

Cybercrime Kill Chain vs. Defense Effectiveness

Results from NSS Labs Security Testing

Dr. Stefan Frei, Research Director

Twitter @stefan_frei



Trusted Advice. Measured.

Speaker – Dr. Stefan Frei

■ Professional

- Research Director @ NSS Labs
- Research Analyst Director @ Secunia
- Senior Researcher & Pentester @ ISS X-Force



■ Contact

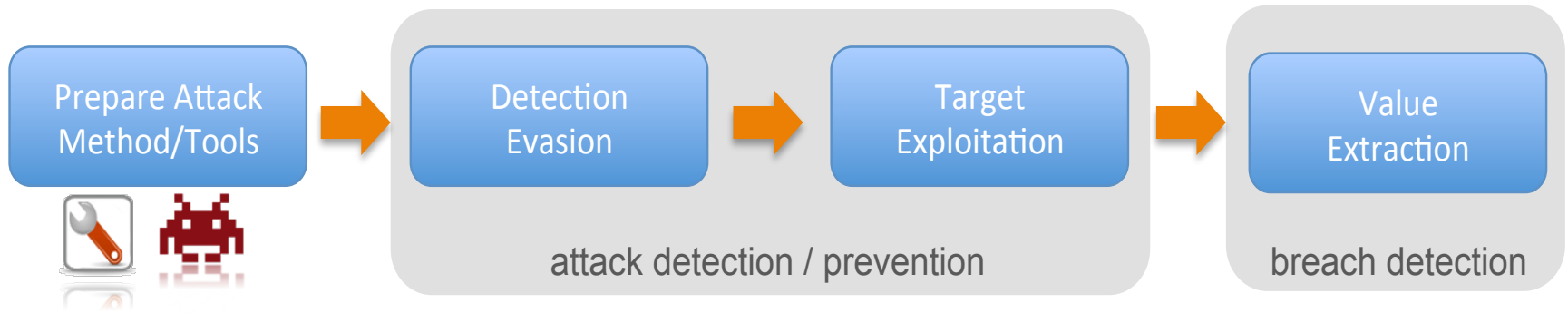
- Mail sfrei@nsslabs.com
- Twitter [@stefan_frei](https://twitter.com/stefan_frei)

Agenda

- How we get attacked
- Layered Defense
- Results from NSS Labs' testing
- Conclusion

Attack Kill Chain – Understand Attacker

Attackers View



Defenders View

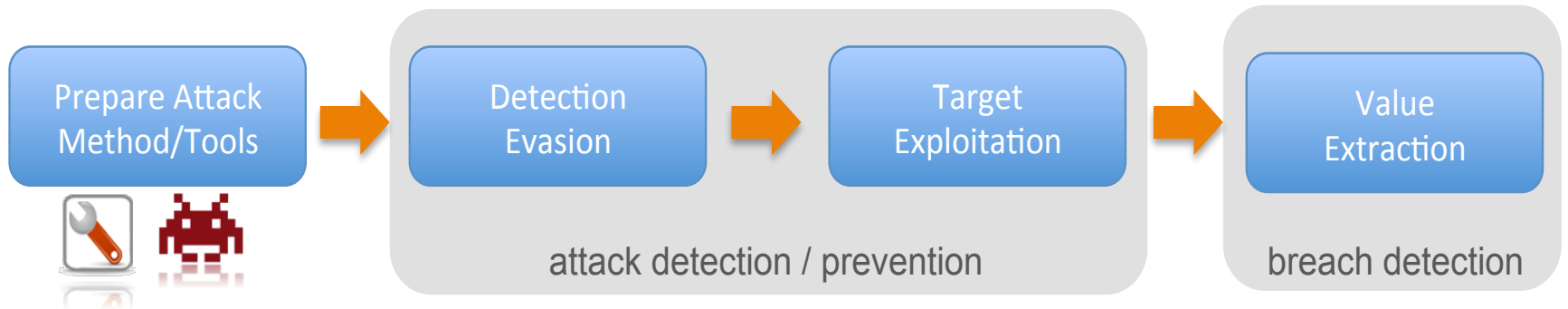
Attack Kill Chain – Understand Attacker

Understand the threat and the attackers motivation & methods



Attack Kill Chain – Understand Evasion

Understand how malware
bypasses detection



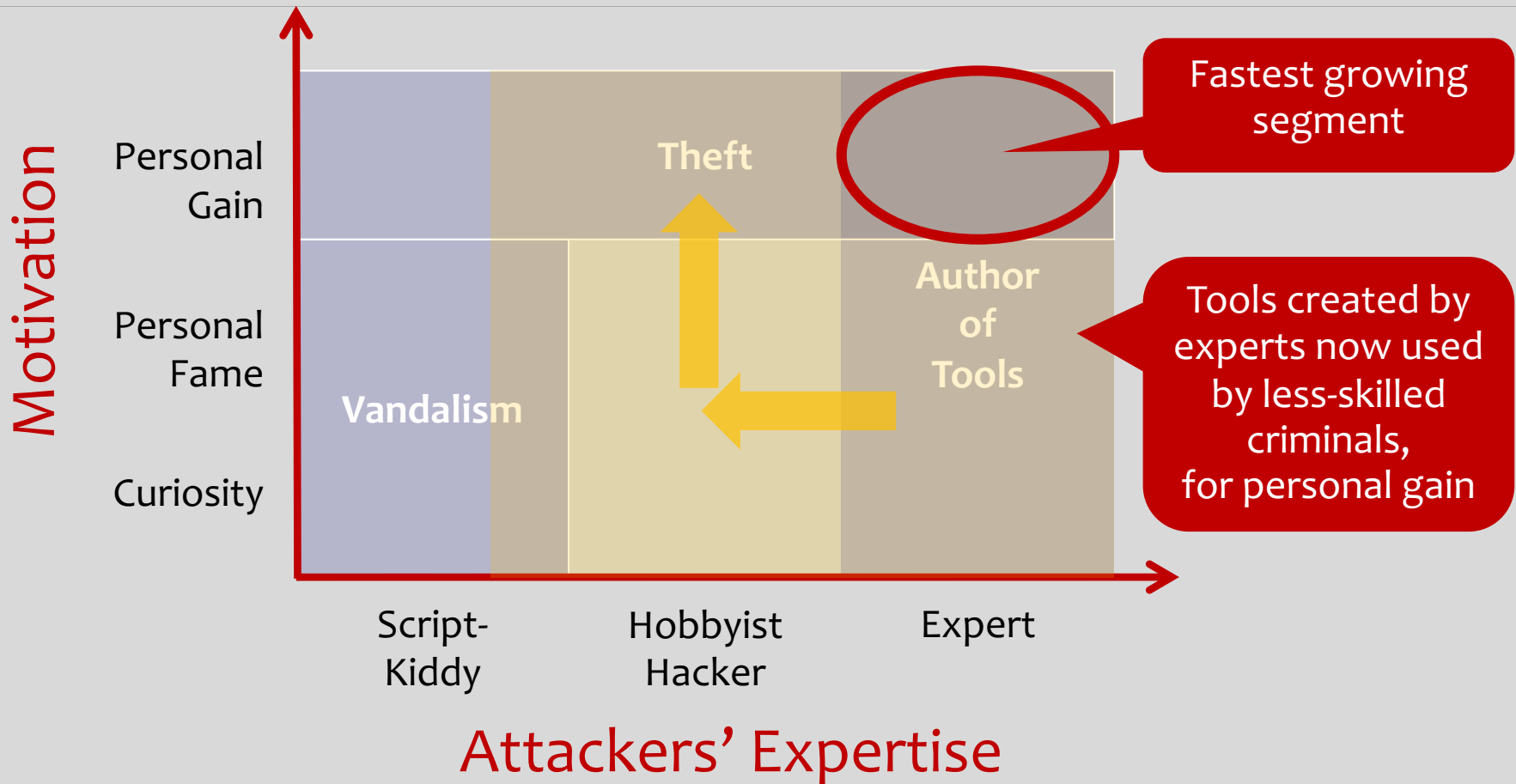
Assess the effectiveness
of layered defenses

