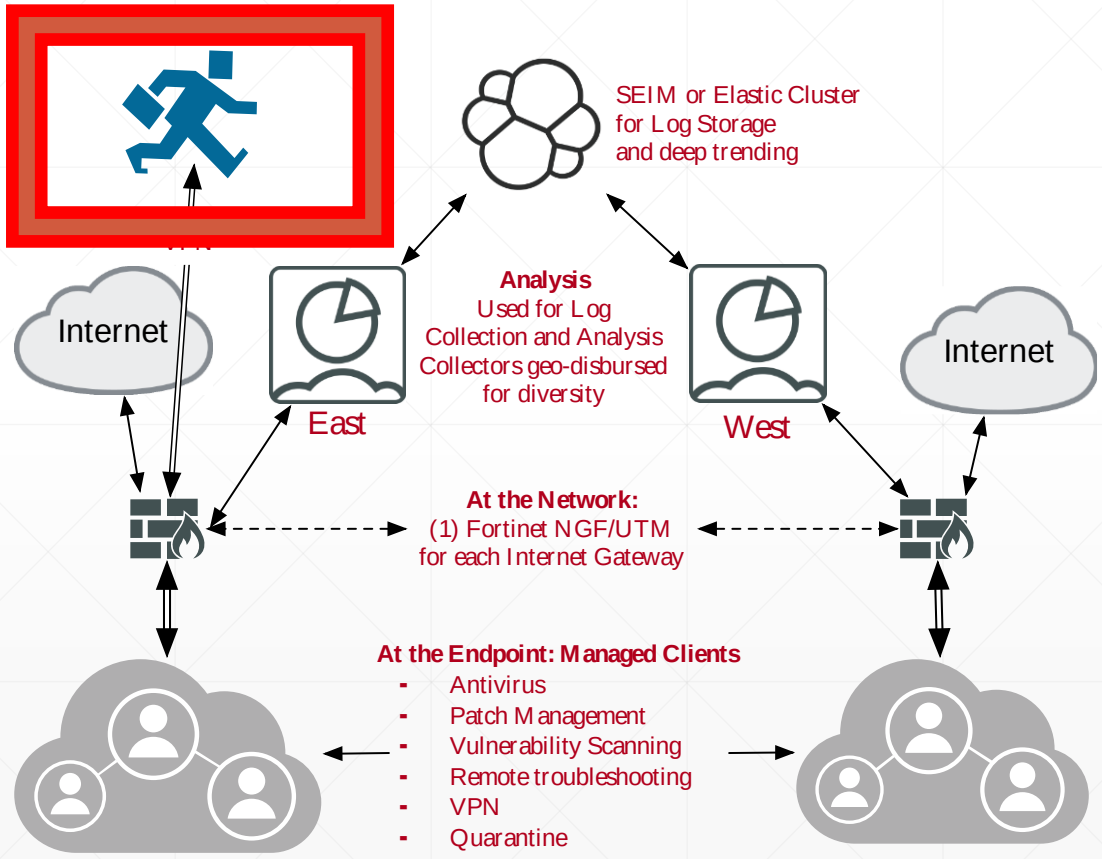
- Managed Anti-Virus
- Vulnerability and Patch status
- 24x7 telemetry connections to the firewall and analysis suite for proactive automation
- Automated quarantine operations
- Optional Always-On SSL or IPSEC VPN

