

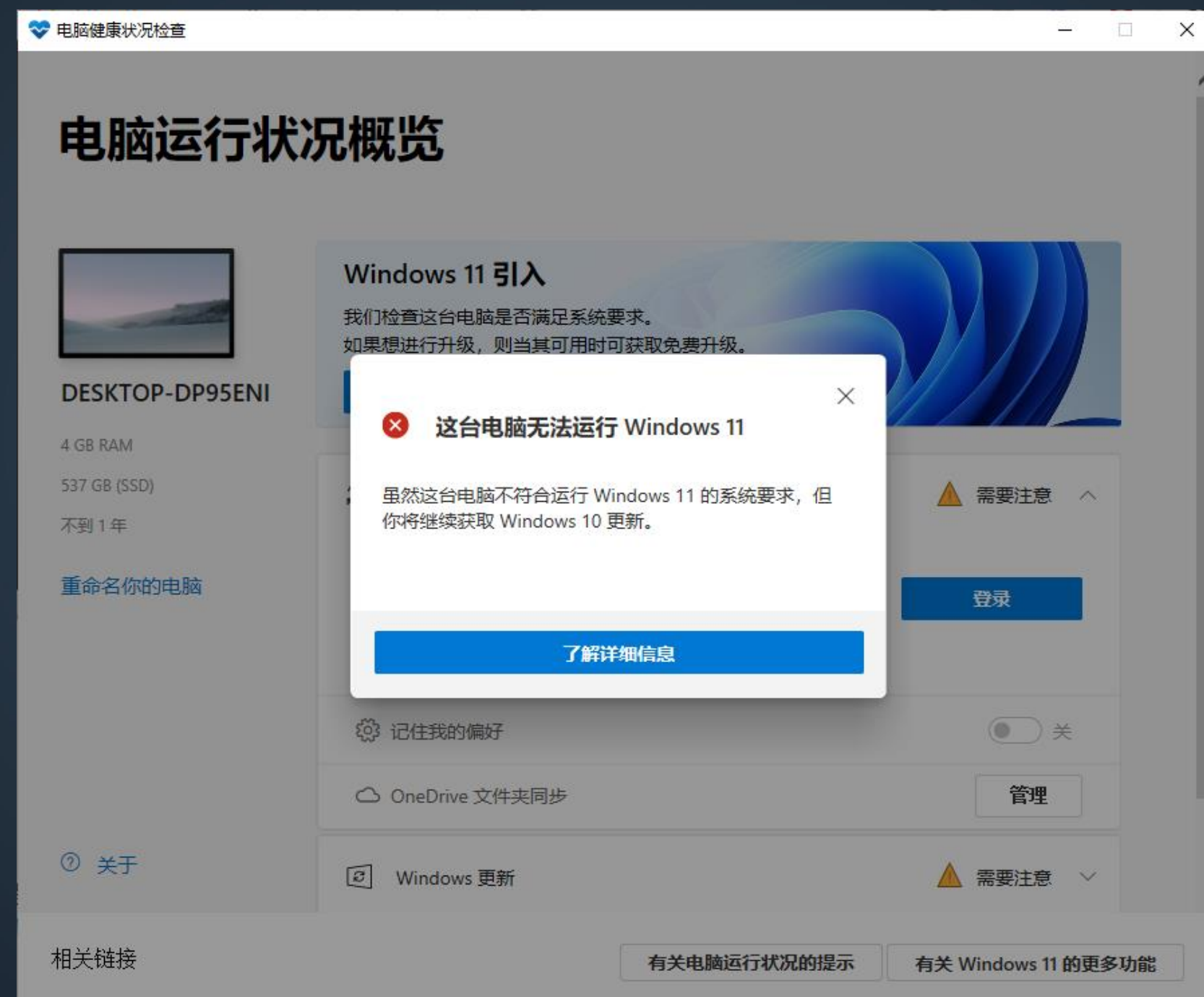
Windows安全体系演进之路

绿盟科技天机实验室 张云海

2021年6月微软发布Windows 11



2021年6月微软发布Windows 11



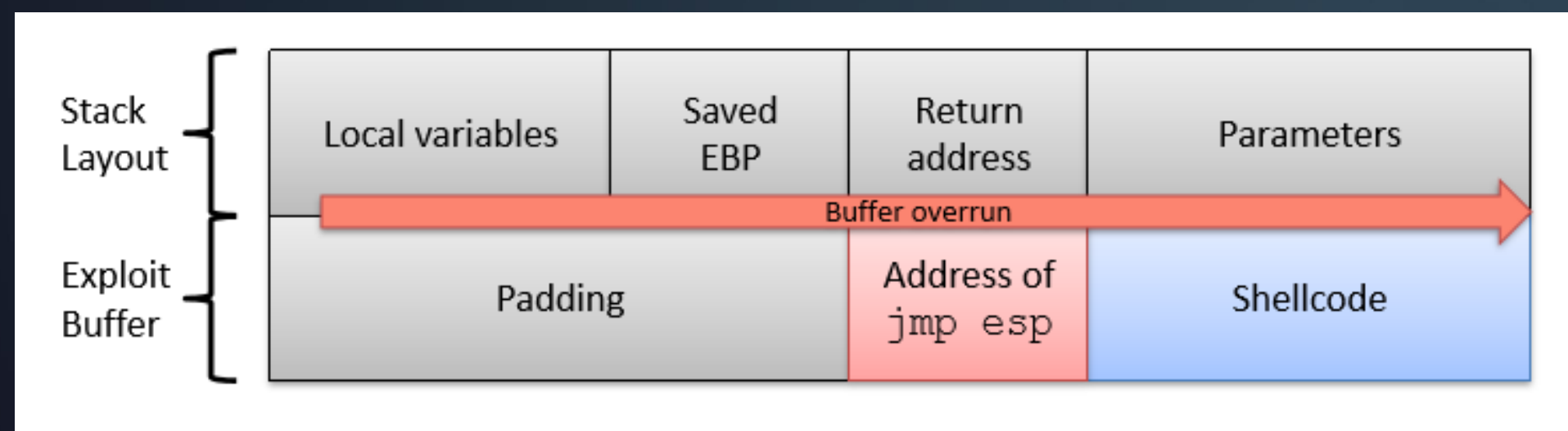
2021年6月微软发布Windows 11



最低系统要求

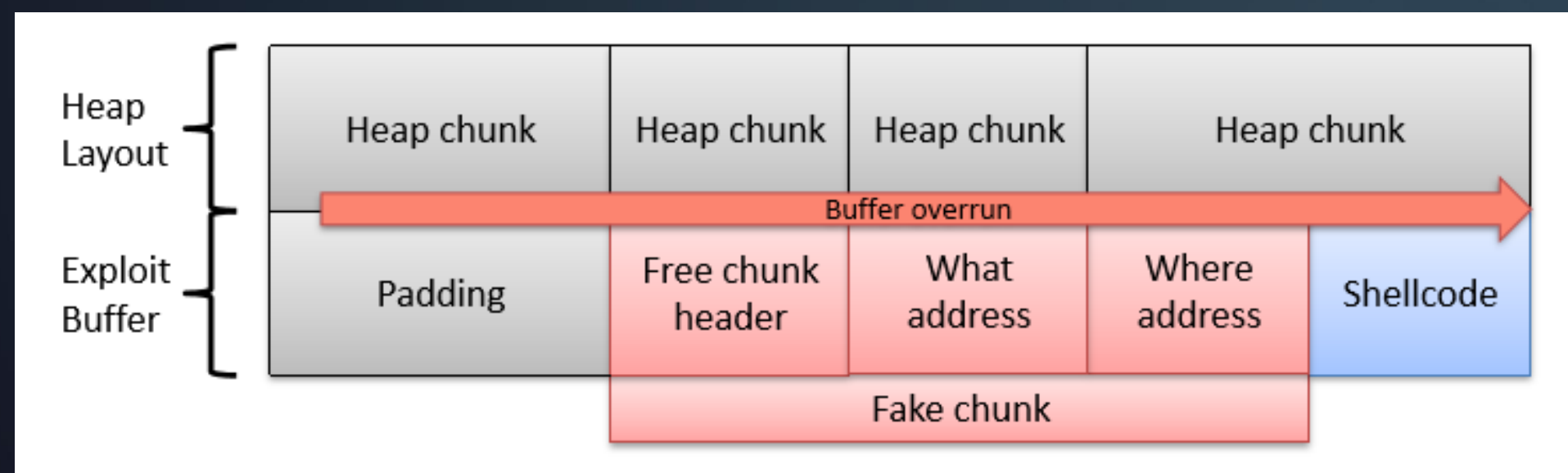
处理器	1 GHz 或更快的 支持 64 位的处理器 (双核或多核) 或系统单芯片 (SoC)	显卡	支持 DirectX 12, 支持 WDDM 2.x
内存	4 GB RAM	显示器	大于 9 英寸, HD 高分辨率 (720p)
存储	64 GB 或更大的存储设备	Internet 连接	Windows 11 家庭版的设置需要具有 Microsoft 帐户和 Internet 连接
系统固件	支持 UEFI 安全启动	某些功能需要特定的硬件, 请参见详细的 系统要求 。	
TPM	可信平台模块 (TPM) 版本 2.0		