Attack Kill Chain – If prevention failed



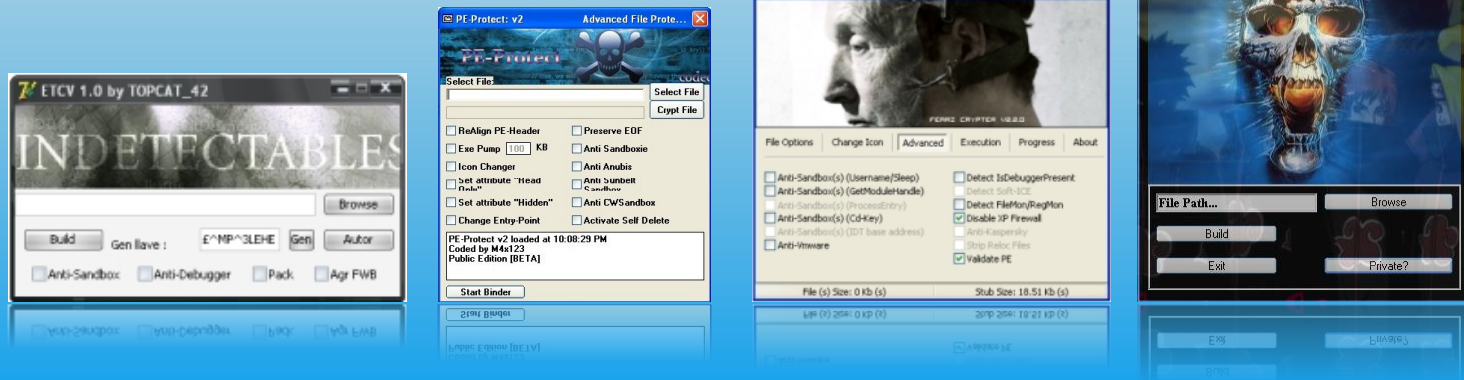
^
Detect &
neutralize

The Changing Threat Environment

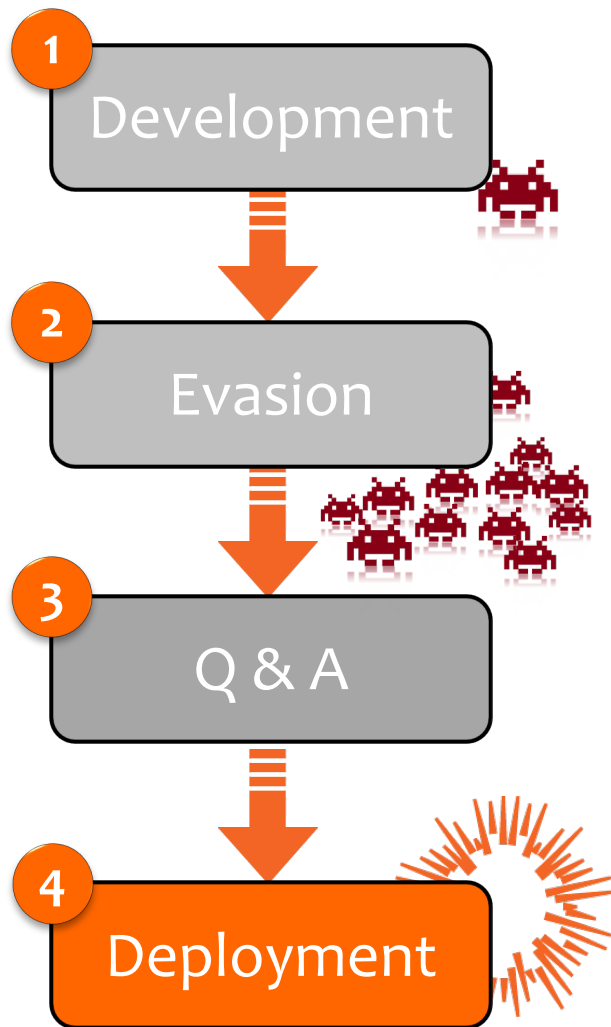










Malware Development & Tools

- Cybercriminals developed formidable tools
Easy to use development tools, Q&A, and service level agreements as in every mature industry
- Detection Evasion and Resilience
By design, malware is developed and deployed with detection evasion in mind



Malware Development Process



1. Create malicious tool 1 x 
2. Obfuscate malware, create permutations 10,000 x 
3. Test against detection engines 5,000 x 

4. Deploy undetected samples    

Underground Market

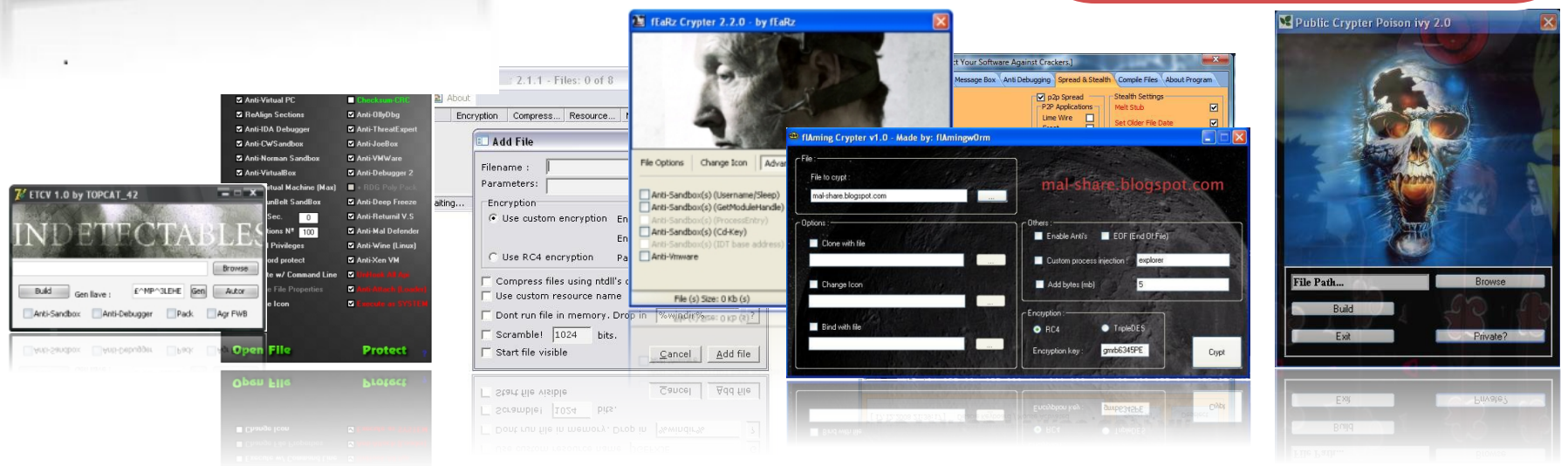


Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/Vista
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249\$ (United State Dollar)

Malware offered for **\$249** with a Service Level Agreement and replacement warranty if the creation is detected by any anti-virus within 9 months



The Availability of Malware Tools ..



Results in a high degree of attack

automation *from systematic identification of targets to fully automated exploitation*

