Virtualization Based Security

Using Endpoint CPU Virtualization to Transform Enterprise Security

Mike Burwick, Principal SE
mike.burwick@bromium.com

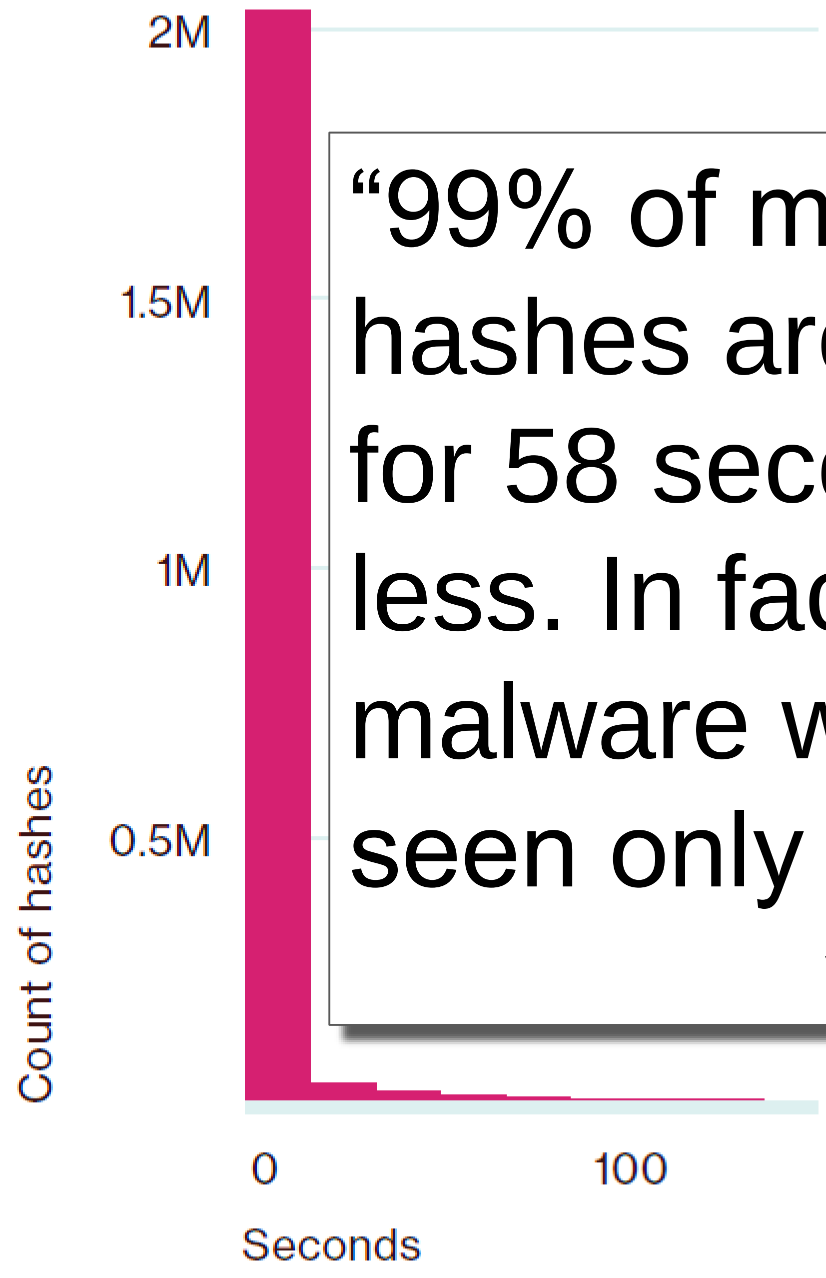

Detection:
Shark or Dolphin?

The key principles of attacks remain true

There will always be software vulnerabilities

Malicious code and threats will always exist

You will get owned
You cannot anticipate the next move

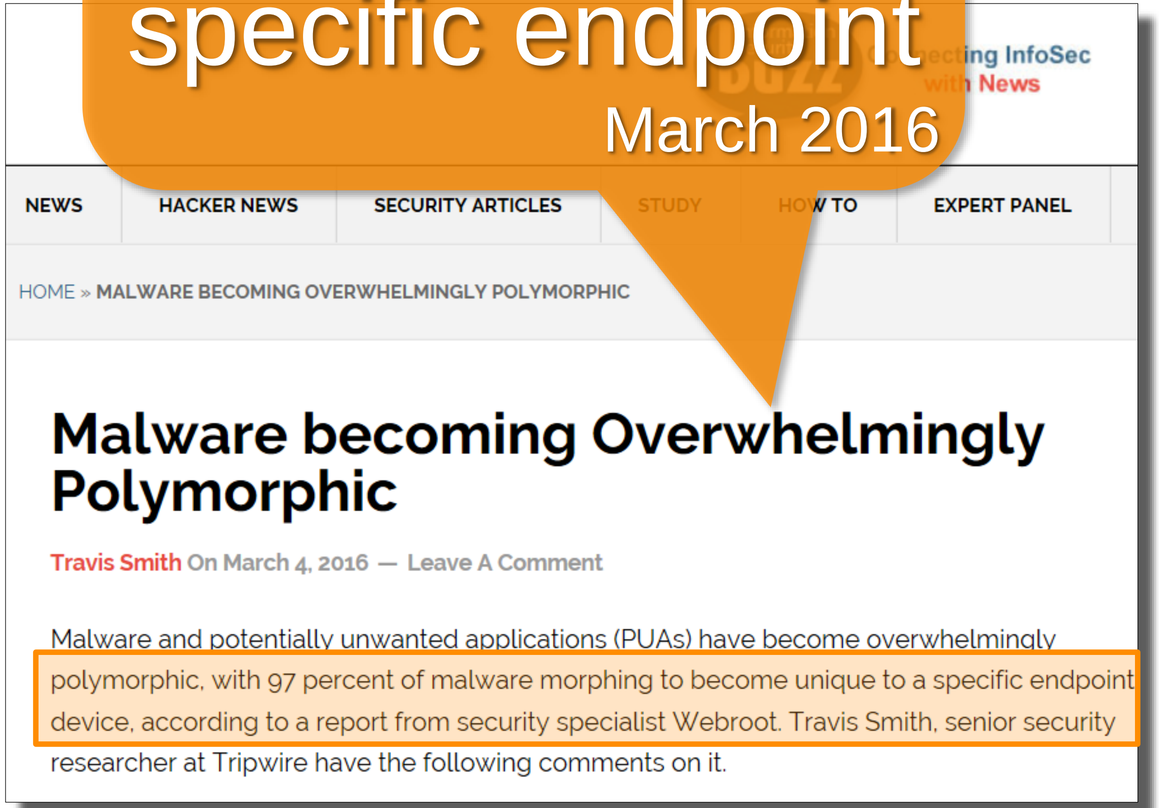


"99% of malware hashes are seen for 58 seconds or less. In fact, most malware was seen only once."

Verizon DBIR '16

97% of malware is unique to a specific endpoint

March 2016


NEWS | HACKER NEWS | SECURITY ARTICLES | STUDY | HOW TO | EXPERT PANEL

HOME » MALWARE BECOMING OVERWHELMINGLY POLYMORPHIC

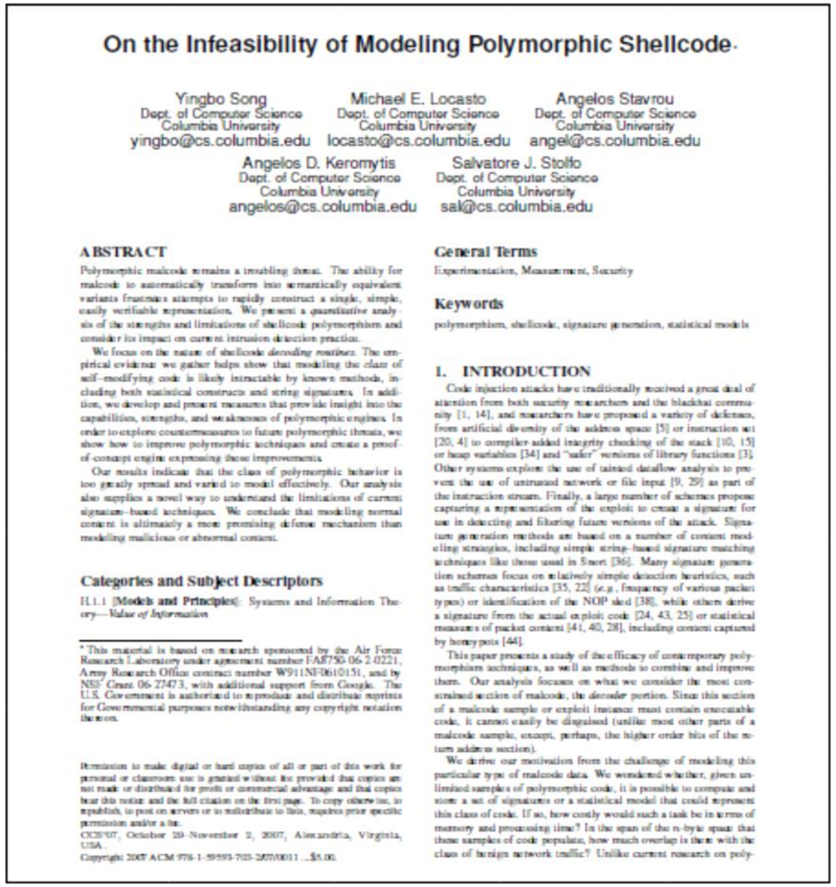
Malware becoming Overwhelmingly Polymorphic

Travis Smith On March 4, 2016 — Leave A Comment

Malware and potentially unwanted applications (PUAs) have become overwhelmingly polymorphic, with 97 percent of malware morphing to become unique to a specific endpoint device, according to a report from security specialist Webroot. Travis Smith, senior security researcher at Tripwire have the following comments on it.