- 缓解措施的引入
 - 2000年之前没有缓解措施
 - 主流漏洞类型是栈缓冲区溢出

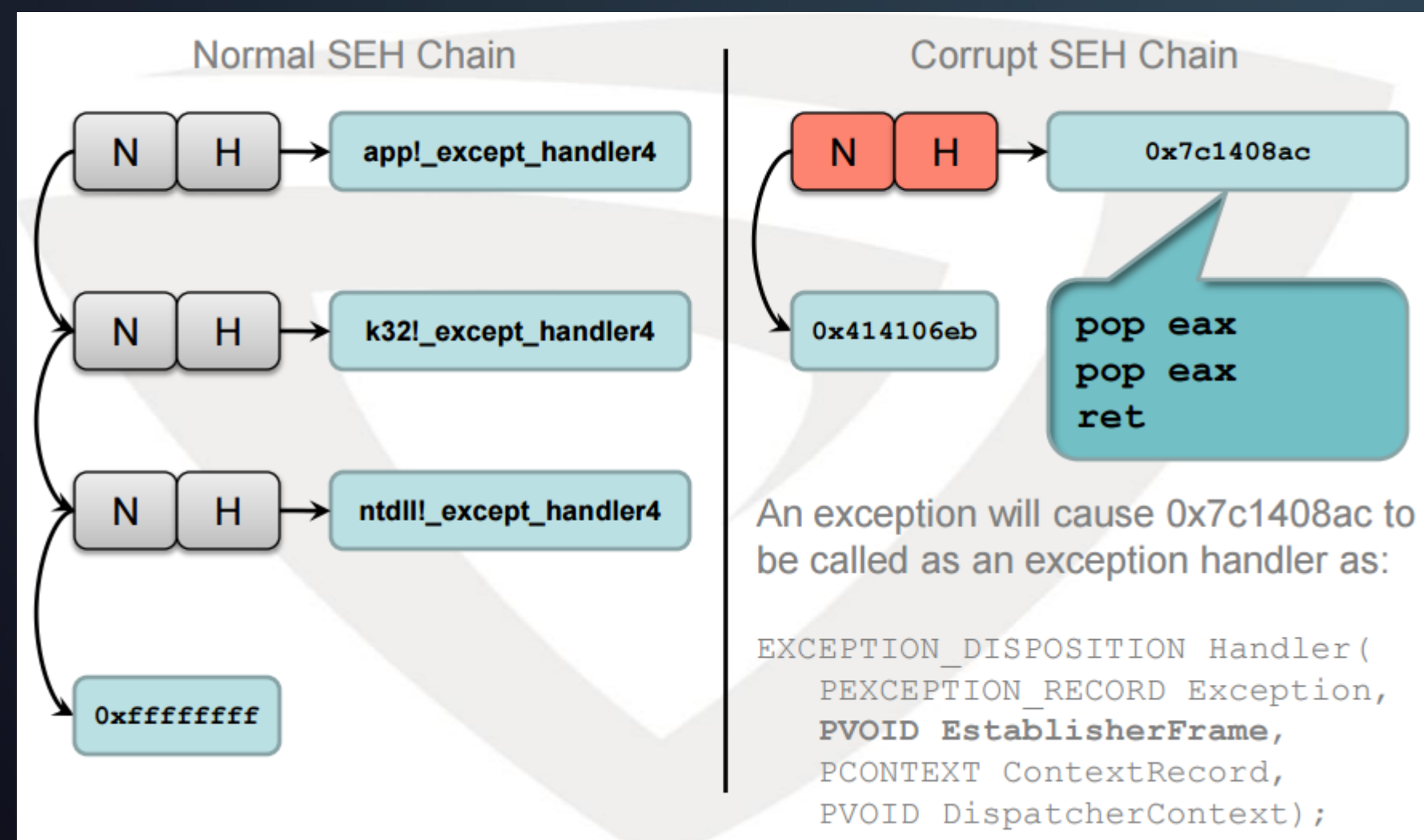




- 缓解措施的引入
 - 2002年引入保护栈的缓解措施
 - 堆缓冲区溢出漏洞开始成为主流



- 缓解措施的引入
 - 2004年引入保护堆的缓解措施
 - 缓解对抗开始成为漏洞利用的重点





- 缓解措施的引入
 - 2006年引入ASLR和DEP
 - 缓解绕过成为高级漏洞利用技术中的必备

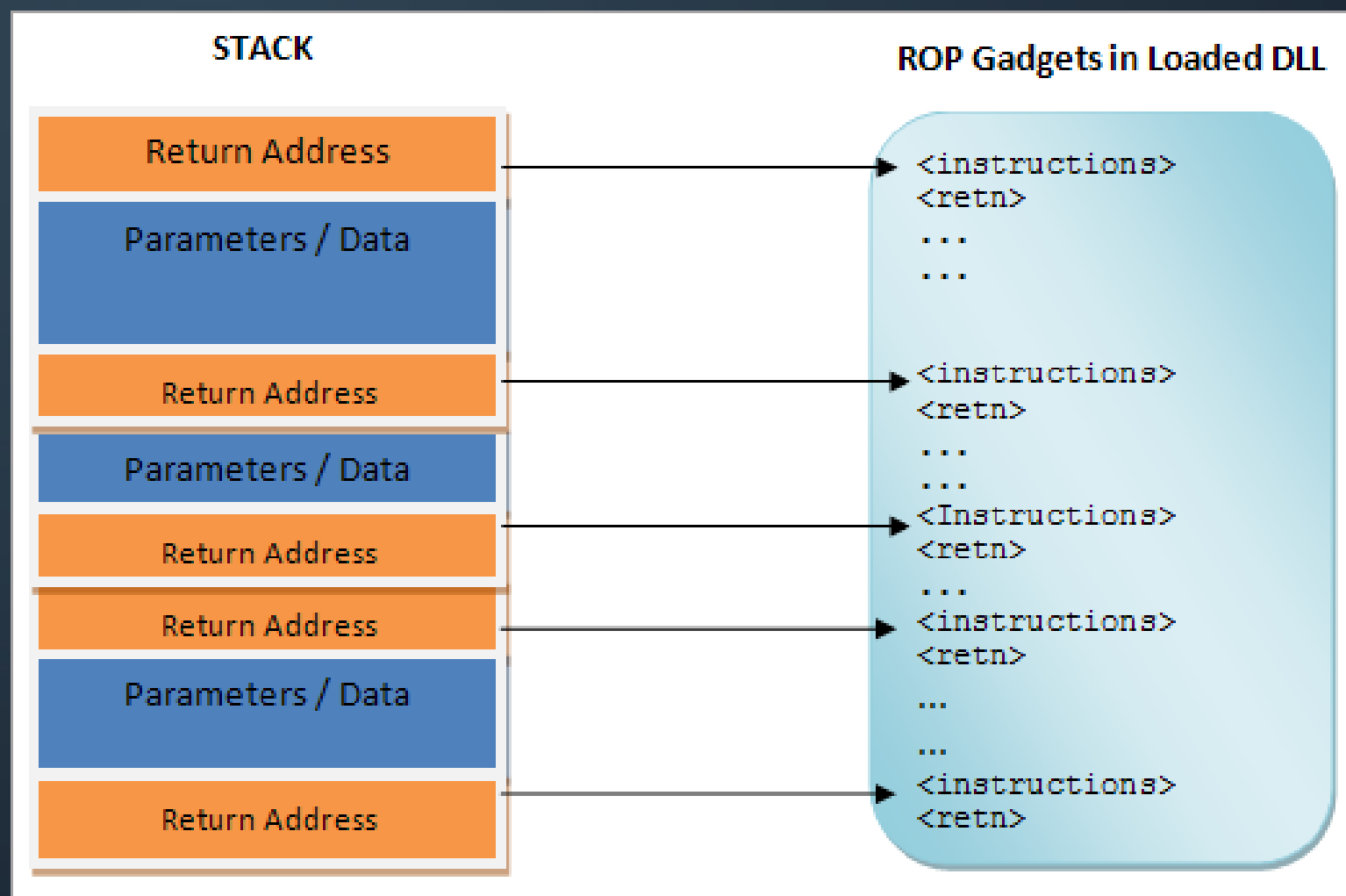
```
var ret=(0x3C909090^0x3C909090^0x3C909090^0x3C909090);
```



```
0x1A1A0100: B89090903C MOV EAX, 3C909090
0x1A1A0105: 359090903C XOR EAX, 3C909090
0x1A1A010A: 359090903C XOR EAX, 3C909090
0x1A1A010F: 359090903C XOR EAX, 3C909090
```