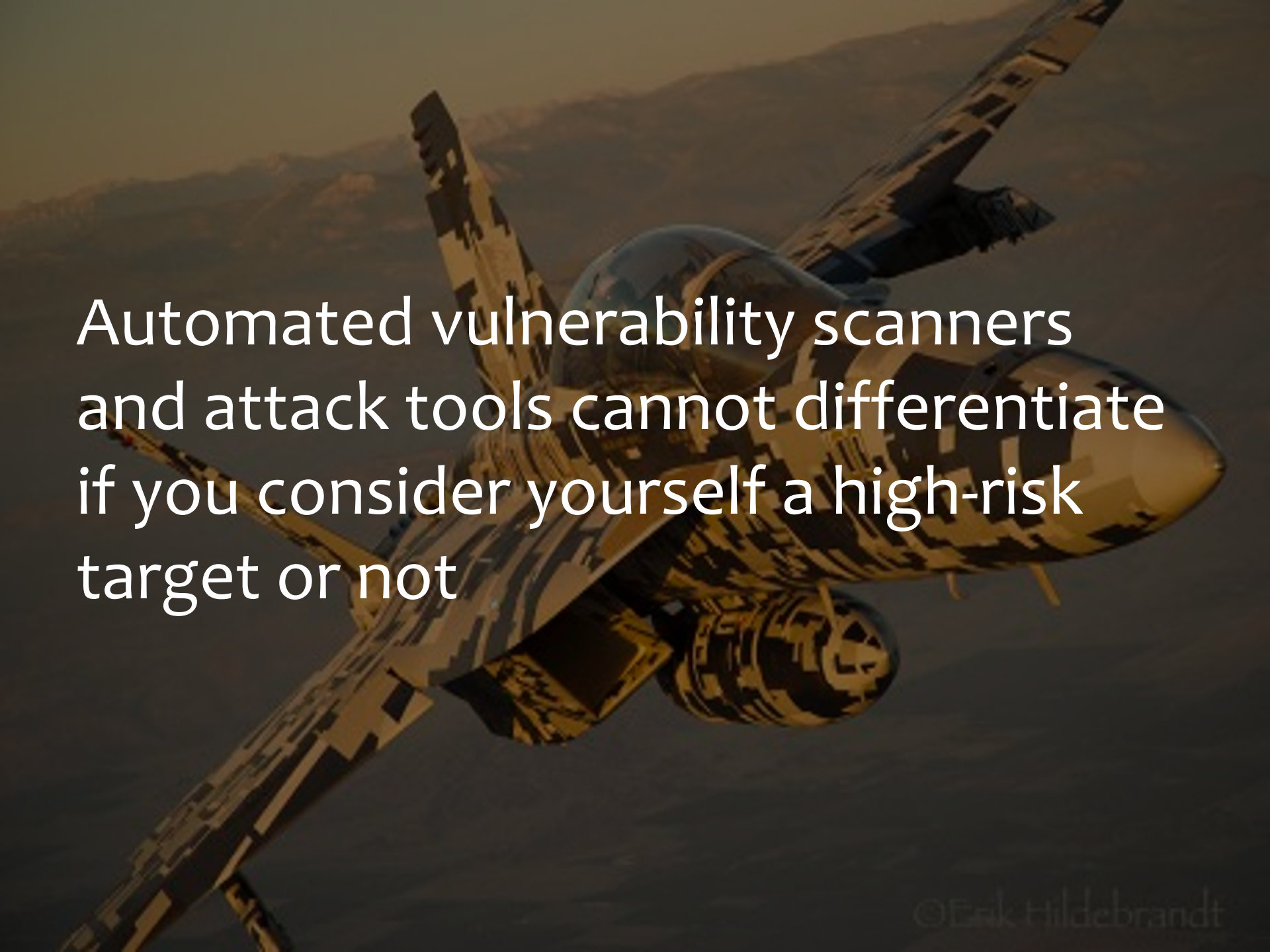


Leads to an increase in opportunistic attacks

as the attacker no longer needs expertise or special skills



***Any enterprise can become a victim of attack:
at any time, for any reason, and without being
specifically targeted.***

A fighter jet, possibly an F-16, is shown in flight against a sunset or sunrise sky. The jet is angled upwards and to the right, with its wings and tail visible. The lighting is warm and golden, creating a dramatic atmosphere. The text is overlaid on the left side of the image.

Automated vulnerability scanners
and attack tools cannot differentiate
if you consider yourself a high-risk
target or not

Our Response: Layered Security

We respond and rely on layered security



Key Security Technologies available:

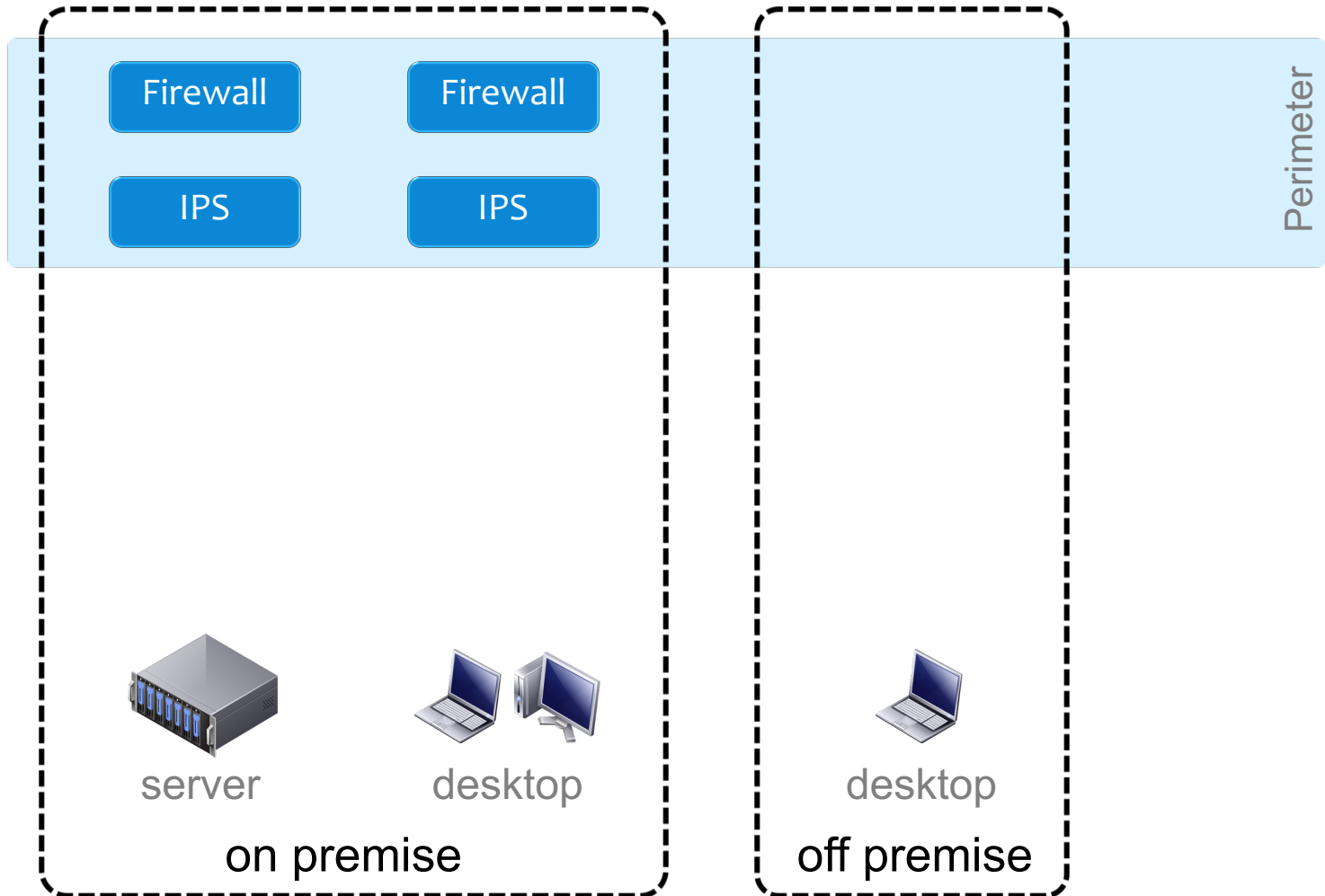
- *Network Firewall*
- *Intrusion Prevention Systems (IPS)*
- *Antivirus / Antimalware*
- *Browser Protection*



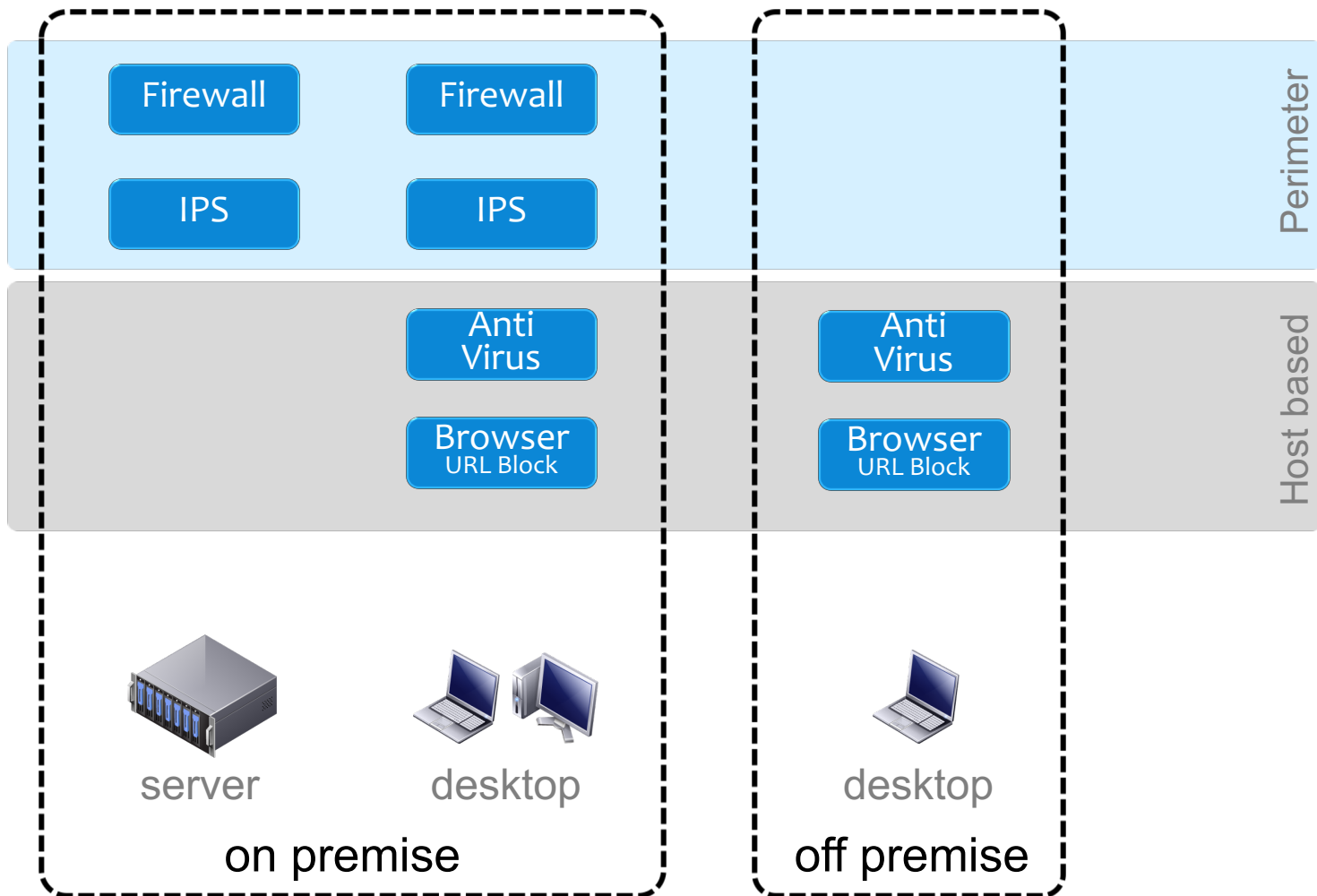
How effective is our defense ?