The Failure of Detection

It is mathematically impossible* to detect all polymorphic or zero day malware in advance


On the Infeasibility of Modeling Polymorphic Shellcode

Yingbo Song, Dept. of Computer Science, Columbia University, yingbo@cs.columbia.edu
Michael E. Locasto, Dept. of Computer Science, Columbia University, locasto@cs.columbia.edu
Angelos Stavrou, Dept. of Computer Science, Columbia University, angel@cs.columbia.edu
Angelos D. Keromytis, Dept. of Computer Science, Columbia University, angelos@cs.columbia.edu
Salvatore J. Stolfo, Dept. of Computer Science, Columbia University, sal@cs.columbia.edu

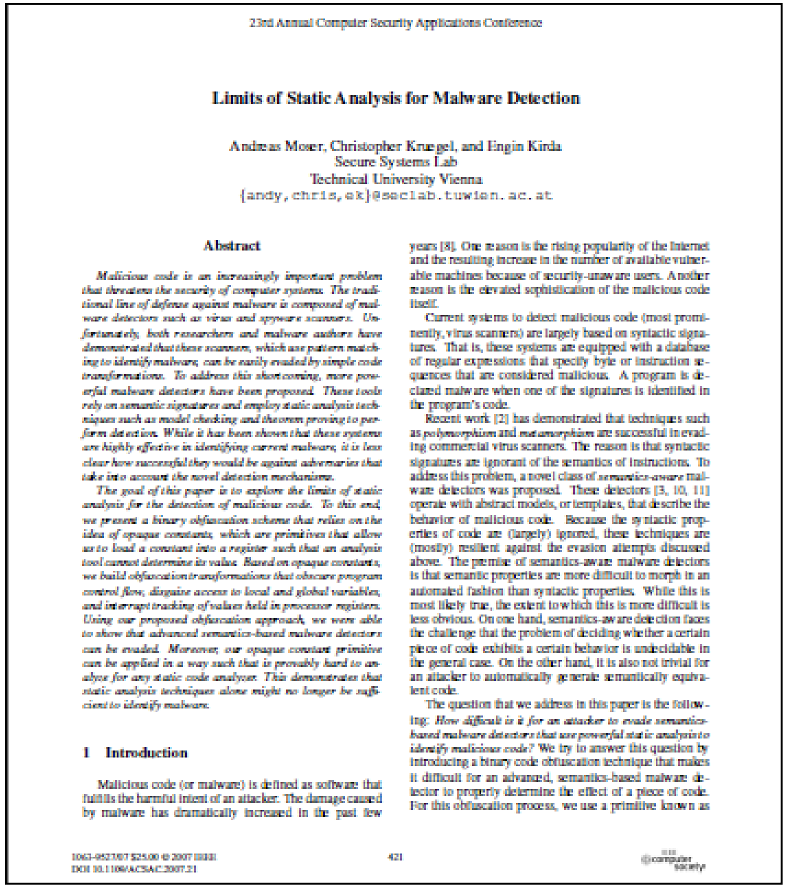
ABSTRACT

General Terms

Keywords

1. INTRODUCTION

Categories and Subject Descriptors


23rd Annual Computer Security Applications Conference

Limits of Static Analysis for Malware Detection

Andreas Moser, Christopher Kruegel, and Engin Kirda
Secure Systems Lab
Technical University Vienna
{andy,chris,ek}@seclab.tuwien.ac.at

Abstract

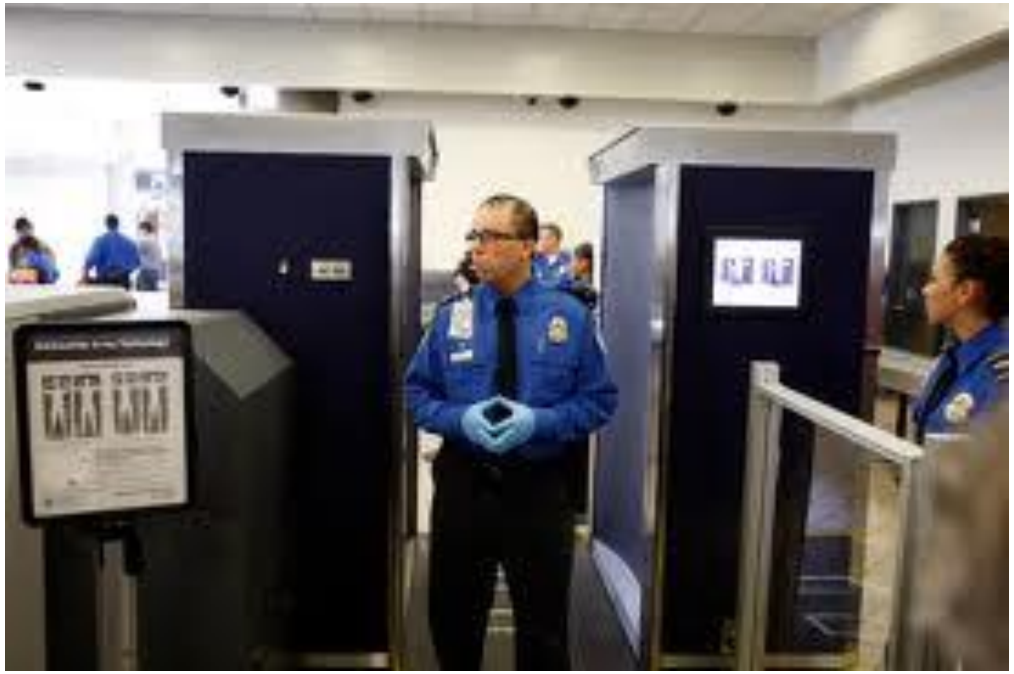
1 Introduction

*Limits of Static Analysis for Malware Detection
Andreas Moser, Christopher Kruegel, and Engin Kirda
Secure Systems Lab Technical University Vienna

*On the Infeasibility of Modeling Polymorphic Shellcode.pdf
Yingbo Song, Michael E. Locasto, Angelos Stavrou
Dept. of Computer Science Columbia University