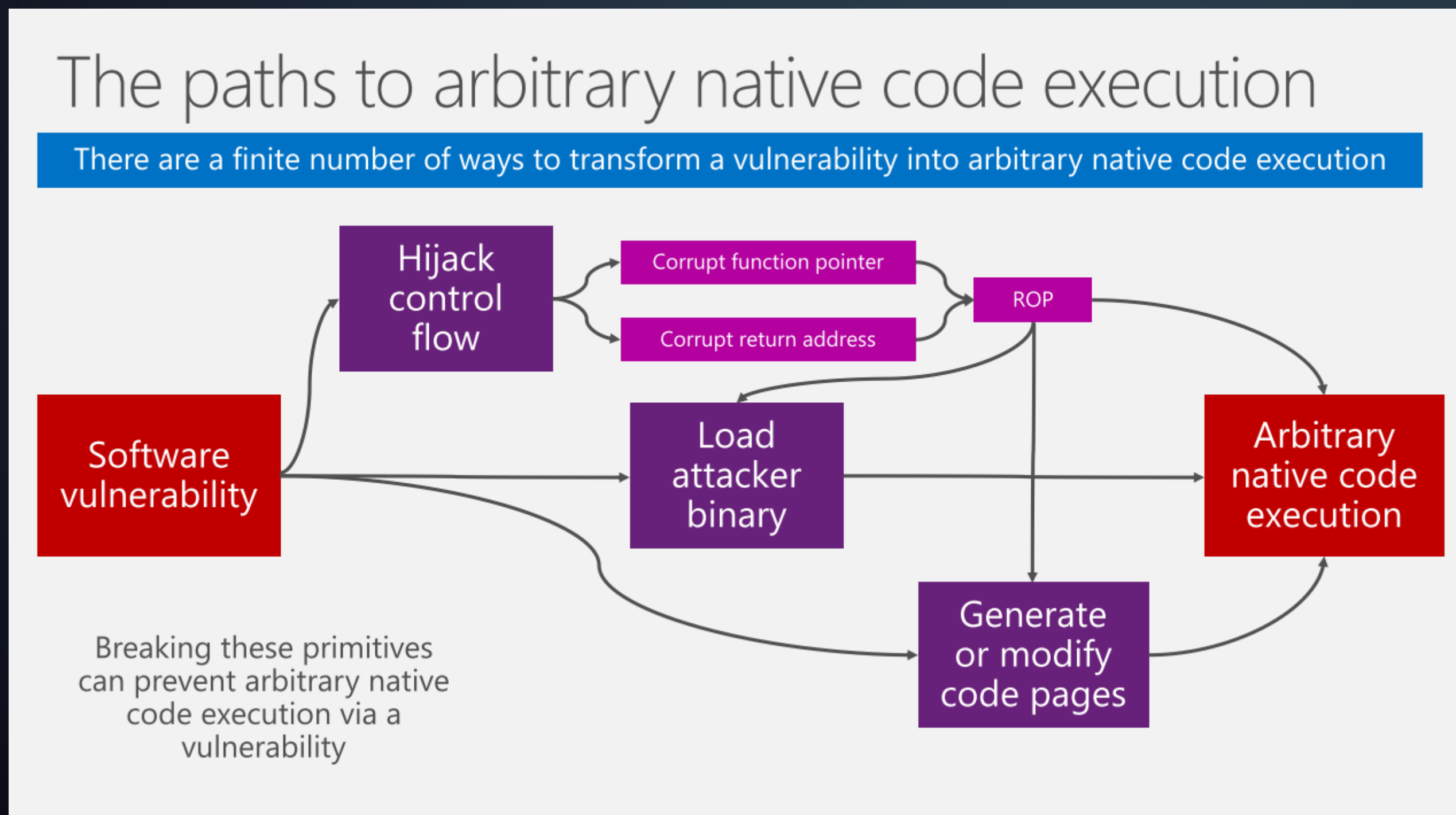


```
0x1A1A0101: 90 NOP
0x1A1A0102: 90 NOP
0x1A1A0103: 90 NOP
0x1A1A0104: 3C35 CMP AL, 35
0x1A1A0106: 90 NOP
0x1A1A0107: 90 NOP
0x1A1A0108: 90 NOP
0x1A1A0109: 3C35 CMP AL, 35
```