How do we know?

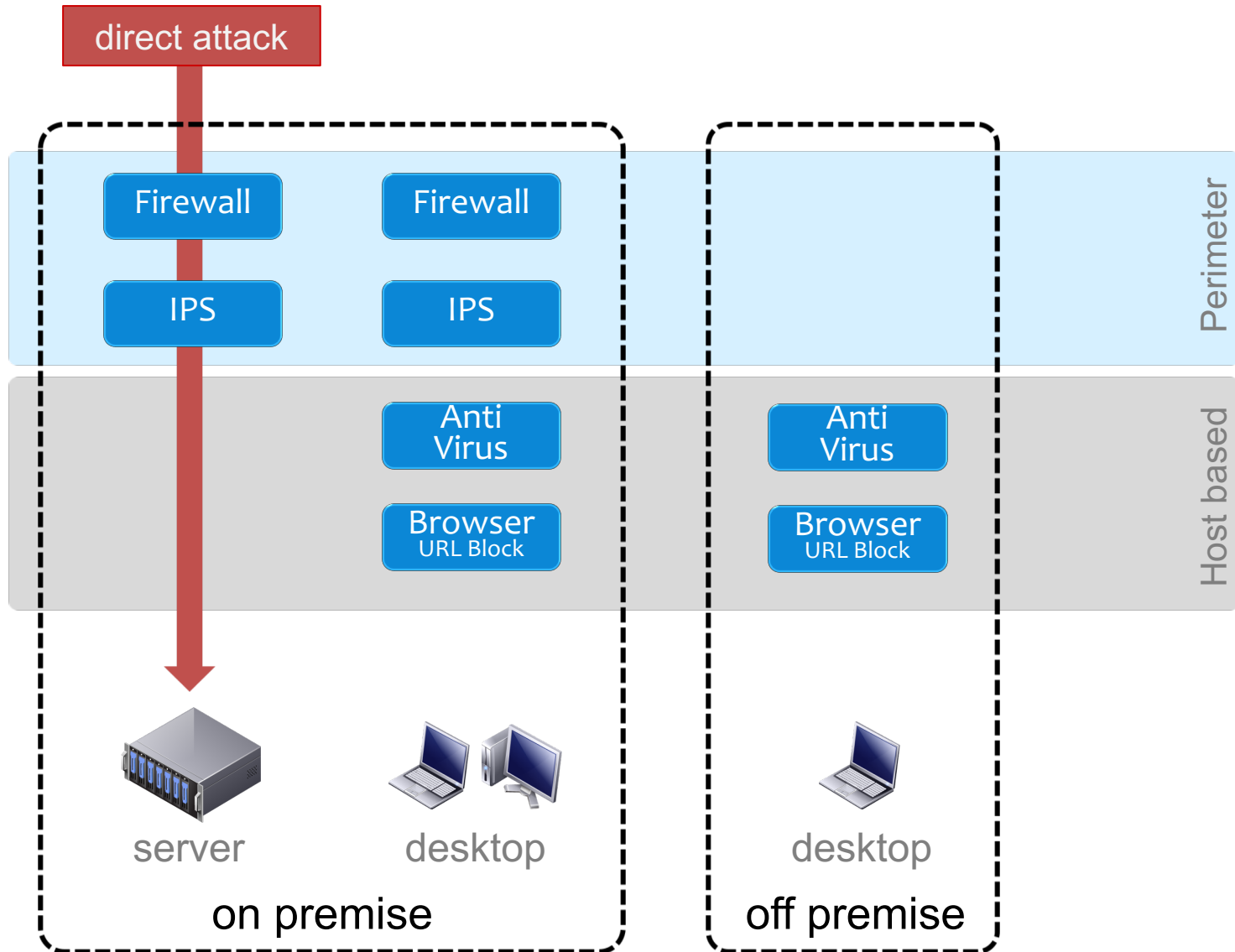
Layered Defense - Perimeter



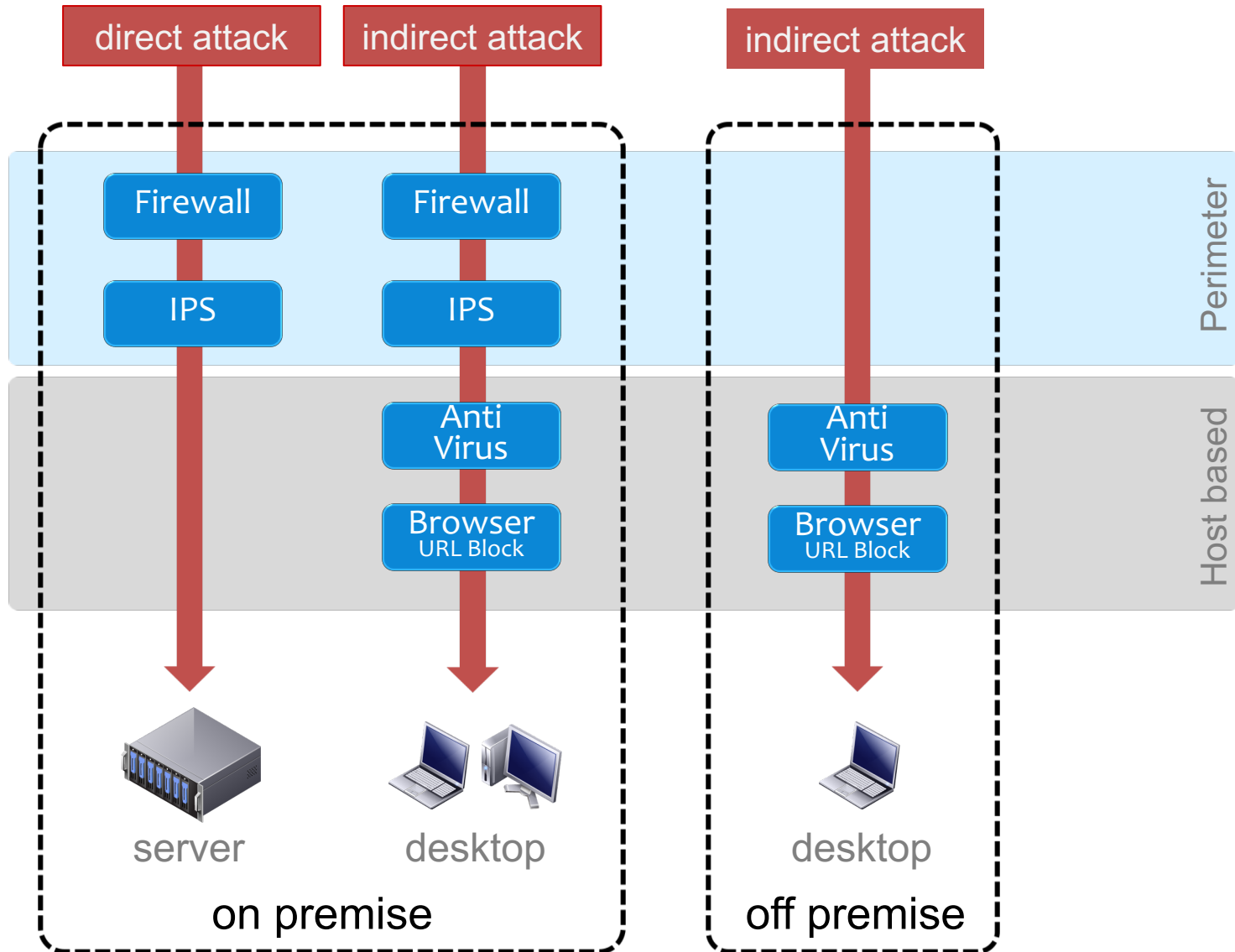
Layered Defense – Host based



Layered Defense – Direct Attacks



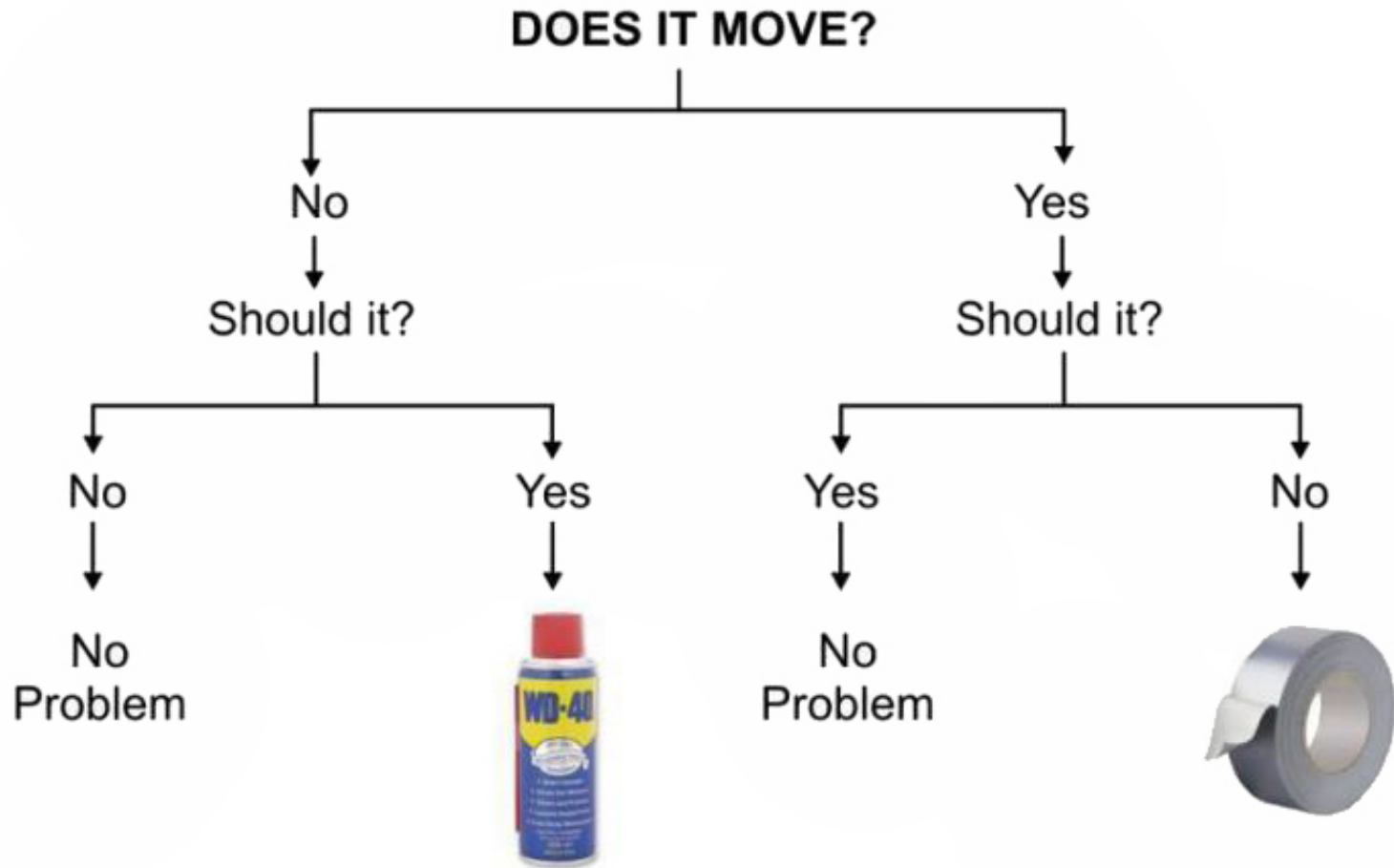
Layered Defense – Indirect Attack



A night-time photograph of a city skyline, likely New York City, with numerous skyscrapers illuminated by city lights. The sky is dark and filled with several bright, jagged lightning bolts striking down. The text "Why independent testing?" is overlaid in white, sans-serif font across the middle of the image.

Why independent testing?

Engineering Workflow ..



.. sadly, security testing is not that simple

NSS Labs' Testing Lab

- Multi-million dollar research and testing facility in Austin/TX
- Capable of 24 x 7 testing
- Global research network captures Internet threats, zero-days & trends live, as they arise



Security Test Metrics

To determine the security effectiveness of devices, the following metrics were used:

1. Exploit Block Performance
2. Anti Evasion Performance
3. Performance/Leakage
4. Stability & Reliability



Exploit Block Performance

- The same types of attack as used by modern cyber criminals