Detection vs Isolation

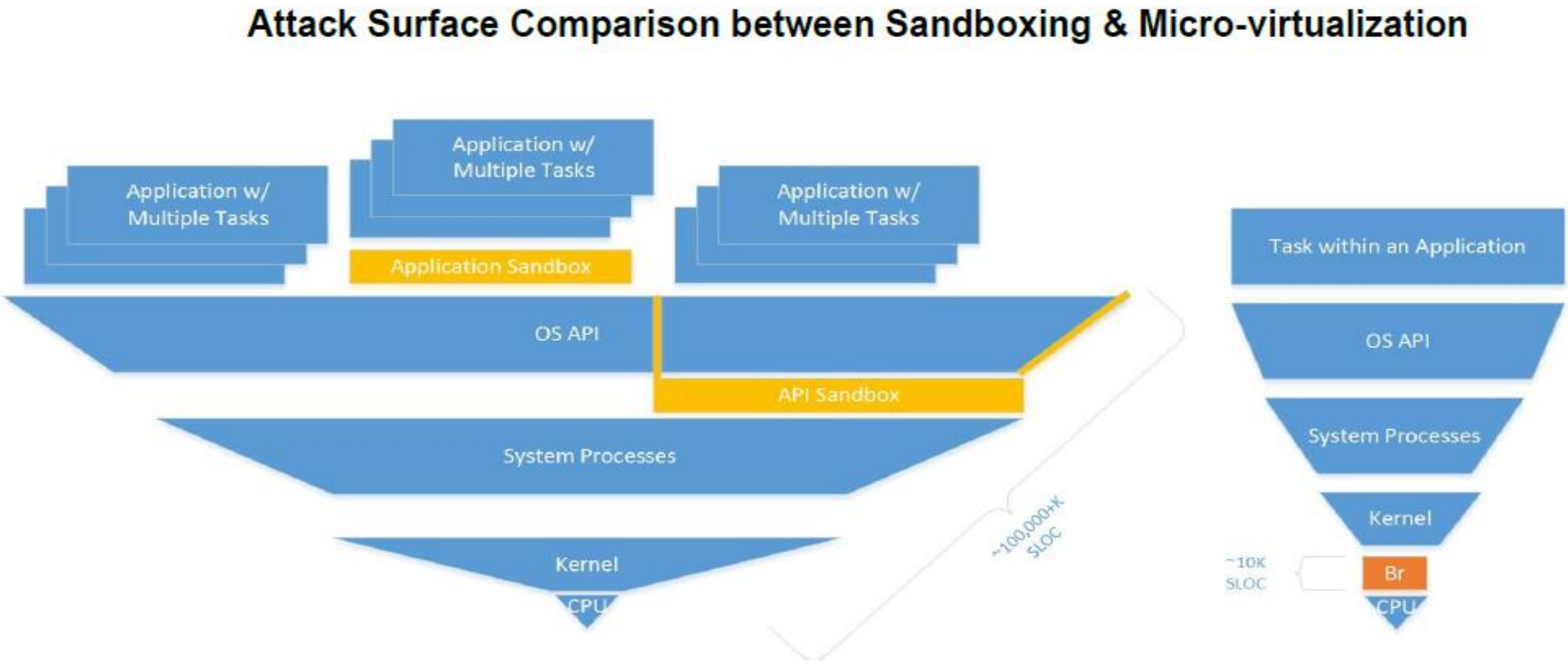
- Existing security solutions today rely on detection
  - A threat must be detected before it can be blocked
  - Polymorphic & “0 day” malware evades AV, white lists, IPS etc.



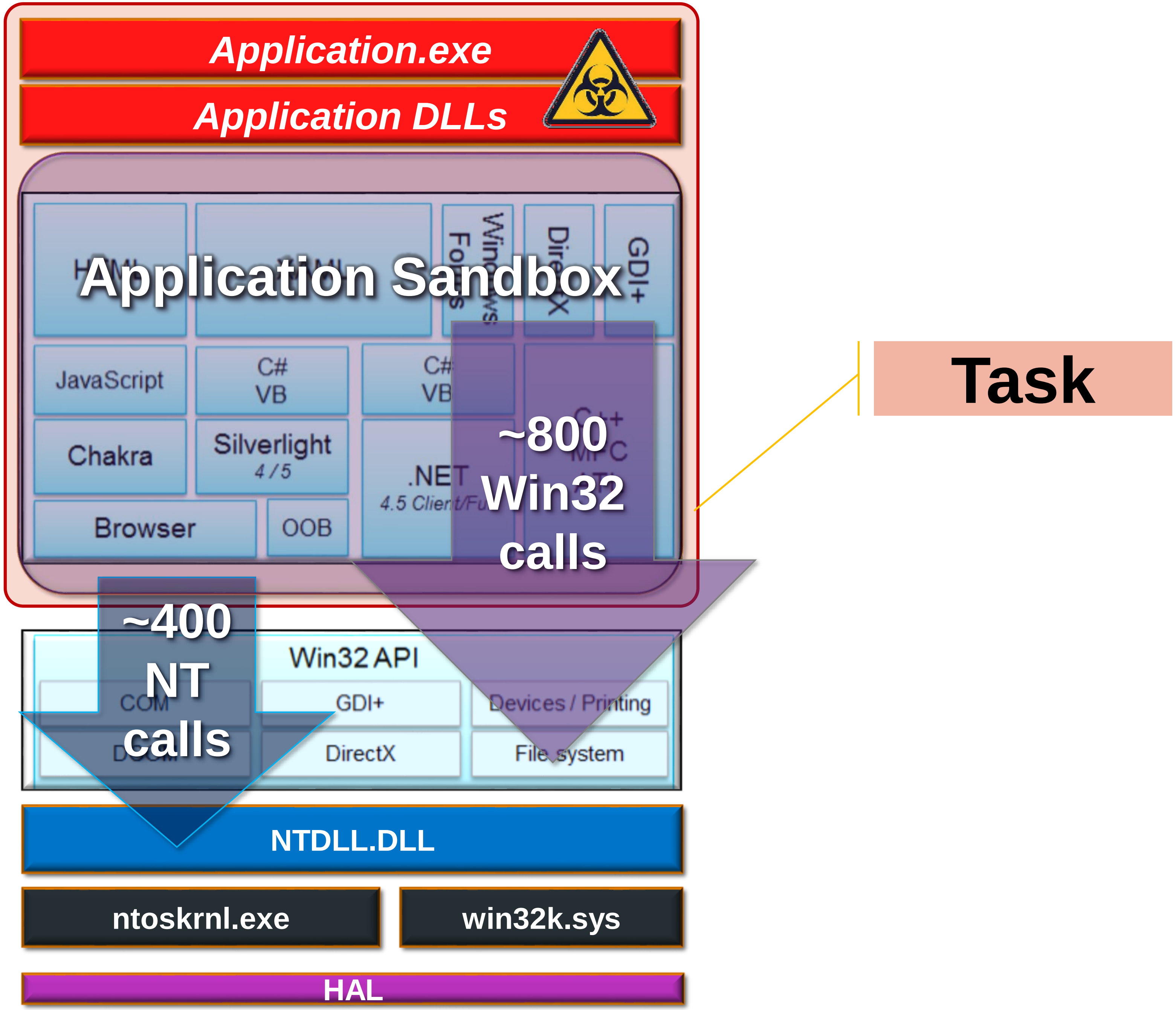
- Micro-virtualization protects through “CPU enforced Isolation”
  - Isolates untrusted content from the OS, files, network, etc.
  - Leverages hardware virtualization for maximum protection

Software Isolation Techniques

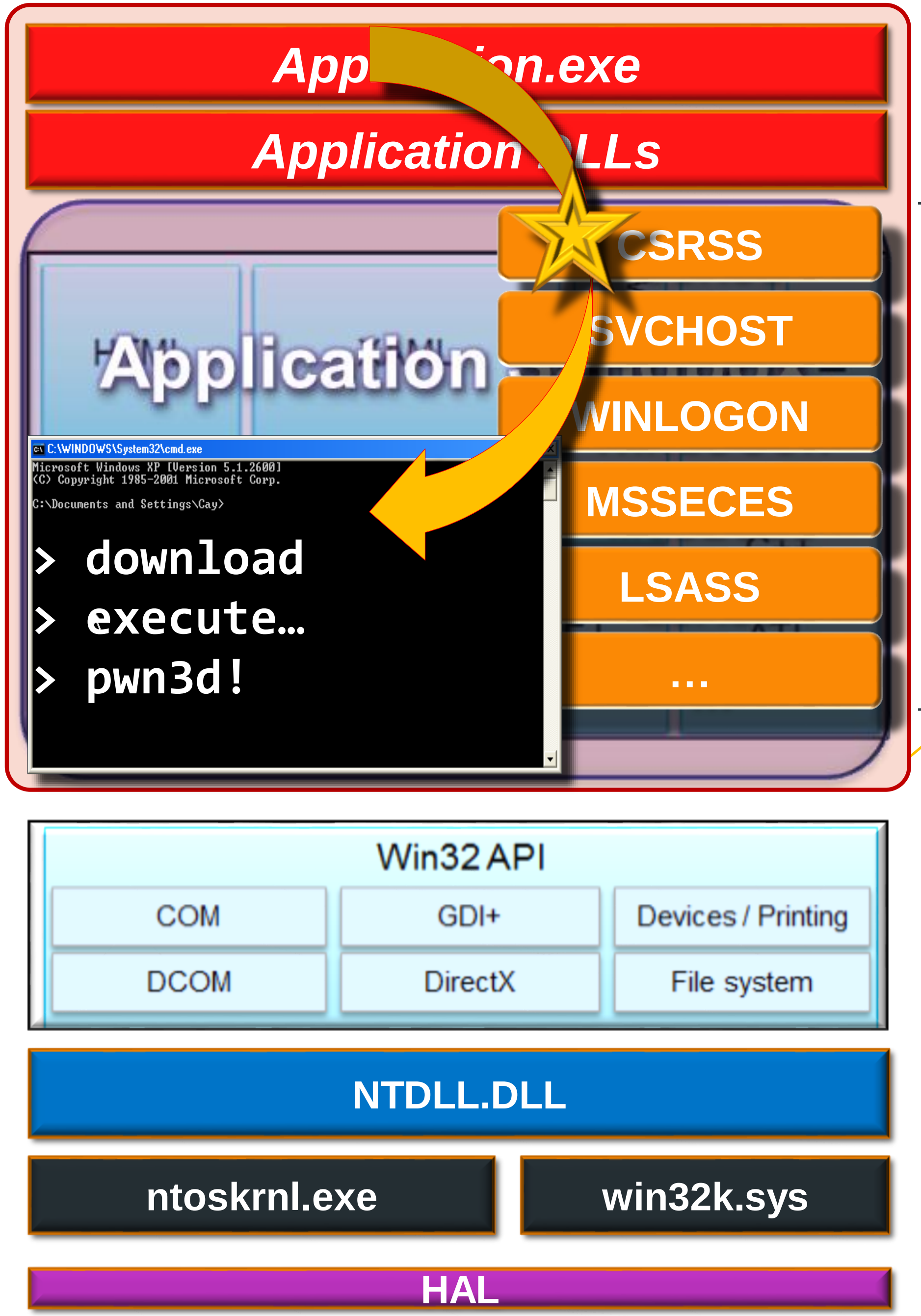
Software vs Hardware Isolation



Goal: Protect the OS kernel by isolating any malicious user task (application)