• 安全体系的建立





• 安全体系的建立

Technologies for mitigating code execution

Prevent
arbitrary code
generation

Code Integrity Guard

Images must be signed and load
from valid places

Arbitrary Code Guard

Prevent dynamic code generation,
modification, and execution

Prevent
control-flow
hijacking

Control Flow Guard

Enforce control flow integrity
on indirect function calls

Intel CET

Enforce control flow integrity on
function returns

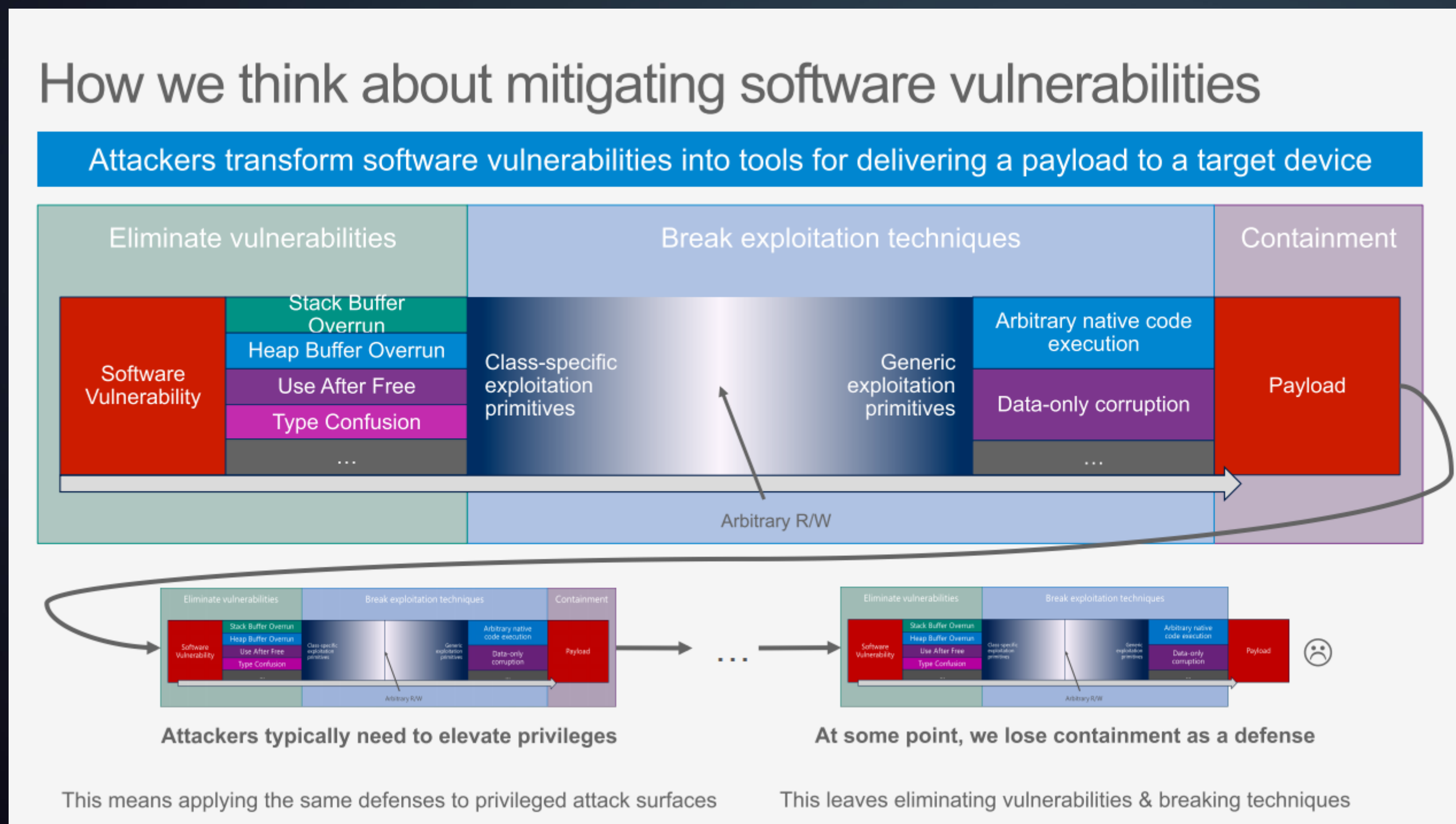
✓ Only valid, signed code pages can
be mapped by the app

