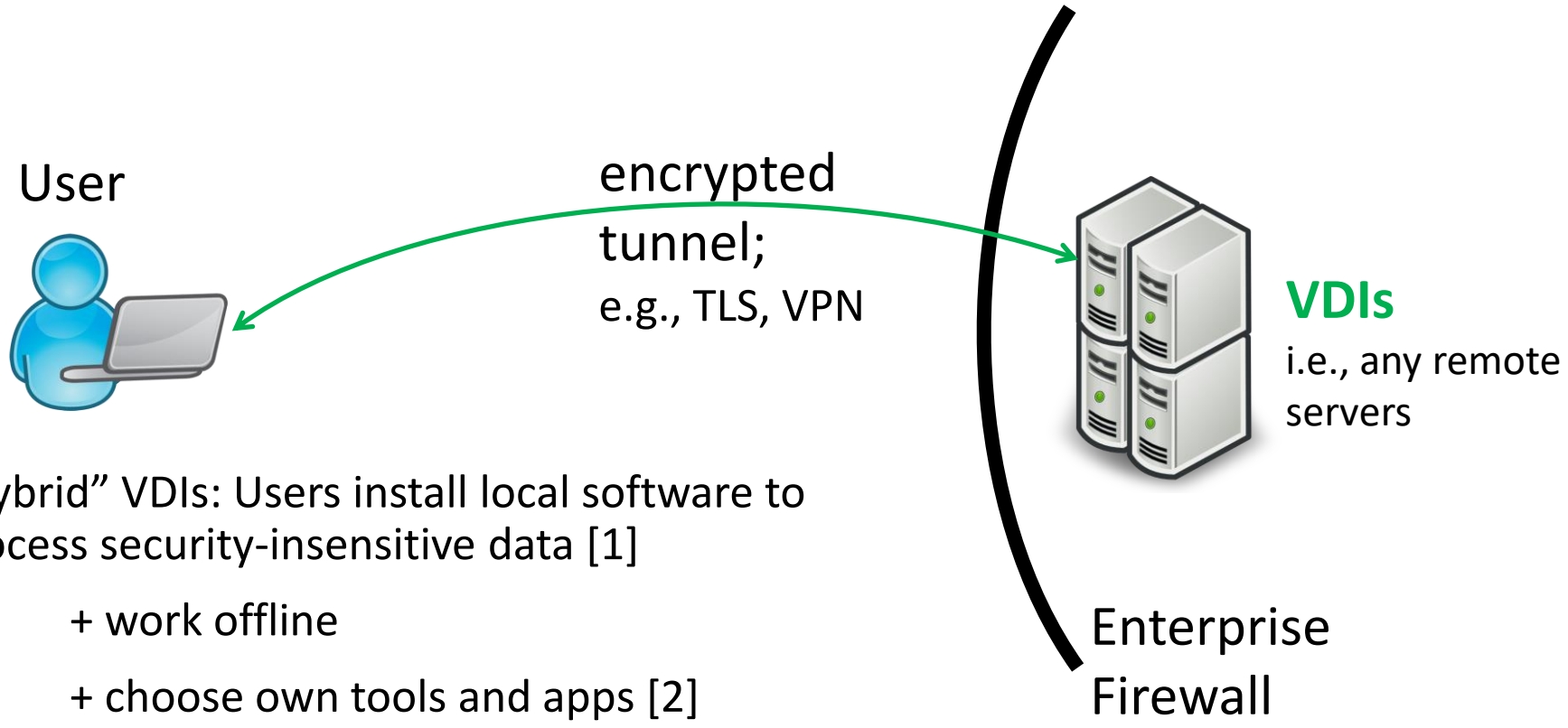
Secure VDI Client on Untrusted Endpoints