Minerva's Armor

- Anti-evasion and Deception
- Behavior based analytics

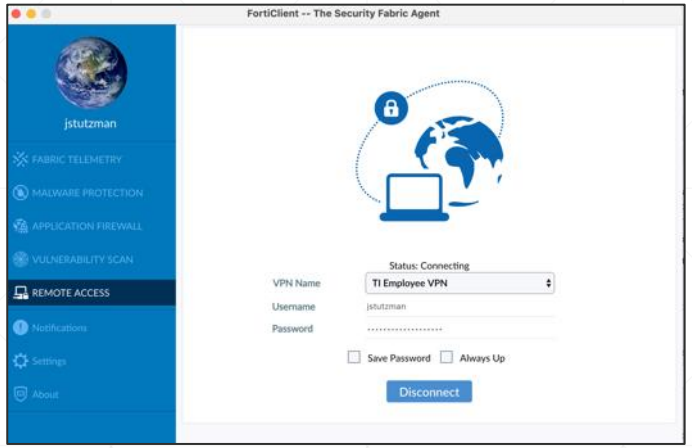
Virtual Private Network

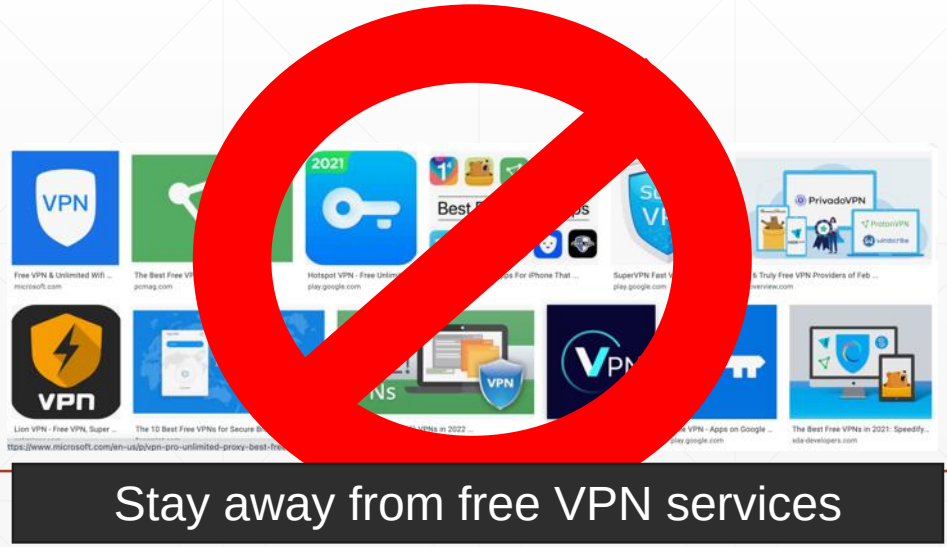
Every endpoint receives FortiClient and Minerva's Armor and/or Cybereason