Goal: Protect the OS kernel by isolating any malicious user task (application)



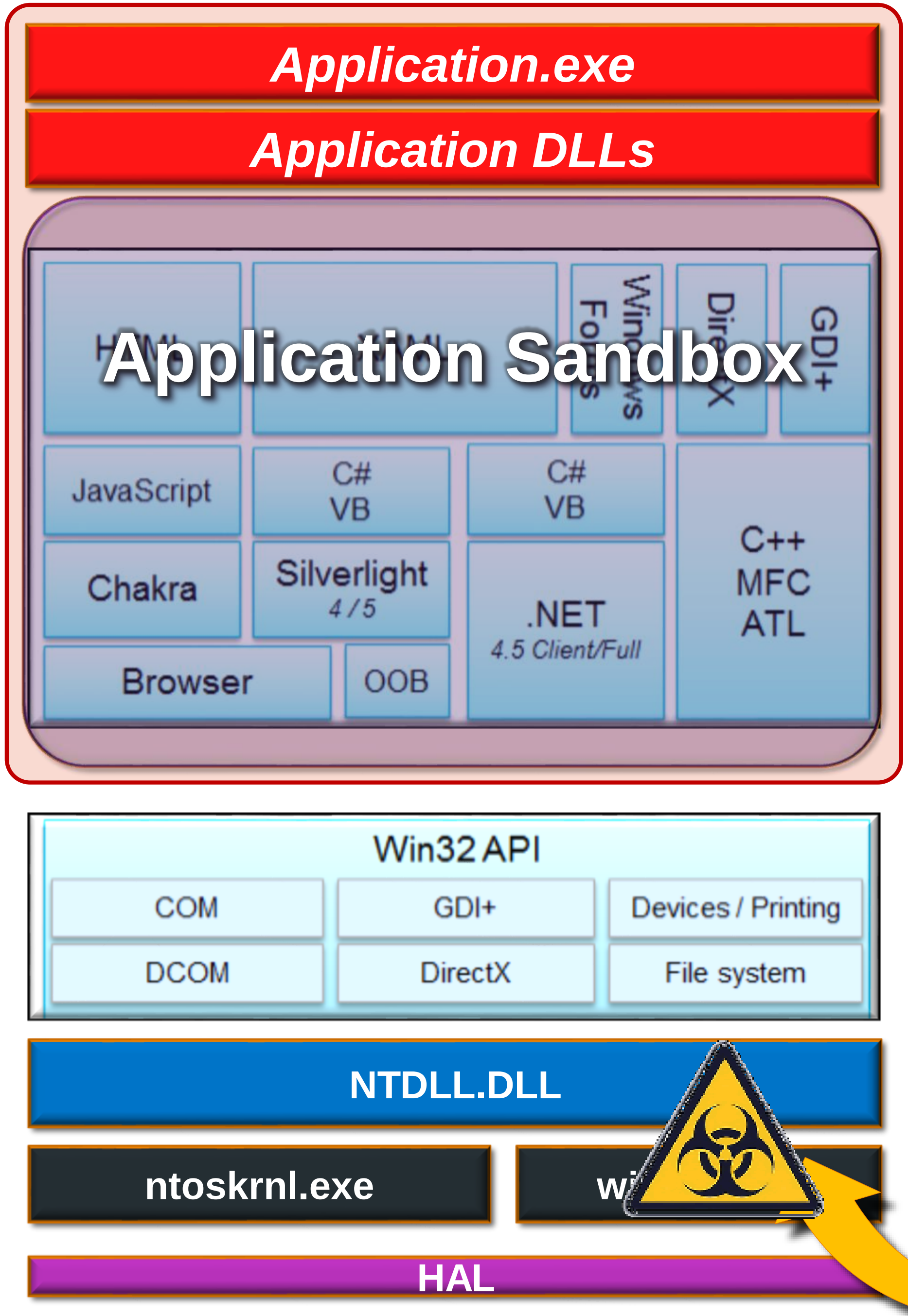
Millions of LOC

Task

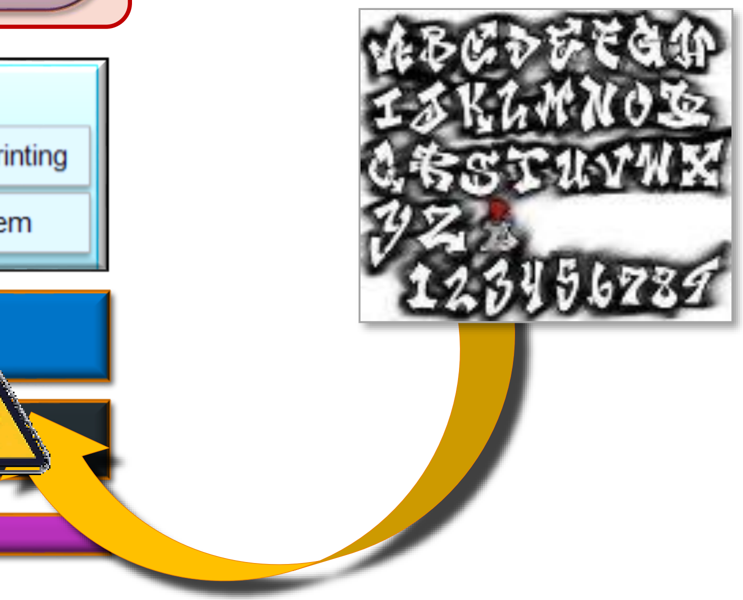
CVE-2015-5119 (Hacking Team)

Goal: Protect the OS kernel by isolating any malicious user task (application)