Secure Virtual Desktop Infrastructure (VDI) for Enterprise IT Security

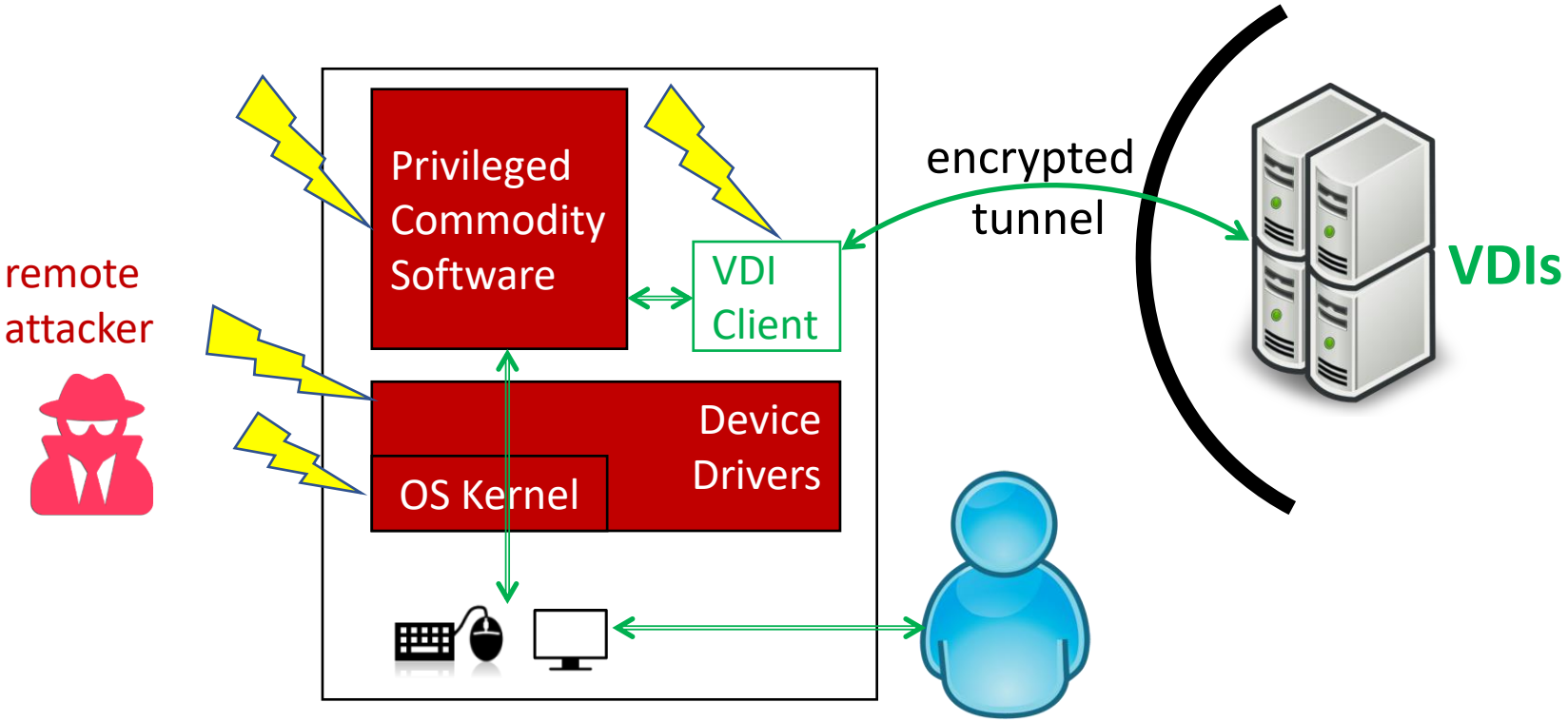


- "Hybrid" VDIs: Users install local software to process security-insensitive data [1]
  - + work offline
  - + choose own tools and apps [2]
  - + setup golden VDI images; i.e., less software

[1] VMWare. Is VDI dead?. 2018
[2] Gartner. Satisfy Digital Workers and Improve Employee Experience by Embracing Choice of Workplaces and Tools. 2020