- Utilizing multiple commercial, open source and proprietary tools as appropriate
- More than 1,400 exploits, tested such that
 - a **reverse shell** is returned, allowing the attacker to execute arbitrary commands
 - a malicious **payload is installed**
 - a system is **rendered unresponsive**



Anti Evasion Performance

- Providing exploit protection without factoring in evasion/obfuscation is misleading
- Additional test cases are generated for each appropriate evasion technique.
 - At TCP, IP, and application protocol level
 - Fragmentation, Segmentation, Obfuscation, Encoding, Compression and all combinations thereof



Performance & Leakage

- Trade-off between security effectiveness and performance

Ensure vendors don't take **security shortcuts** to maintain or **improve performance**

- Tested based upon three traffic types
 - a mix of perimeter traffic common in enterprises
 - a mix of internal traffic common in enterprises
 - 21KB HTTP response traffic



Stability & Reliability

- Long-term stability is particularly important for an in-line device

Verify the **stability** of the device under test

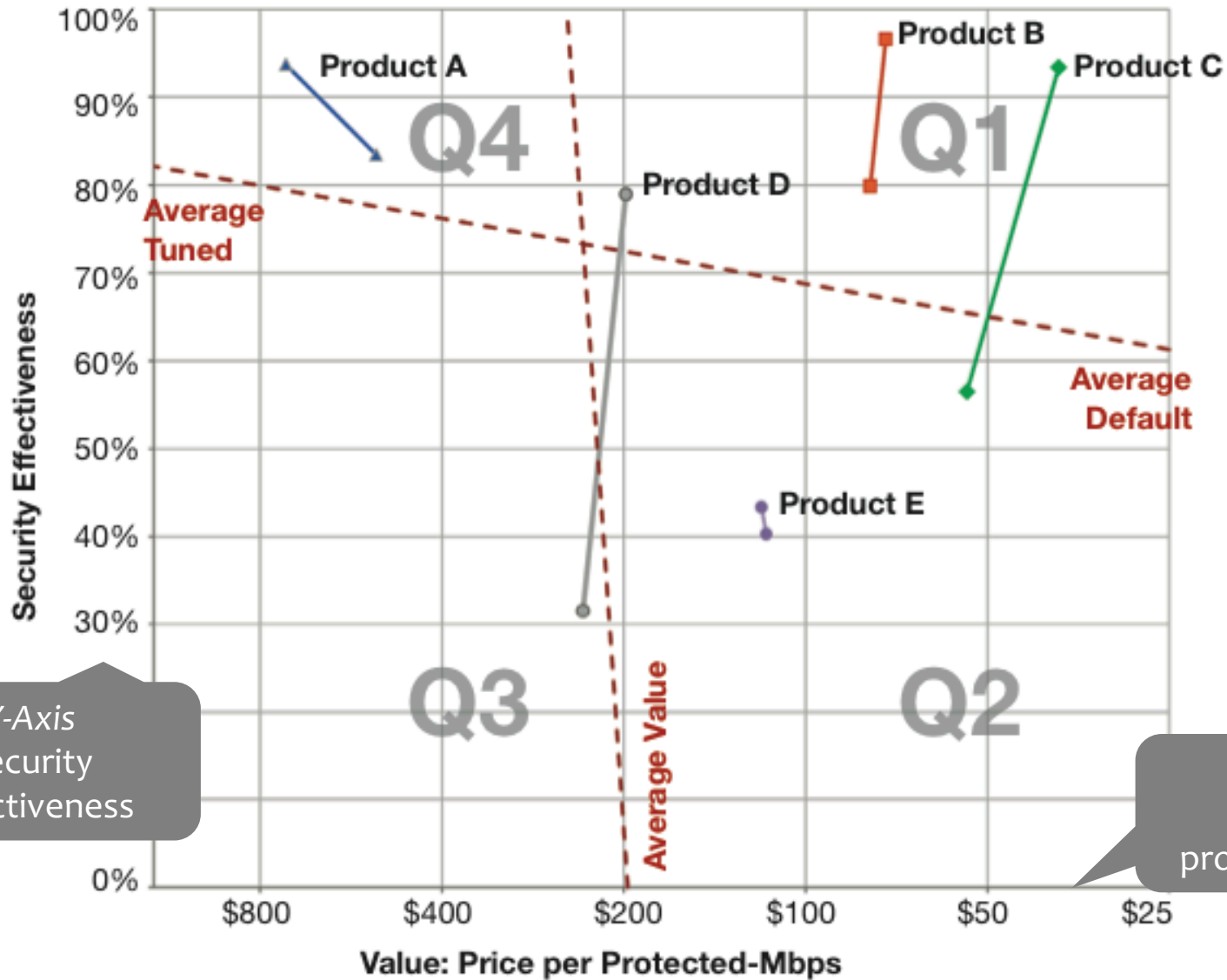
- Tests the ability to maintain security effectiveness under normal & malicious traffic load