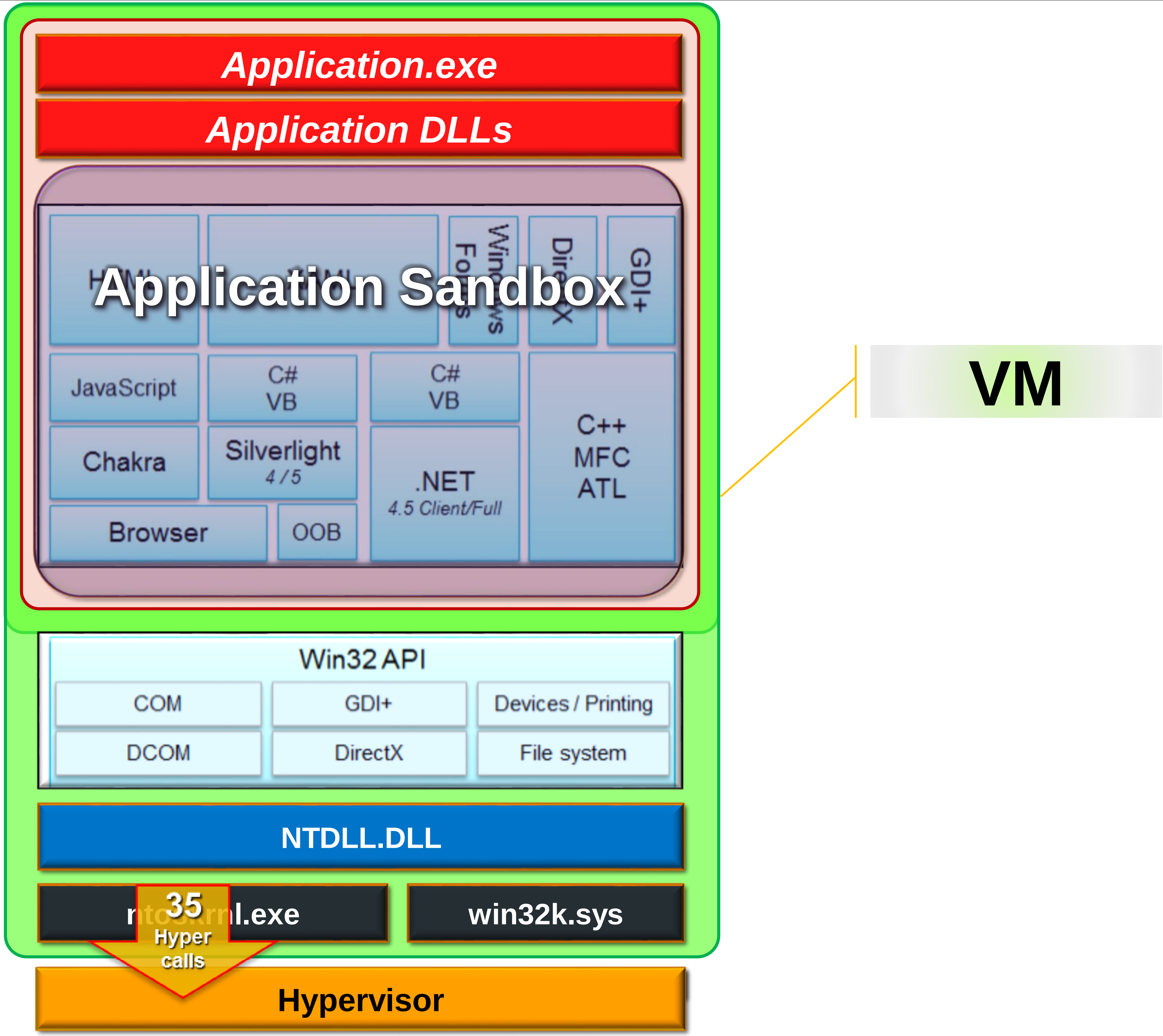
✗



CVE-2015-2426



The attacker directly compromises the kernel, bypassing the sandbox

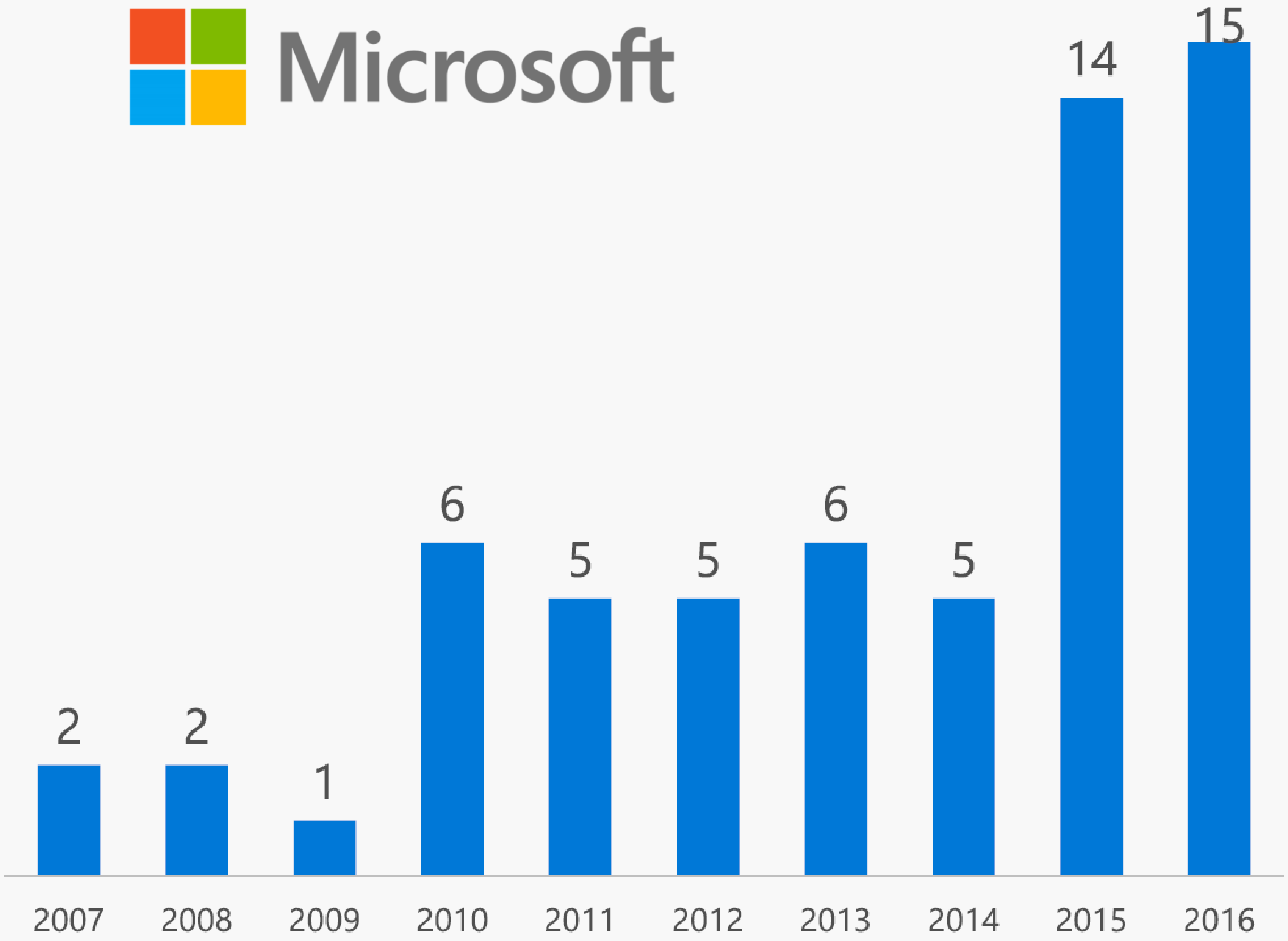

Application.exe
Application DLLs
Application Sandbox
JavaScript
C#
VB
C#
VB
GDI+
Chakra
Silverlight
4 / 5
.NET
4.5 Client/Full
C++
MFC
ATL
Browser
OOB
Win32 API
COM
GDI+
Devices / Printing
DCOM
DirectX
File system
NTDLL.DLL
35
Hyper
calls
win32k.sys
Hypervisor
VM

Current threat landscape

Driving the need for hardware based isolation

Microsoft

Our research indicates that there has been a dramatic increase in kernel exploits over the past two years



Source: MSRC and Microsoft One Protection Team


Microsoft

Windows 10 Device Guard

Device integrity

UEFI Secure Boot prevents device tampering and ensures OS starts with integrity

Cryptographic processor

TPM processor provides tamper proof integrity validation and prevents unauthorized access to sensitive information

Virtualization

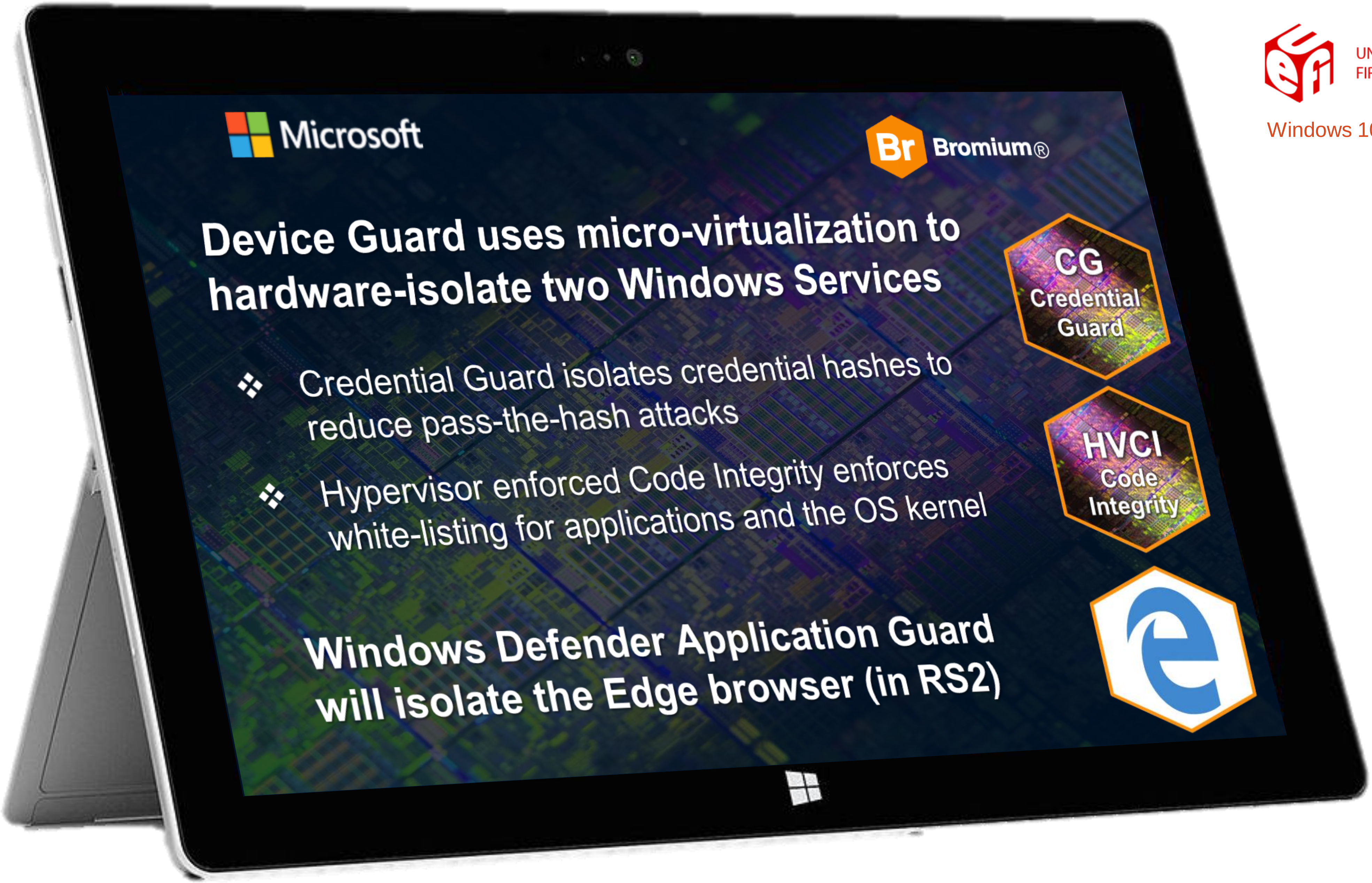
Processor based virtualization isolates critical system components and data and protects even in the event full system compromise