✓ Code pages are immutable and
cannot be modified by the app

✓ Code execution stays “on the rails”
per the control-flow integrity policy

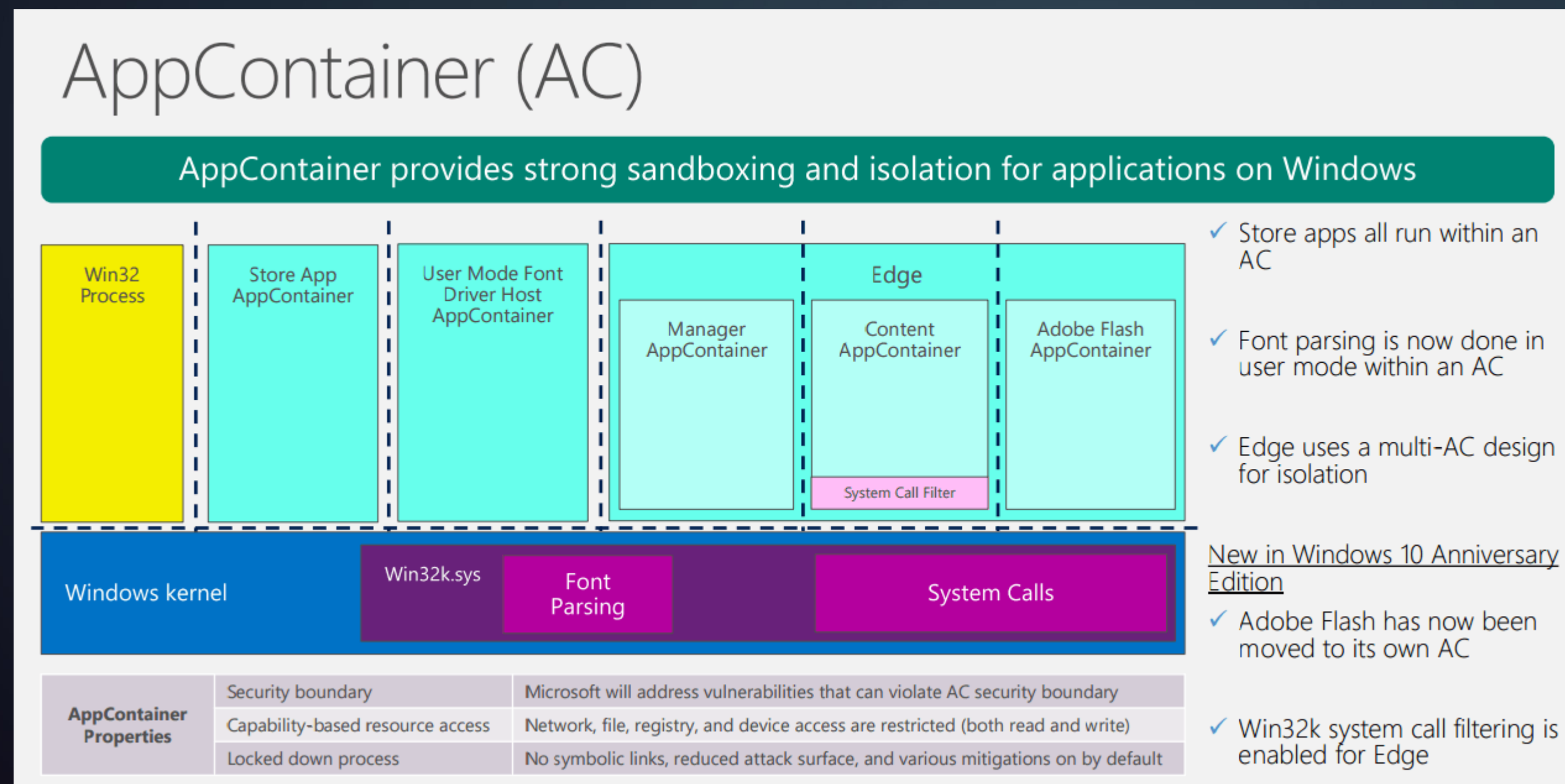


• 安全体系的建立