Products that **are not able** to sustain legitimate traffic (or which crash) while under hostile attack **will not pass**

Security Effectiveness

- **Security Effectiveness**
combines measured *cost of ownership*, *security protection*, *performance*, *leakage*, and *stability*
- **Security Value Map (SVM)**
shows *security effectiveness* and *value* (cost per protected Mbps) of tested product configurations
- **Customizable**
SVM is *customizable* to reflect individual weights of the different factors

Security Effectiveness



Y-Axis
Security
Effectiveness

X-Axis
Price per
protected Mbps

NSS Labs tested:

6

Network Firewalls

Q1/2011

15

Intrusion Prevention Systems

Q3/2012

13

End-point Antivirus Suites

Q4/2012

4

Browsers

Q3/2012

Network Firewalls

- Three of the six products tested crashed when subjected to our stability tests

This lack of resilience is **alarming** and indicates the presence of a **vulnerability** that could be exploited

- Performance claims in vendor datasheets are generally grossly overstated

Performance based on RFC-2544 (UDP) **does not reflect** live real world environments

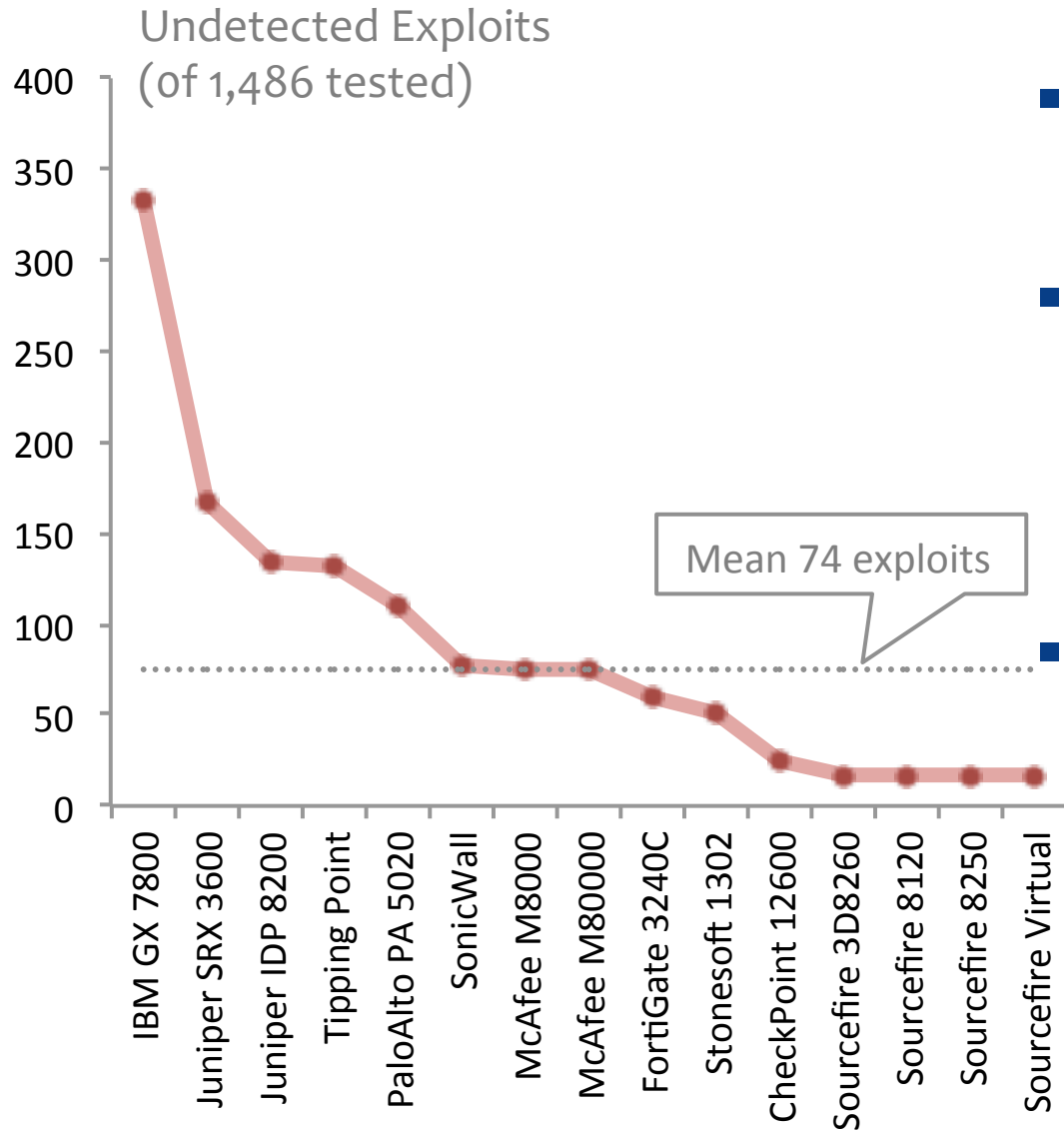
- Five of the six products failed the TCP Split Handshake test

Allowing an attacker to **reverse the flow** and bypass security. Four vendors released a **patch within a month**

Network Firewalls

- Longstanding, tried, and field proven technology, such as firewalls, **can still fail** on basic networking attacks
- Attacks never expire – security devices must maintain protection for the **complete range** of attacks
- Independent tests are valuable to identify, and have **vendors remediate** shortcomings

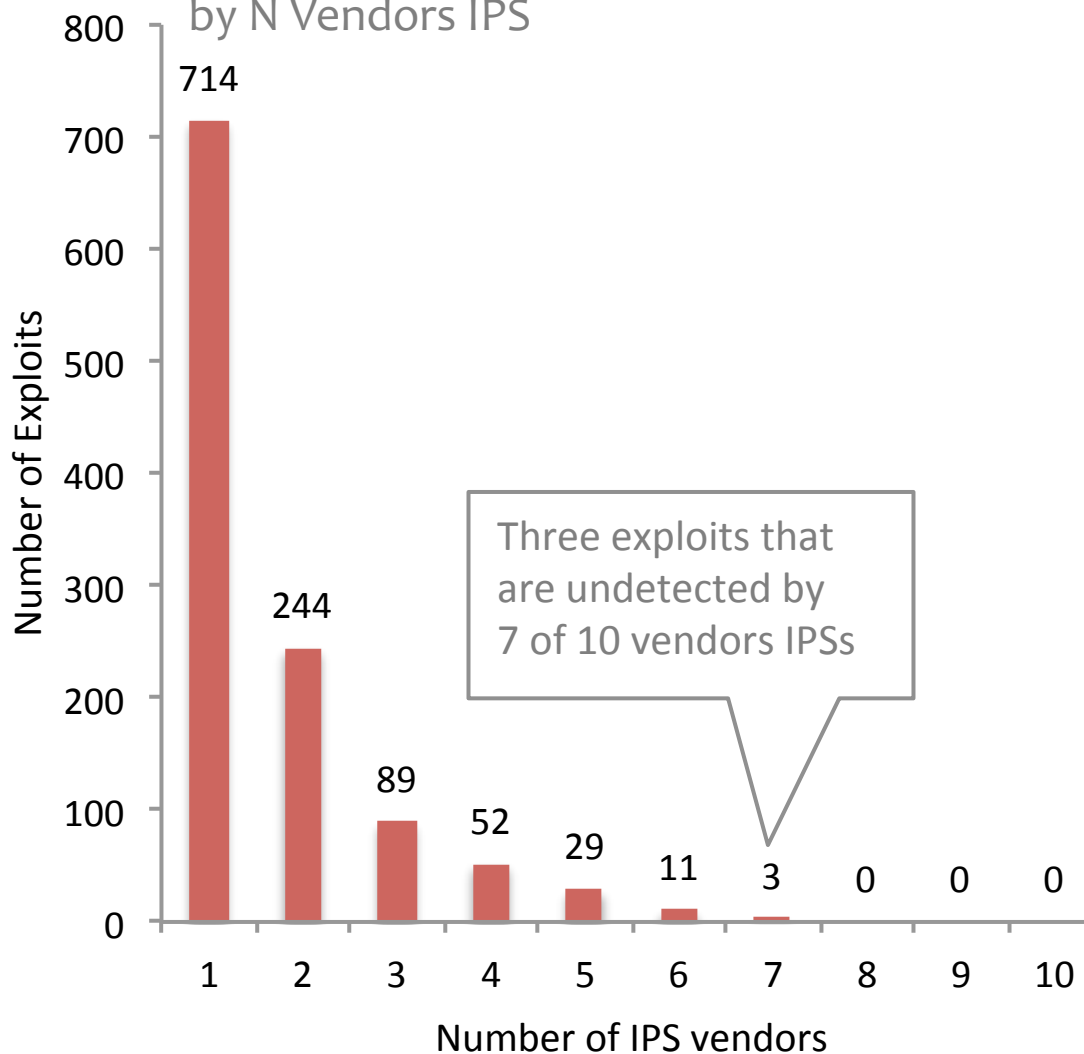
Intrusion Prevention Systems (IPS)