Biometric sensors

Using a biometric for authentication increases the level of difficulty for an attacker to the highest level

On Windows 10

50% of the time is spent in the browser



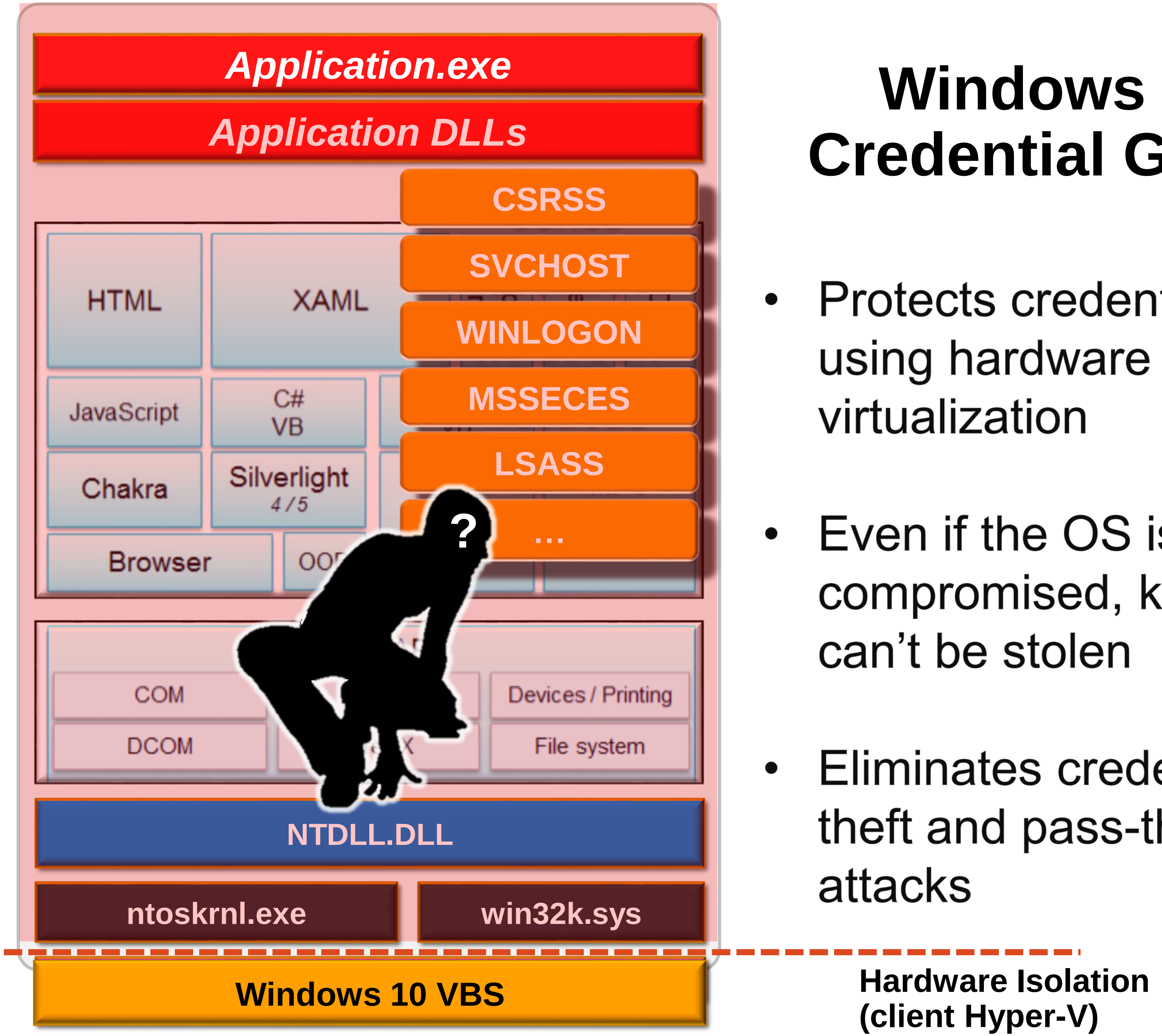
UNIFIED EXTENSIBLE FIRMWARE INTERFACE

Secure Boot

Windows 10 Enterprise License

Result

- A compromised PC is less valuable to attackers
- The device still has access to enterprise network and infrastructure (AD, Exchange, Intranet sites, shares)
- Files/data can be stolen
- A keylogger / screen scraper can steal non-Windows credentials

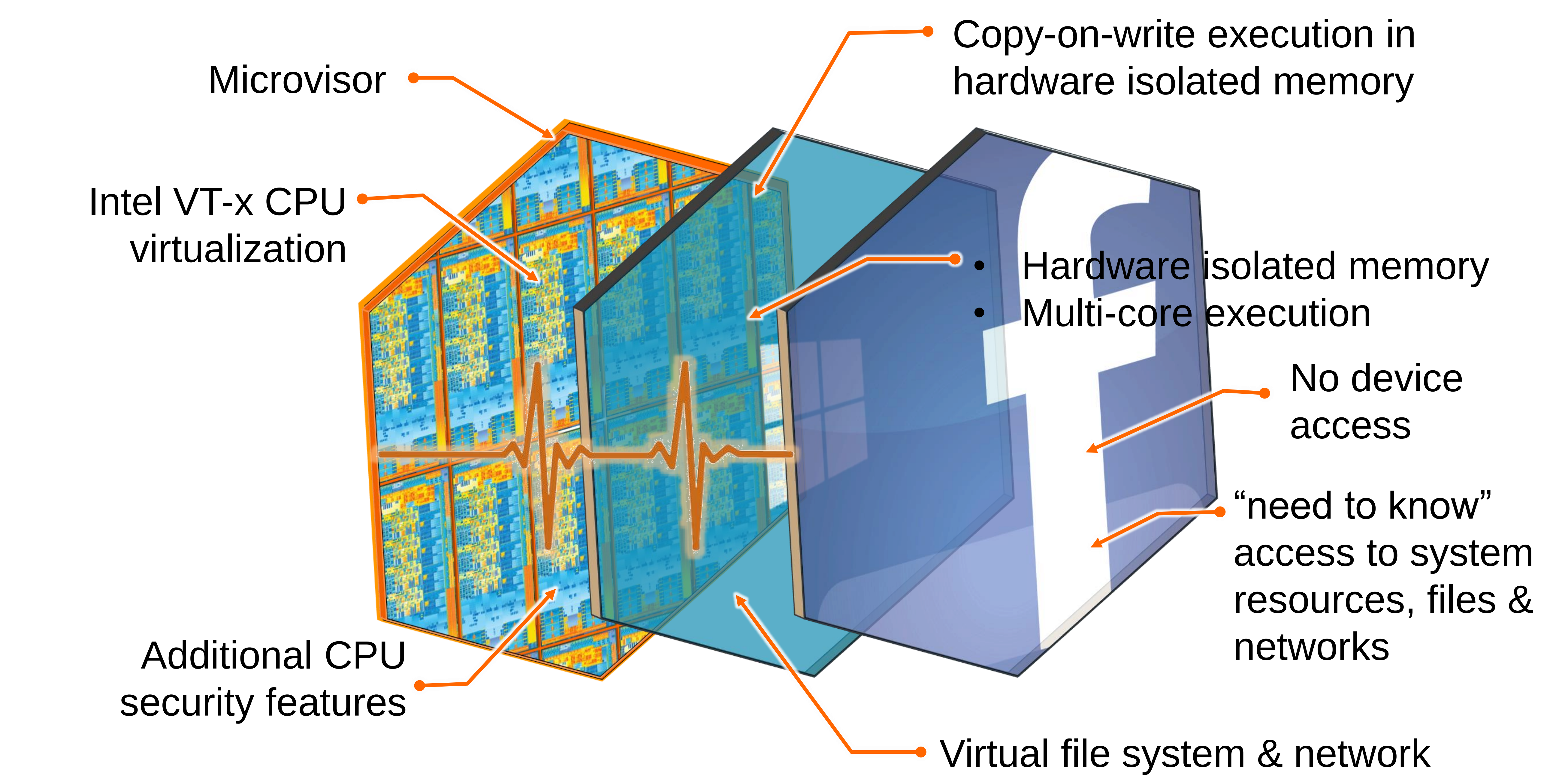


Windows 10 Credential Guard

- Protects credentials using hardware virtualization
- Even if the OS is compromised, key data can't be stolen
- Eliminates credential theft and pass-the-hash attacks