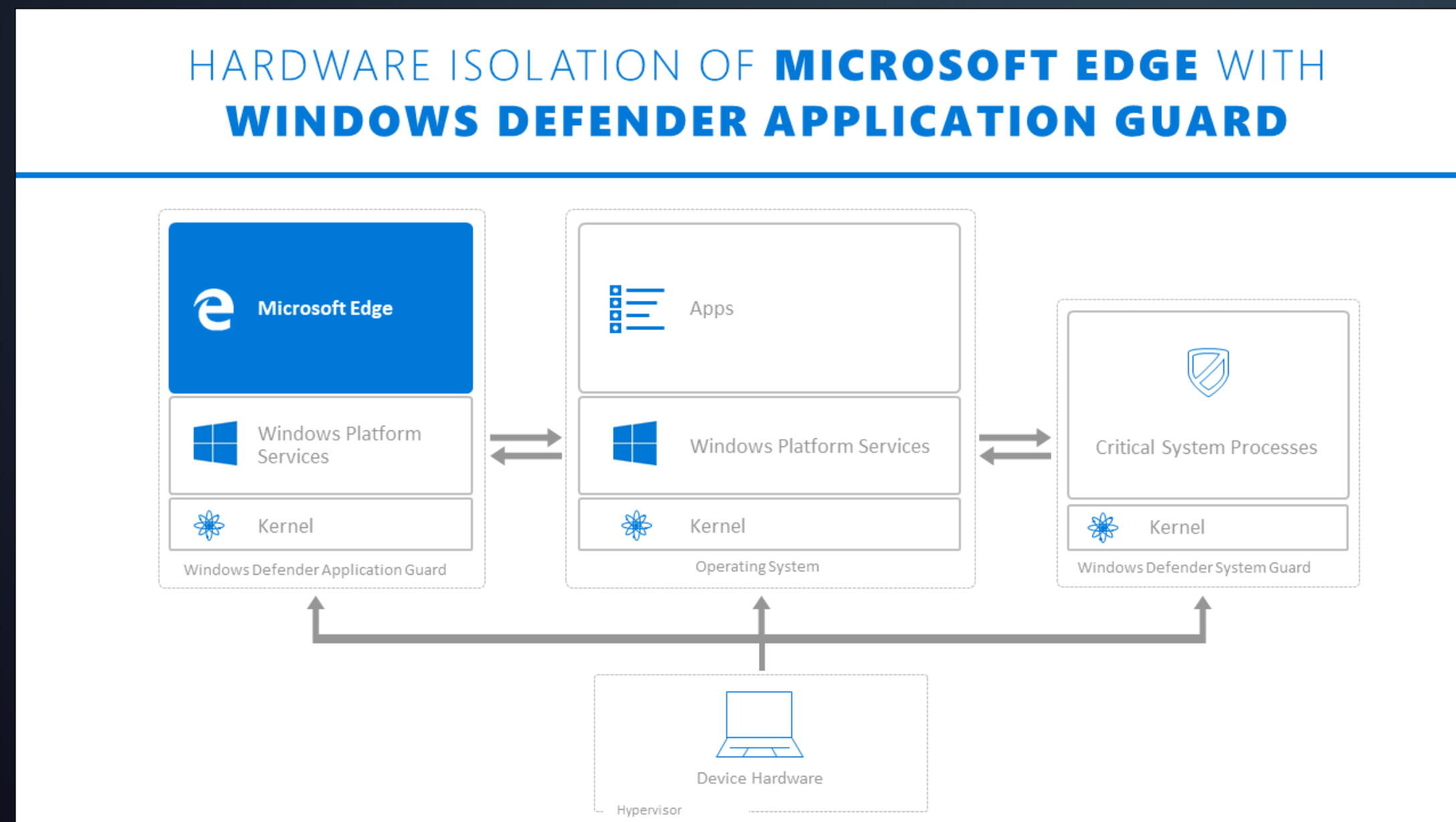


- 安全体系的建立
 - 应用沙箱



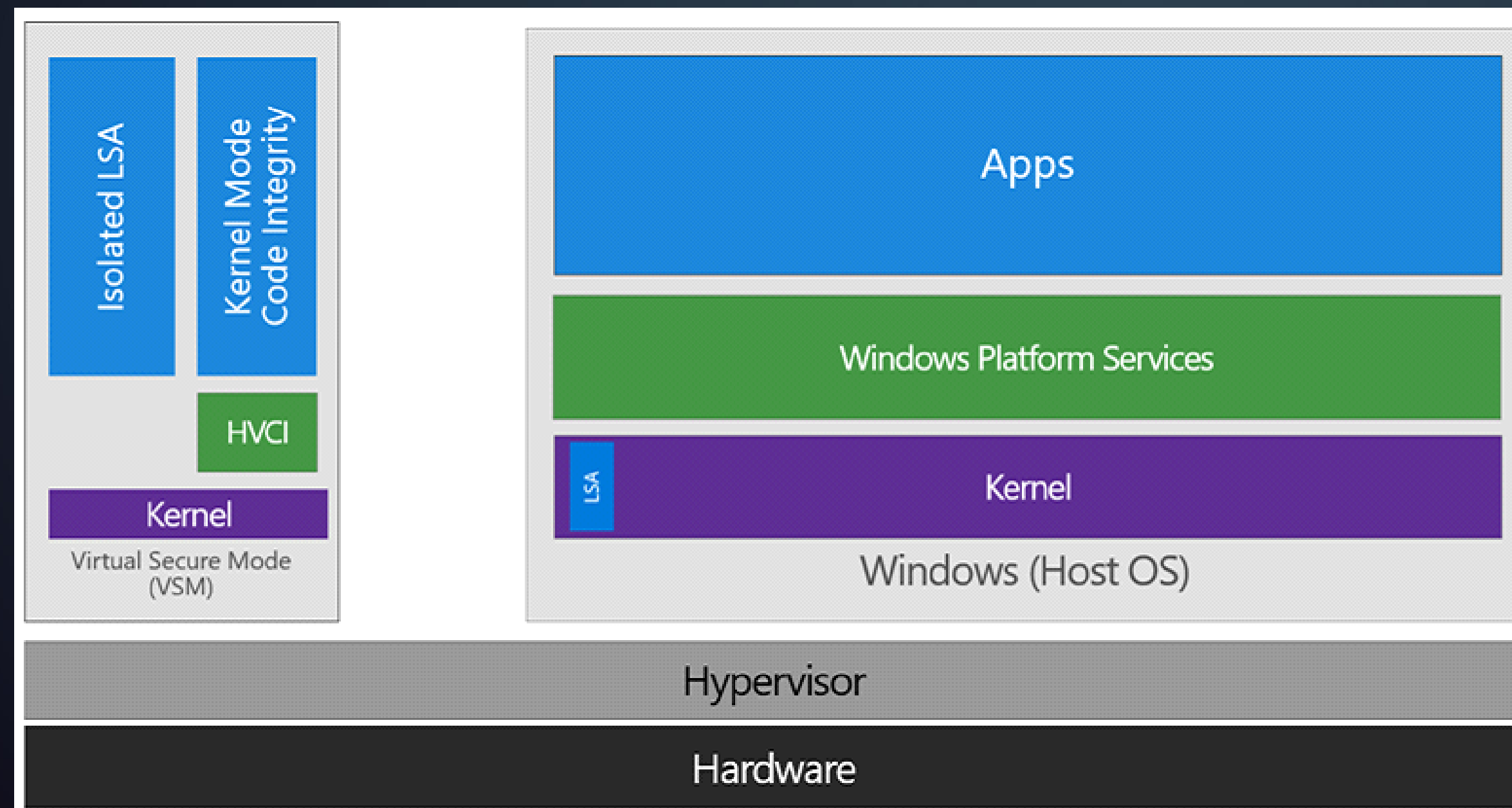


- 安全体系的建立
 - Windows Defender 应用程序防护





- 安全体系的建立
 - 基于虚拟化的安全



Windows安全体系发展历史

- 安全体系的建立
 - 固件安全