Virtual Private Network

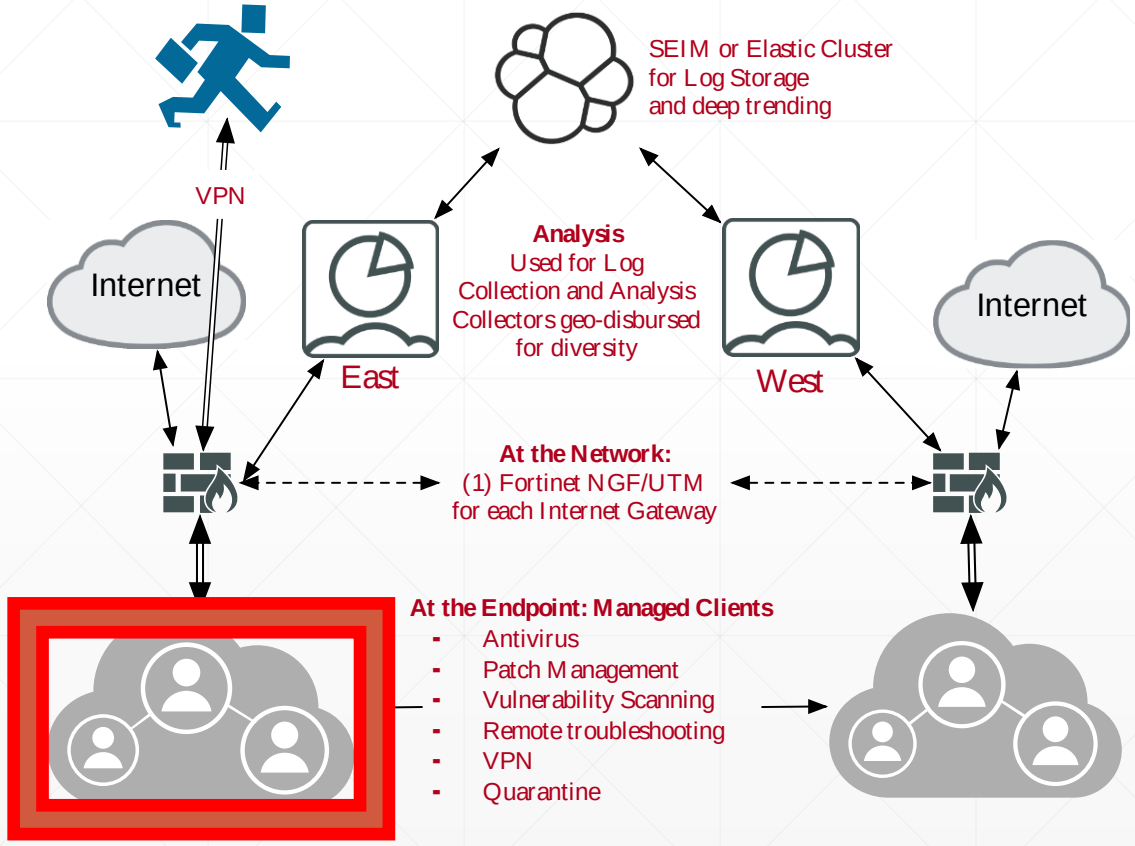
- **Encrypted communications**

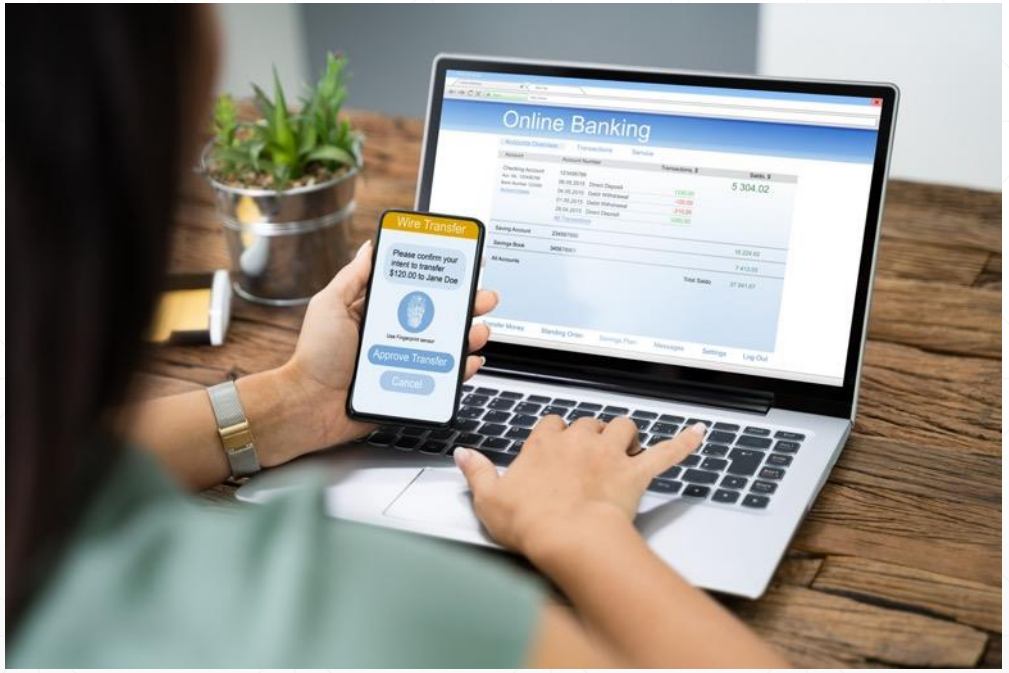




Stay away from free VPN services

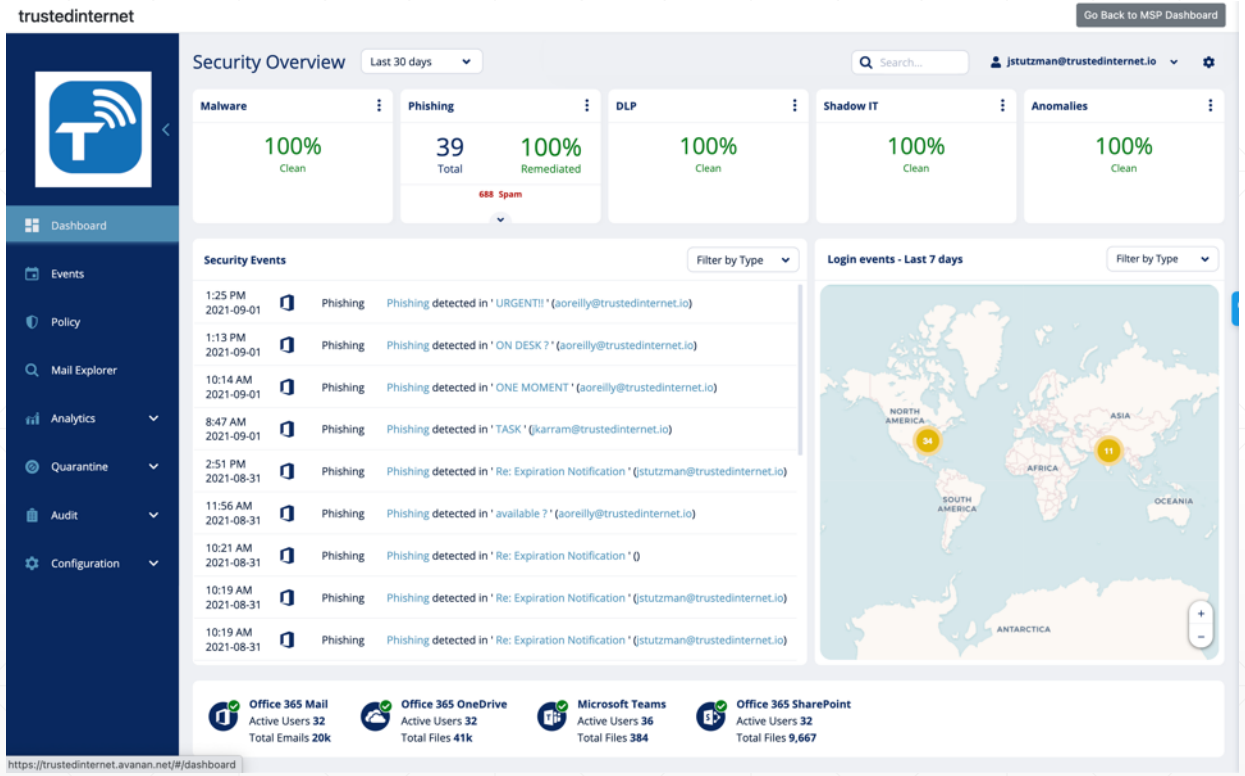
Two Factor Authentication



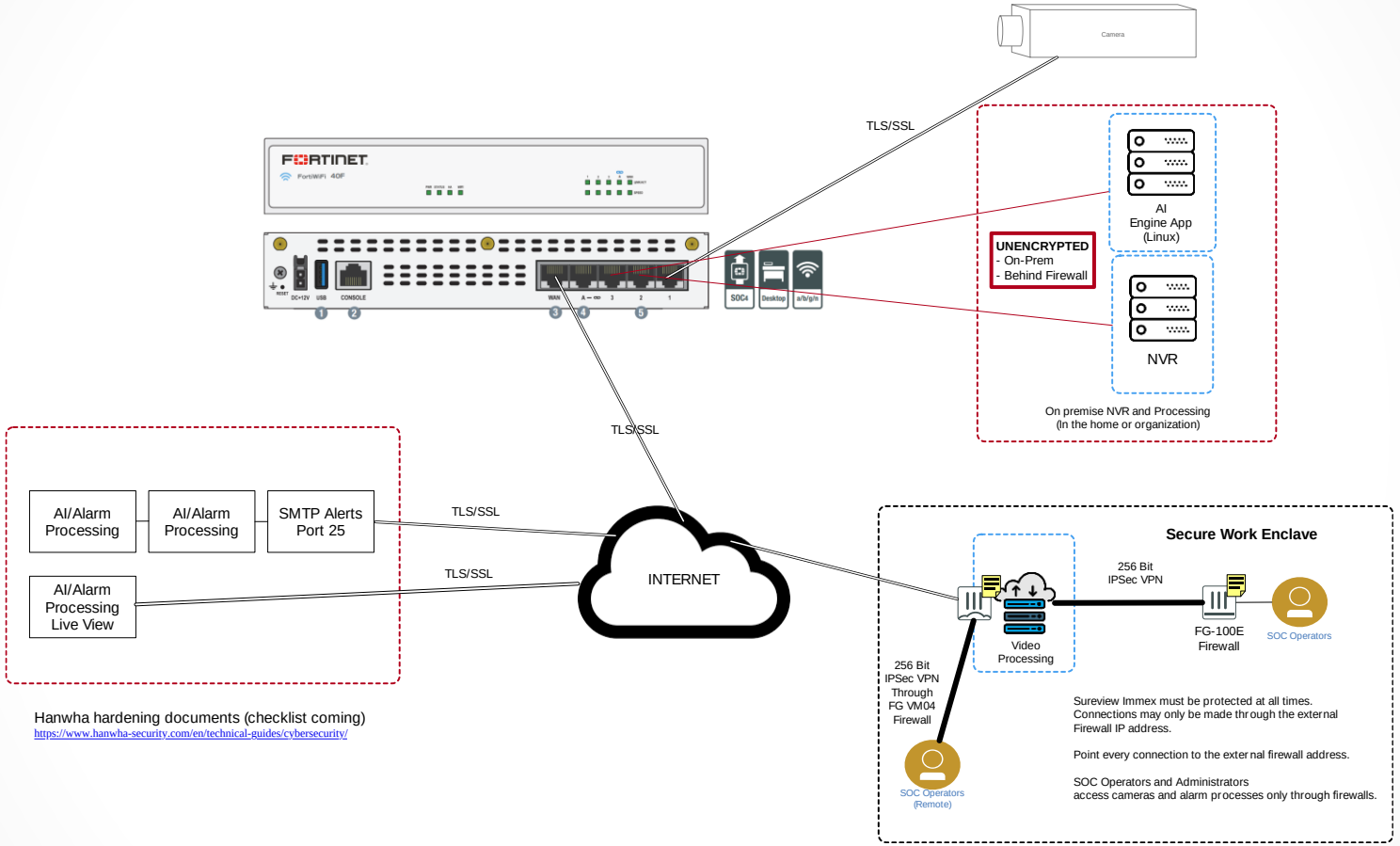


And threats from Email

- Avanon sits in the cloud
- Protects against threats targeting O365 and Google Mail, Dropbox, Google Drive, Slack, and more.
- AI and Machine learning read emails for threats
- Automatically quarantines phishing, spam, potential BES, and more.
- Very proactive. Low cost, high payoff.



Protecting physical security systems



Hanwha hardening documents (checklist coming)
https://www.hanwha-security.com/en/technical-guides/cybersecurity/

Video Surveillance

Video Surveillance and Security Systems are compromised nearly 100% of the time.

This is our Reference Architecture for Secure Integration.

TRUSTED INTERNET

Key Takeaways

TRUSTED INTERNET®

Heightened Security Threat from Warfare, Hactivists, and Sympathizers

- Ransomware
- Business Email Compromise
- Physical Security System Security
- Smart Home Systems
- Personal Cyber Security