Br
Bromium®

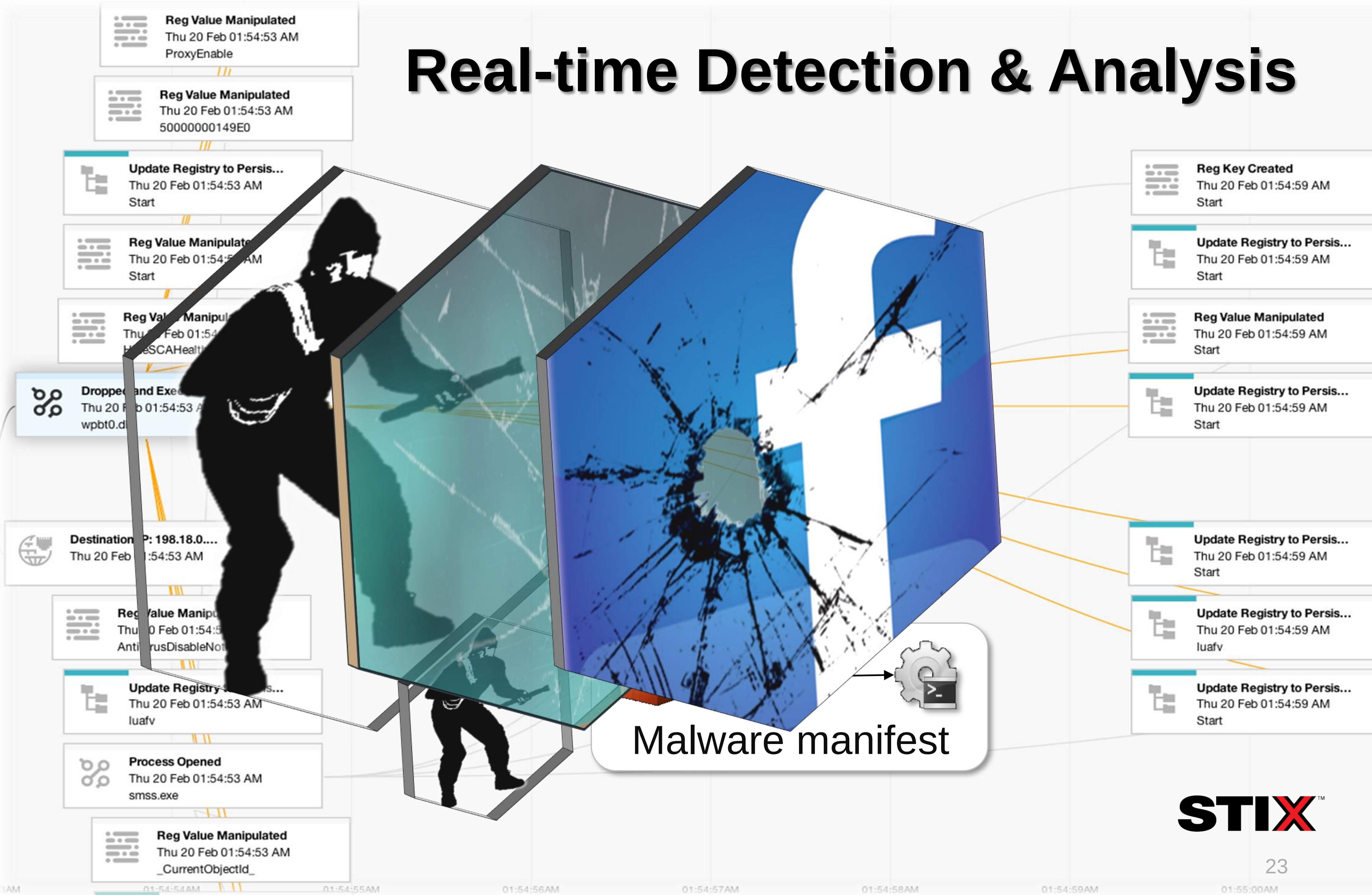

Bromium®
PDF
Task Isolation
Tamper-proof Monitoring
Micro-virtualization



Microvisor
Intel VT-x CPU virtualization
Additional CPU security features
Copy-on-write execution in hardware isolated memory
• Hardware isolated memory
• Multi-core execution
No device access
“need to know” access to system resources, files & networks
Virtual file system & network