Meet the most secure Windows PC

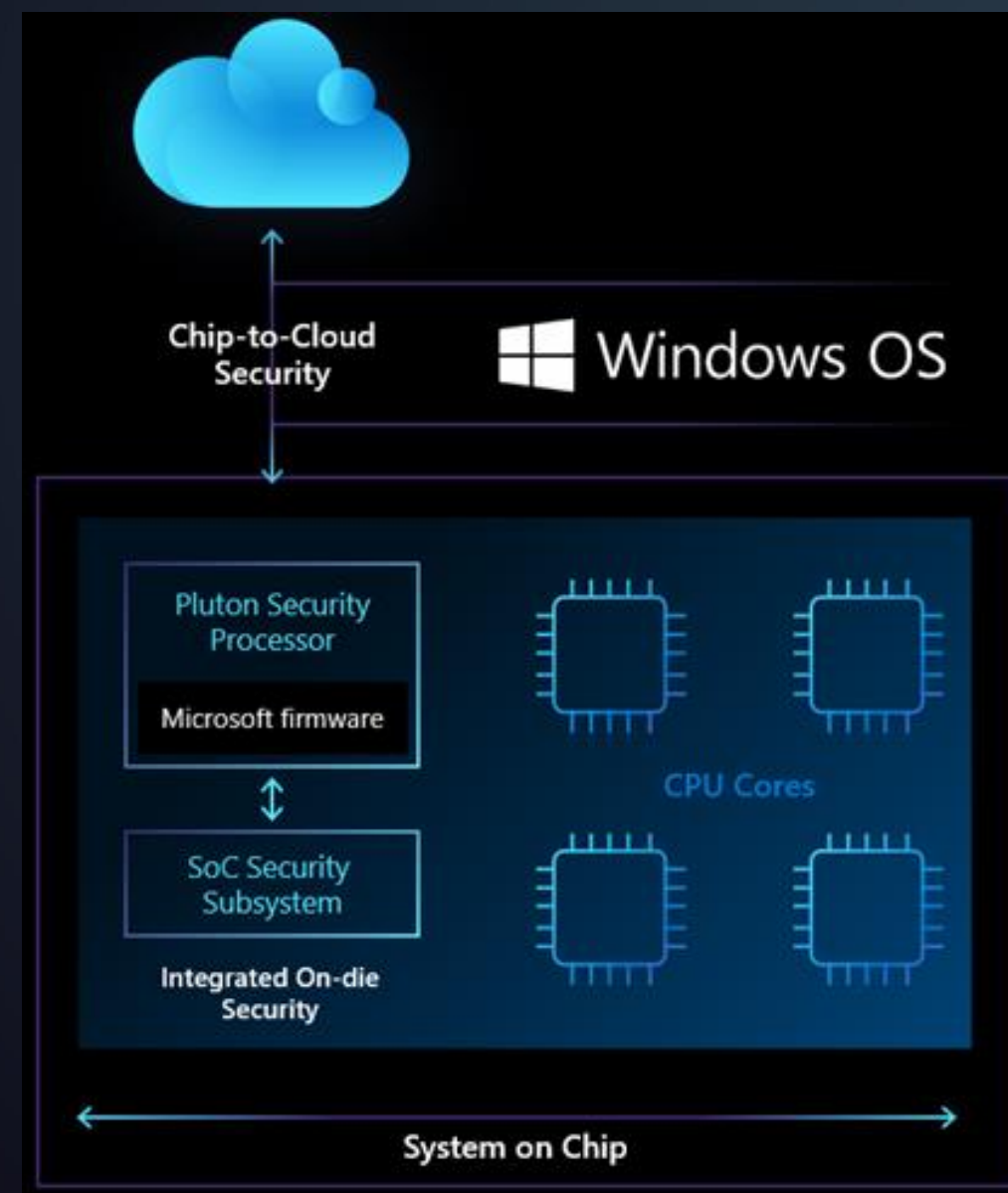
Secured-core PCs are the most secure Windows 10 devices out-of-the-box¹ with integrated hardware, firmware, software, and identity protection.