- Exploit block rate varies between **77% and 98%**
- Tuning of the **IPS policy** makes a difference, **up to 50%** less protection with default policy
- Evasion detection has **improved** considerably, all but one vendor tested passed

Intrusion Prevention Systems (IPS)

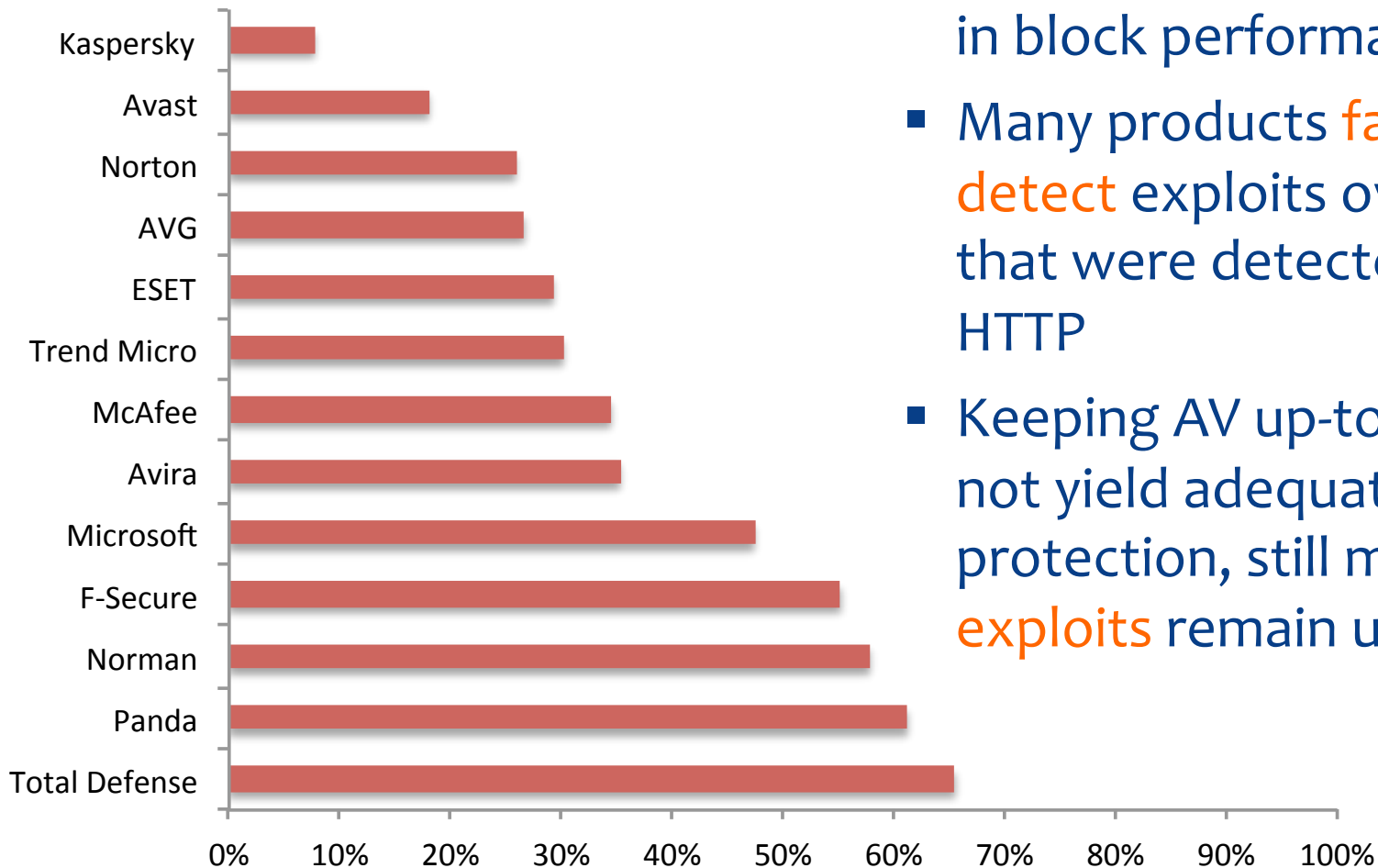
Unique Exploits undetected
by N Vendors IPS



- Correlation of undetected exploits between vendors products
- Only a small set of exploits is required to successfully bypass all IPS products
- Only one combination of different IPS products blocked all exploits

End-Point Antivirus

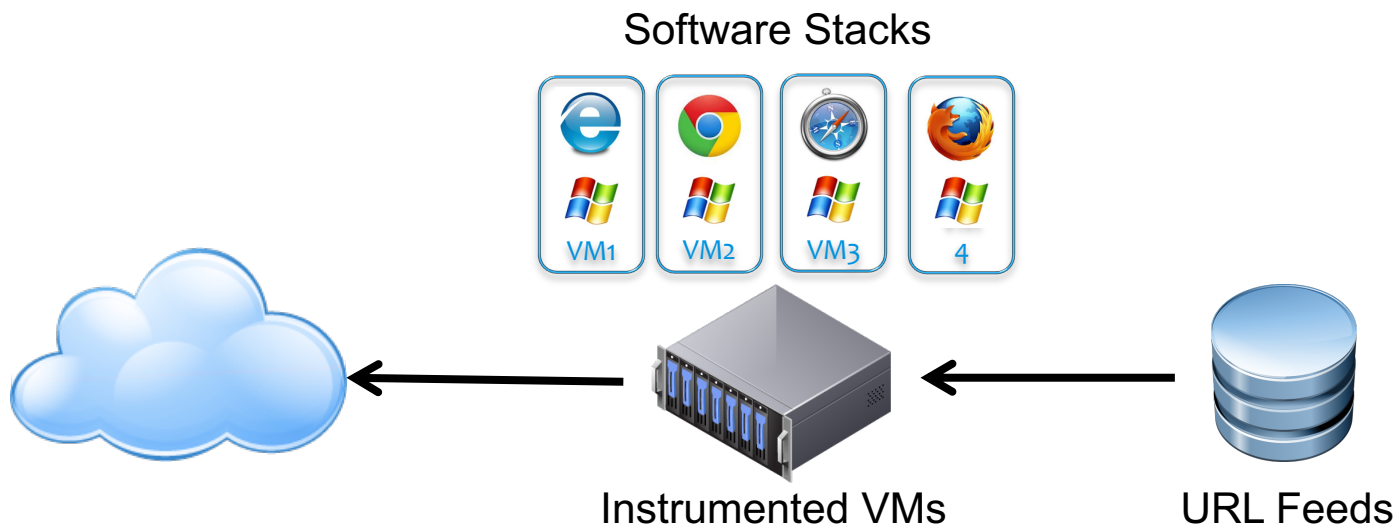
Percent undetected exploits
(of 144 exploits tested)



- AV products differ **up to 58%** in block performance
- Many products **failed to detect** exploits over HTTPS that were detected over HTTP
- Keeping AV up-to-date does not yield adequate protection, still many **old exploits** remain undetected