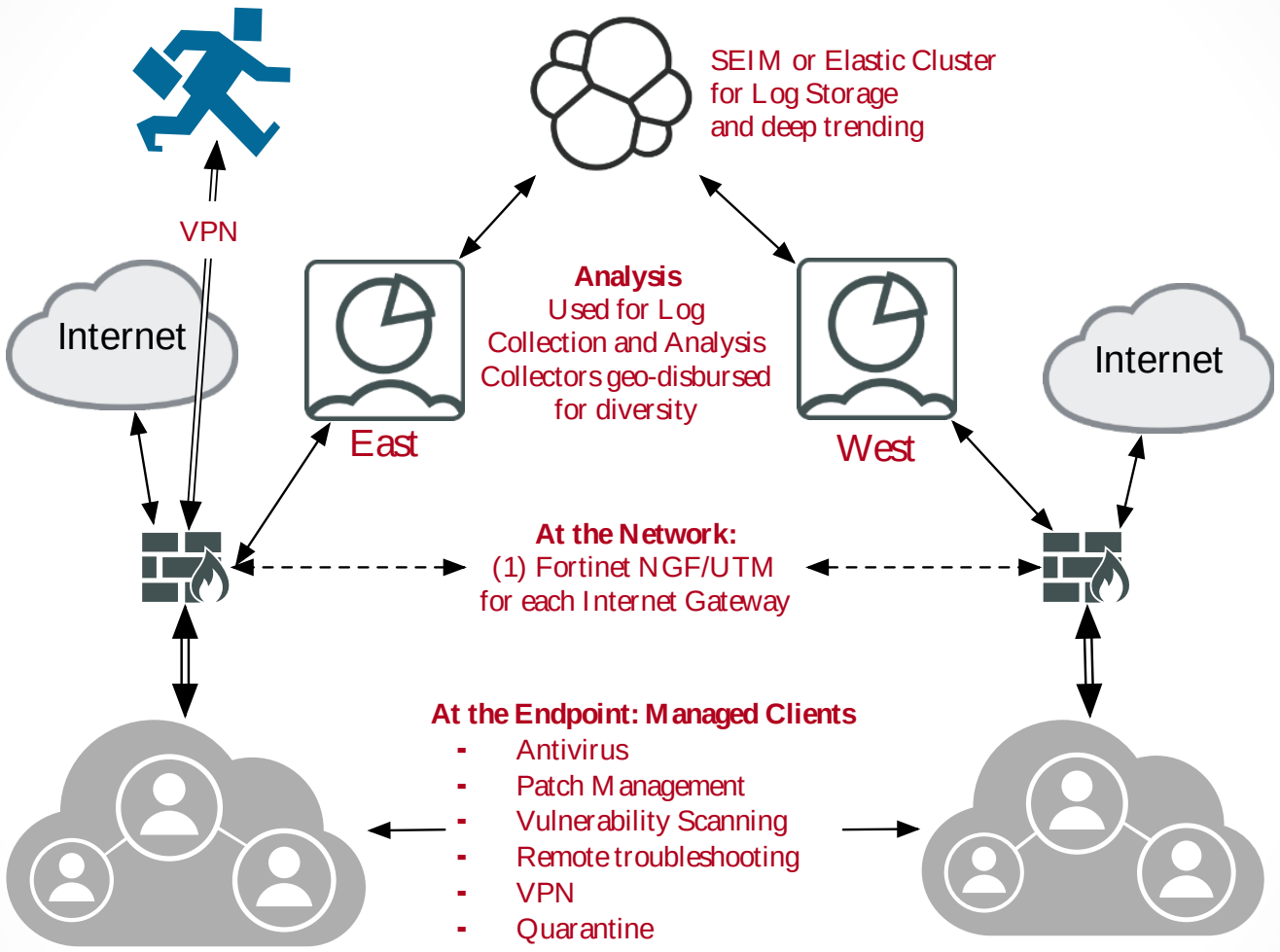
Key Points

Proactivity is cheaper than incident response.

- **Insurance may help, and will give you money, but… not time, frustration, burnout, or lost data**

Key Points

Physical security systems are almost never considered, but always targeted (and hacked).



TRUSTED INTERNET

Key Points

Defense in depth doesn't have to be expensive to be effective.

Key Points

Know your tools.

Even the best tools don’t work if you don’t know how to use them.

Last

Have a plan –and practice it. Tabletop exercises go a long way.

How to contact Trusted Internet for help:

Concierge: 800-853-6431

staysafeonline@trustedinternet.io

When you're connected. You're protected.(R)

TrustedInternet.io

JUST IN CASE

TRUSTED INTERNET®

Q&A