[▶ Watch Video](#)





- 安全体系的建立
 - 安全硬件



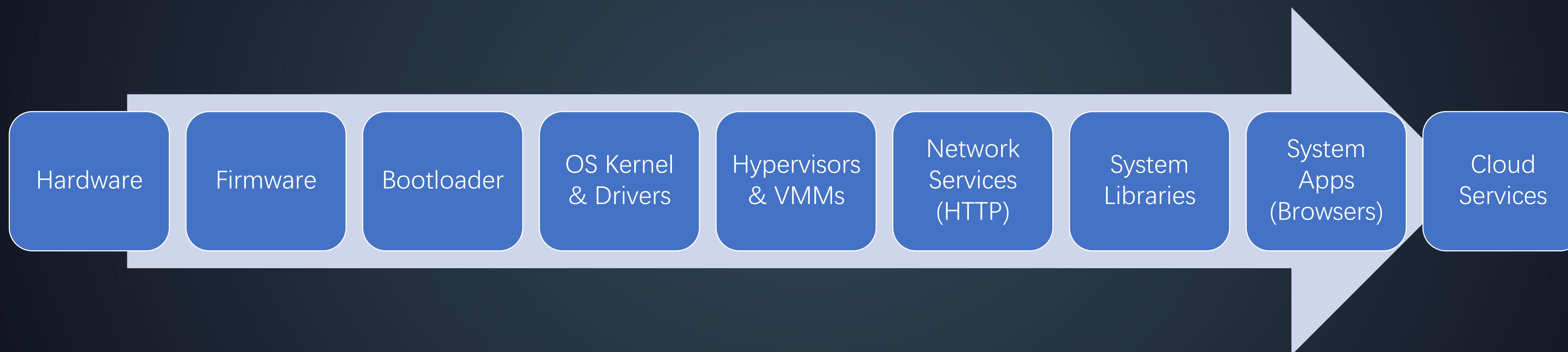


Windows安全体系的未来

- Windows 11建立了良好的安全体系基线
 - 缺省启用的安全机制
 - Virtualization-Based Security (VBS)
 - Hypervisor-protected Code Integrity (HVCI)
 - Secure Boot
 - Windows Hello
 - 支持的硬件安全特性
 - Hardware-enforced Stack Protection
 - Microsoft Pluton security processor



• 从芯片到云端的安全体系设计

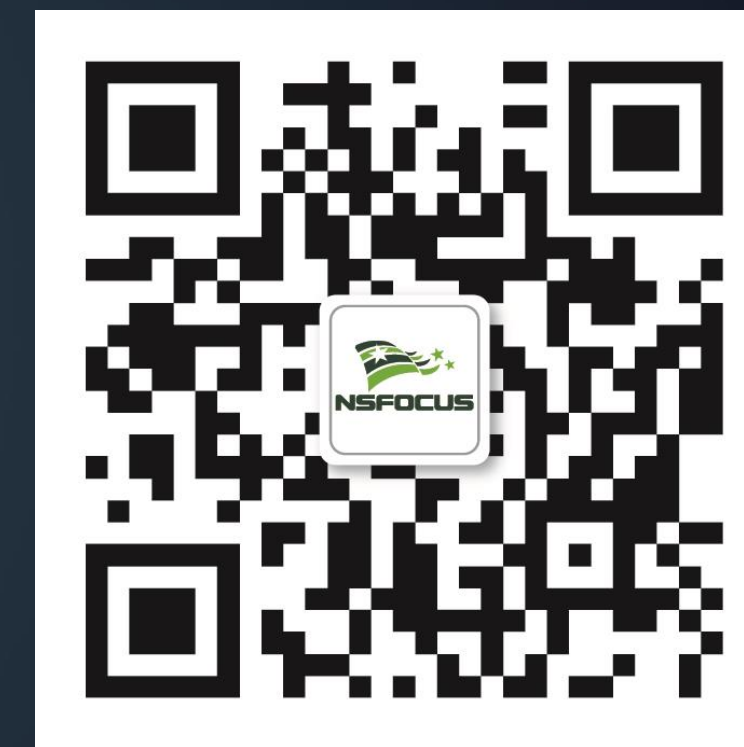


THANKS

欢迎关注绿盟科技
了解更多安全资讯



微信公众号



新浪微博