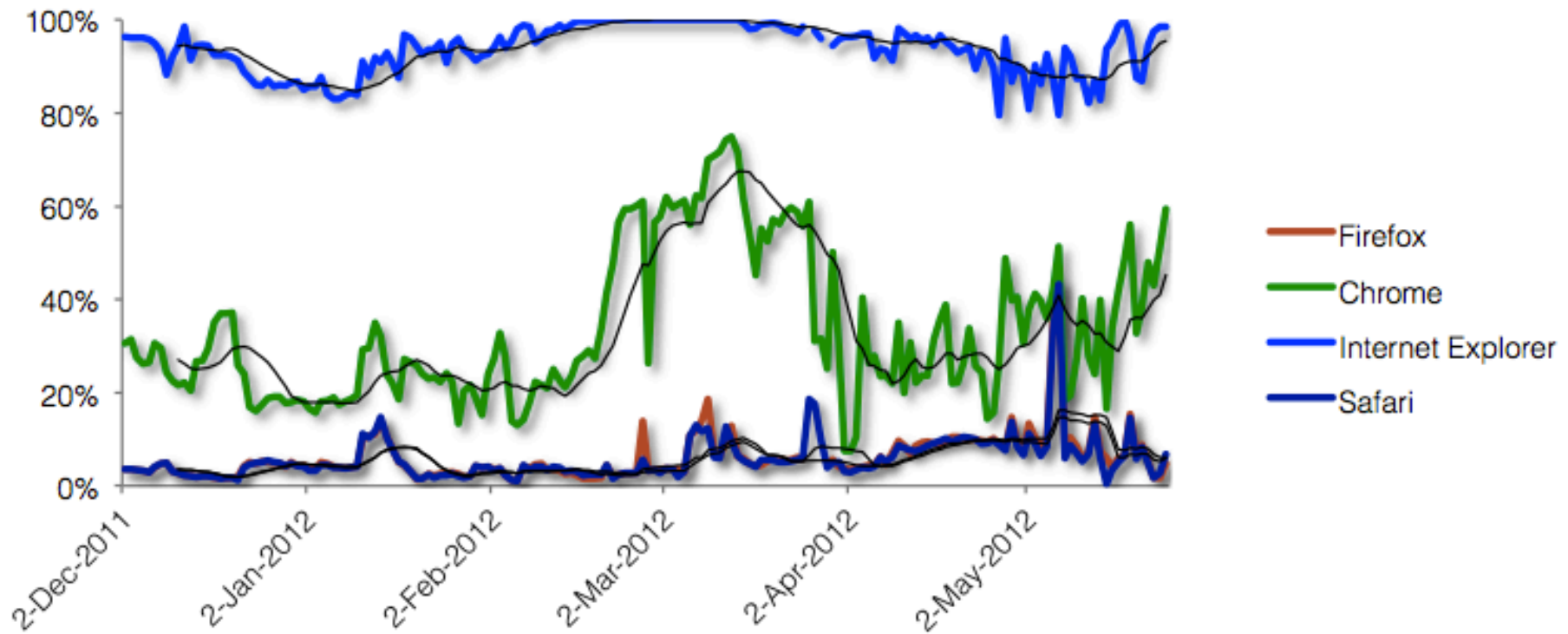
Browser Blocking

- Browsers offer the largest attack surface in most enterprise networks
- Browsers are the most common vector for malware installations
- NSS Labs continuously measures browsers block performance since 2011



Browser Blocking

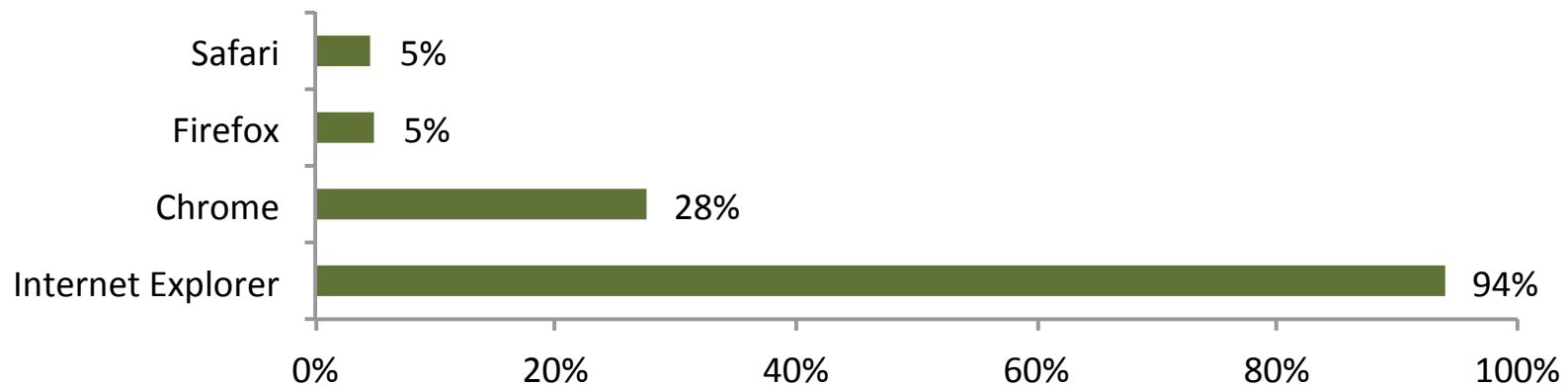
■ Suspicious URL block performance



Browser Blocking

- Internet Explorer maintained a malware block rate of 95%
- Firefox and Safari's block rate was just under 6%
- Chrome's block rate varied from 13% to 74%

Percent blocked URLs

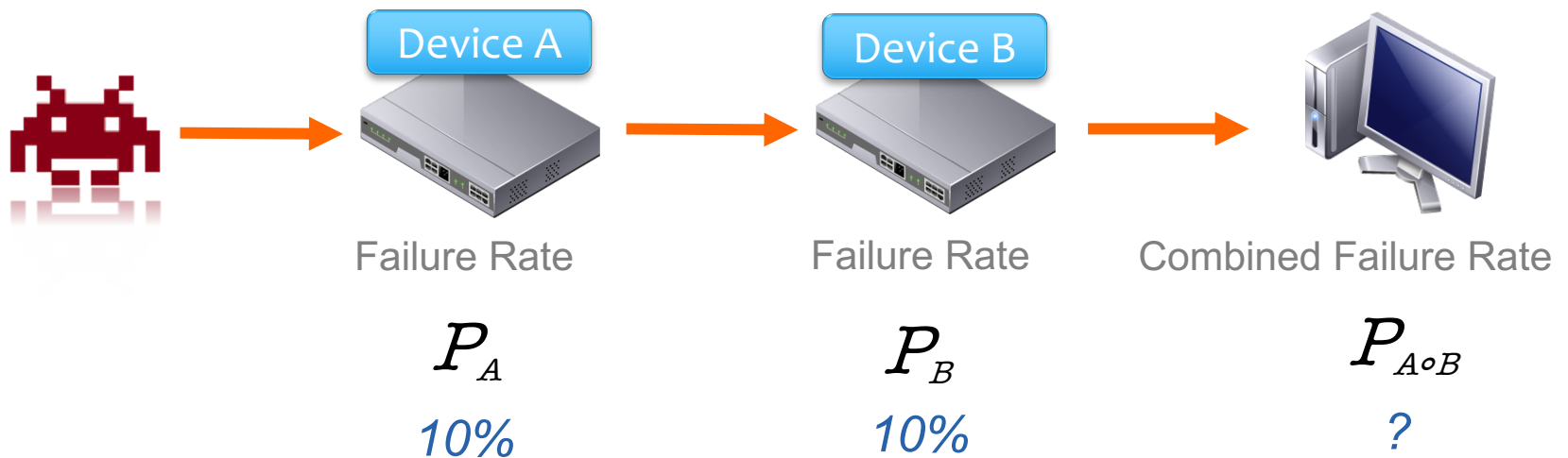


Combined Failure Rate

Attacker

Layered Defense

Target



$$P_{A \circ B} = P_A \cdot P_B = 1\%$$



Correlation Fallacy

$$P_{A \circ B} \neq P_A \cdot P_B$$

- Failures are correlated, they are not independent events
- Thus, the combined failure rate is typically considerably higher: $P_{A \circ B} > P_A P_B$
- Rethink your risk assessment

Key Findings

- Vendor **claims** on the effectiveness or performance of products are frequently **overstated**, or based on non-realistic **assumptions**
- Several network firewall products tested **crashed** when subjected to our **stability tests**
- Antivirus does **not prevent** a dedicated attacker from compromising a target
- Several products **failed detection** of exploits when switching from HTTP to HTTPS

Recommendations

- There is **no** product or combination of products tested by NSS Labs that provide **100% protection**
- Assume that you are **already compromised**
- Organizations should **complement prevention** with **breach detection** and **SIEM** to identify and act on successful security breaches in a timely manner
- Access to **independent information** on security product effectiveness and performance is important

Complexity

- Technology **alone** can not provide the highest protection
- Competent **security personal** is key to effective security – and make the best use of the tools



Thank you

sfrei@nsslabs.com



Reading List

- **Network Firewall Group Test 2011**

<https://www.nssslabs.com/reports/network-firewall-group-test-2011>

- **IPS Comparative Analysis 2012**

<https://www.nssslabs.com/reports/ips-comparative-analysis-2012>

- **Consumer AV/EPP Comparative Analysis - Exploit Protection**

<https://www.nssslabs.com/reports/consumer-avepp-comparative-analysis-exploit-protection>

- **Is Your Browser Putting You At Risk?**

<https://www.nssslabs.com/reports/your-browser-putting-you-risk-part-1-general-malware-blocking>