Protect • Detect • Respond

Real-time Detection & Analysis




Bromium®
Self remediation eliminates persistence

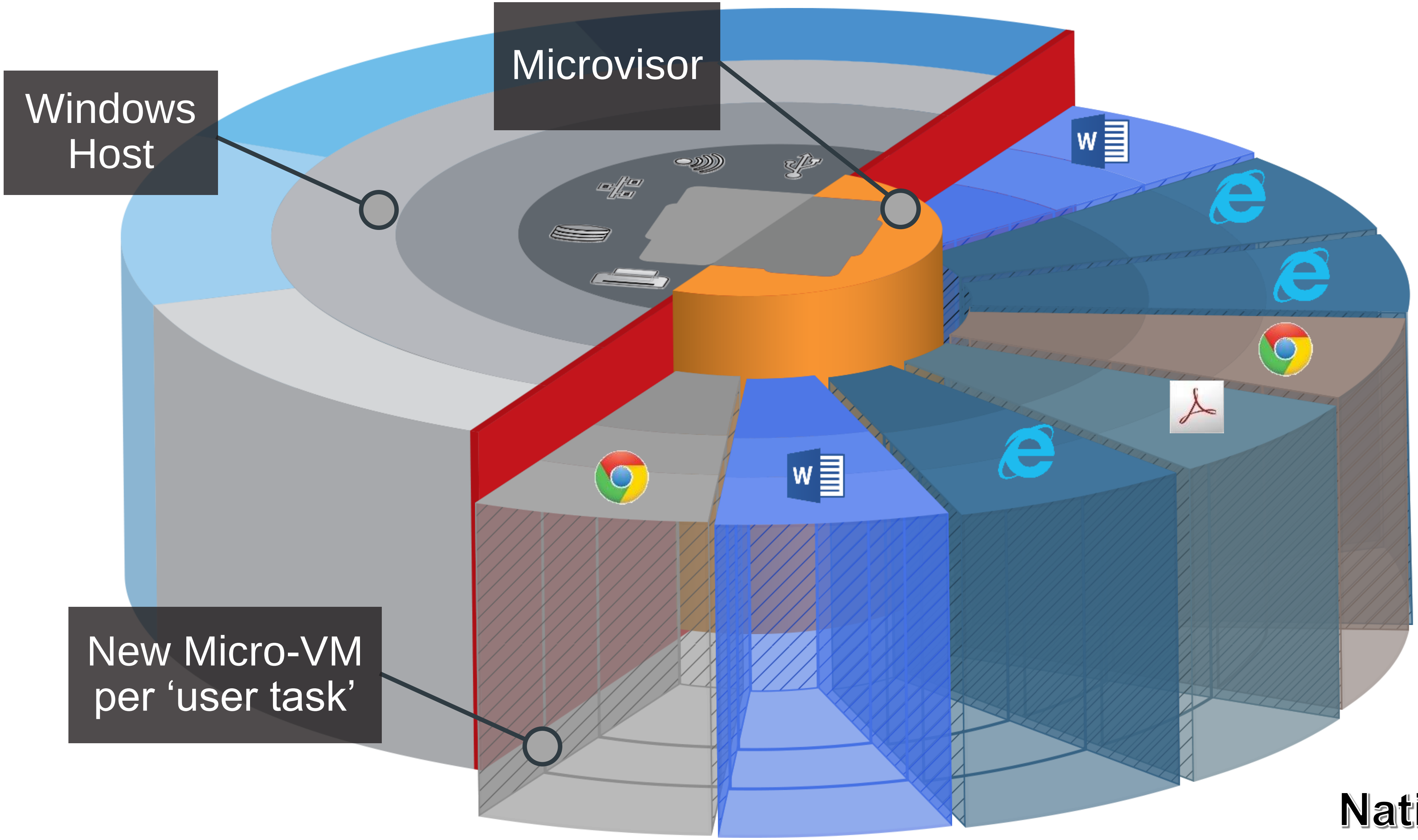
Top 4 Ransomware Attack Vectors

Weaponized e-mail attachments

Embedded hyperlinks within emails

Browser (drive-by) attacks

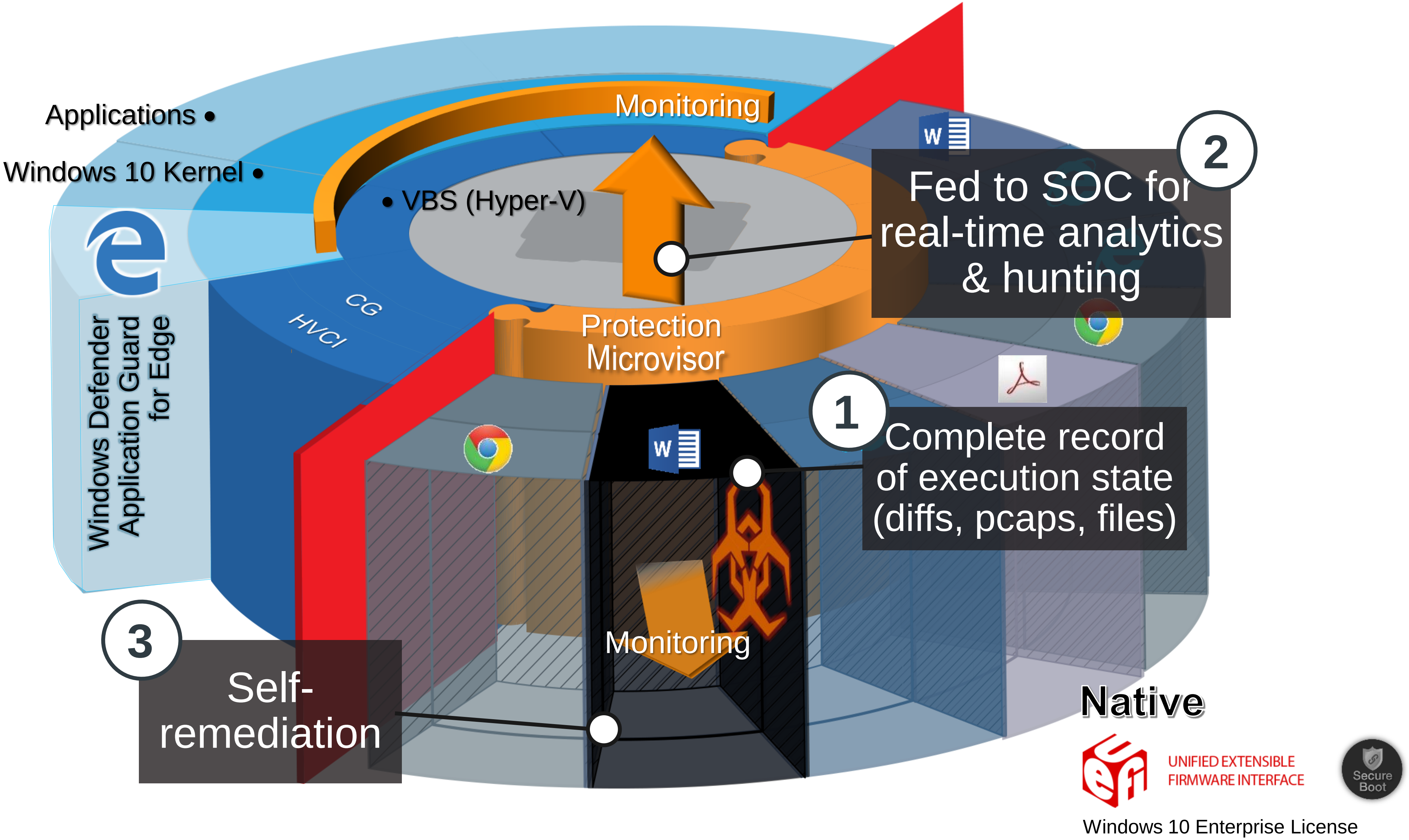
Web application vulnerabilities



Native

BIOS Boot

(Windows 7, 8, 10)


Applications •
Windows 10 Kernel •
• VBS (Hyper-V)
Monitoring
Windows Defender Application Guard for Edge
CG
HVCI
Protection Microvisor
2
Fed to SOC for real-time analytics & hunting
1
Complete record of execution state (diffs, pcaps, files)
Monitoring
3
Self-remediation
Native
UNIFIED EXTENSIBLE FIRMWARE INTERFACE
Secure Boot
Windows 10 Enterprise License

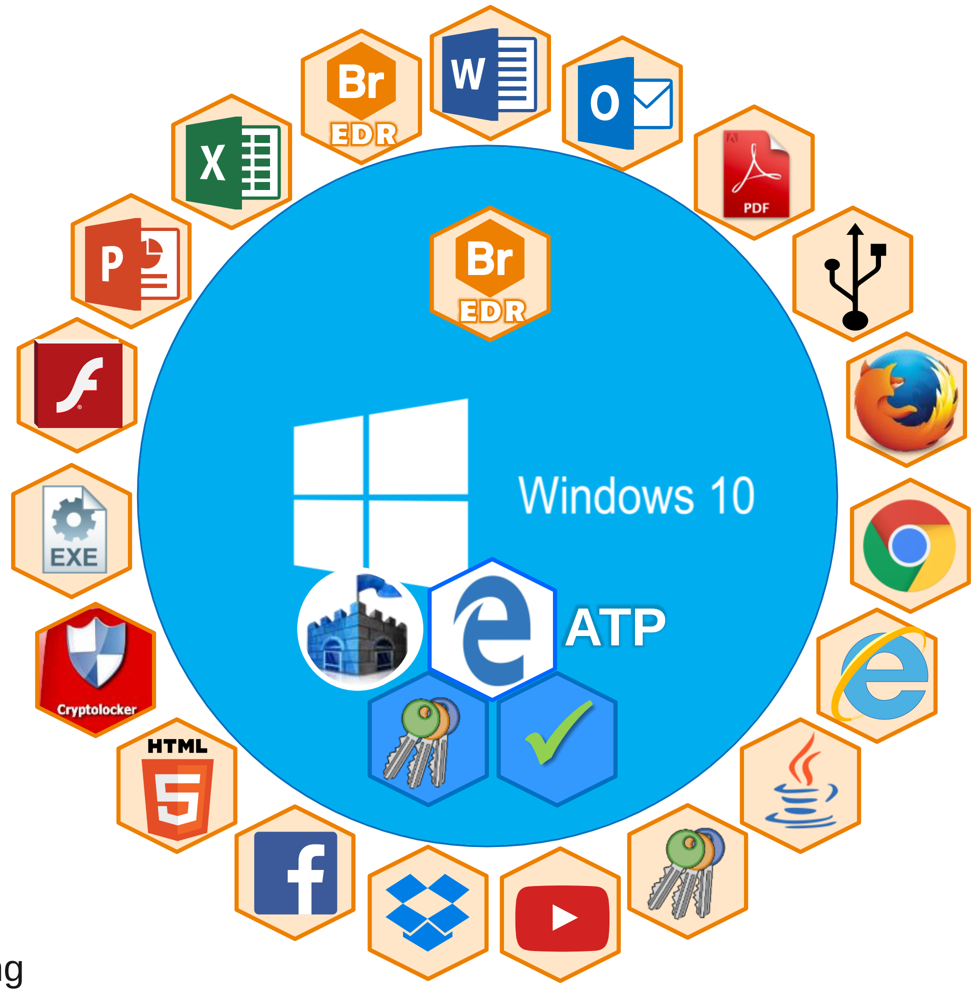
Bromium Complements Microsoft Security

Windows 10

- CG for pass-the-hash attacks
- HVCI kernel code integrity
- WDAG isolates Edge
- ATP for cloud based EDR

Bromium®

- Protection & self-remediation for
  - Network-based attacks
  - File or data loss
  - Key-loggers & screen scrapers
  - Ransomware
  - Persistent APTs
  - Pass-the-hash attacks
  - All malicious execution
- Tamper-proof real-time monitoring (EDR) of isolated tasks and the Windows desktop



Micro-virtualization for the masses…

Next Steps

- Learn how hardware-enforced isolation is transforming Microsoft security http://bit.ly/VBSPartnership
- Watch this demo how Bromium stops ransomware on Windows 7, 8, or 10: http://bit.ly/GoodbyeRansomware

Evaluate your top threat vectors then talk to us.