Problem: No *End-to-End* Security to VDIs

***Huge untrusted code base → Many 0-day vulnerabilities* [1]**

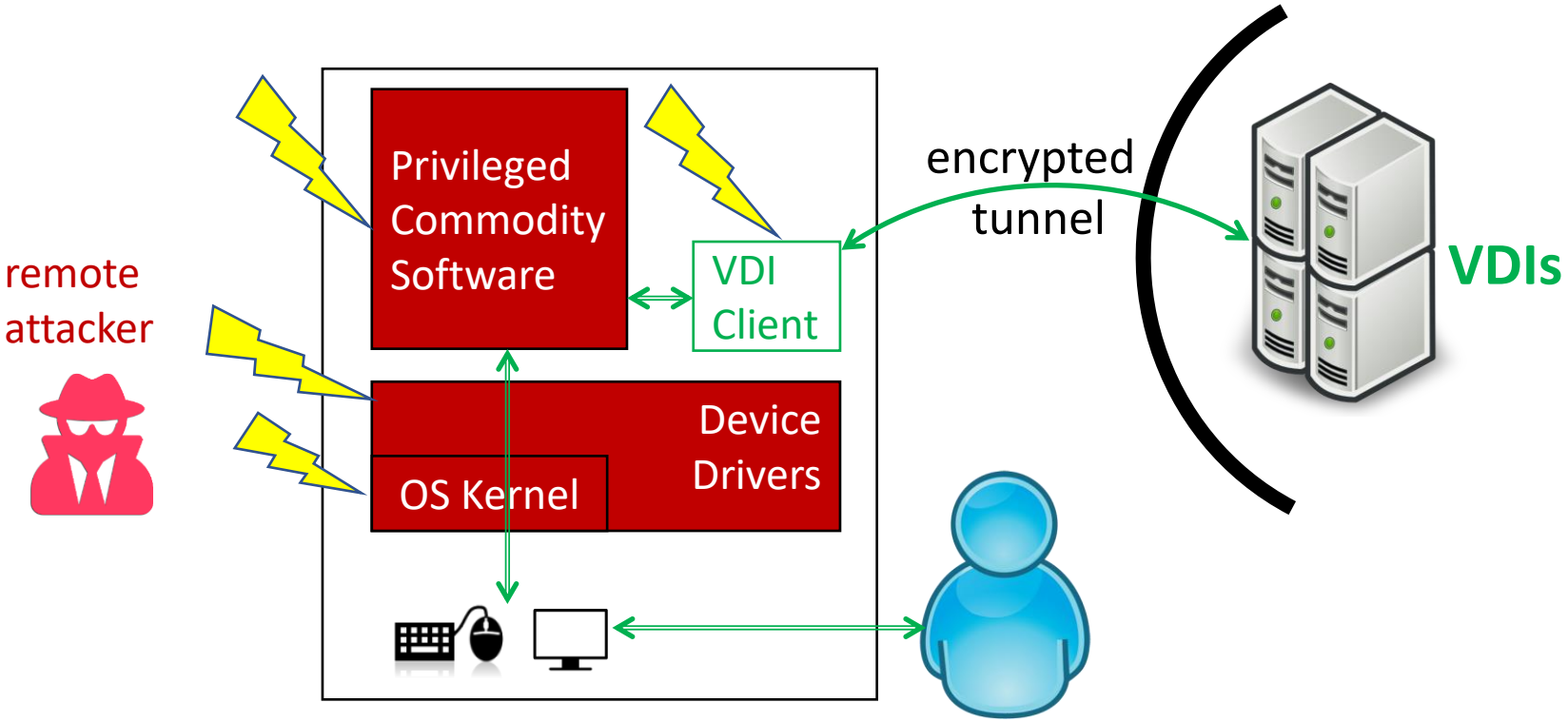


Need: ***trusted path User*** <-> VDI client

[1] Klein et al. *seL4*: Formal Verification of an OS Kernel. SOSP. 2009

Problem: No *End-to-End* Security to VDIs

***Huge untrusted code base → Many 0-day vulnerabilities* [1]**

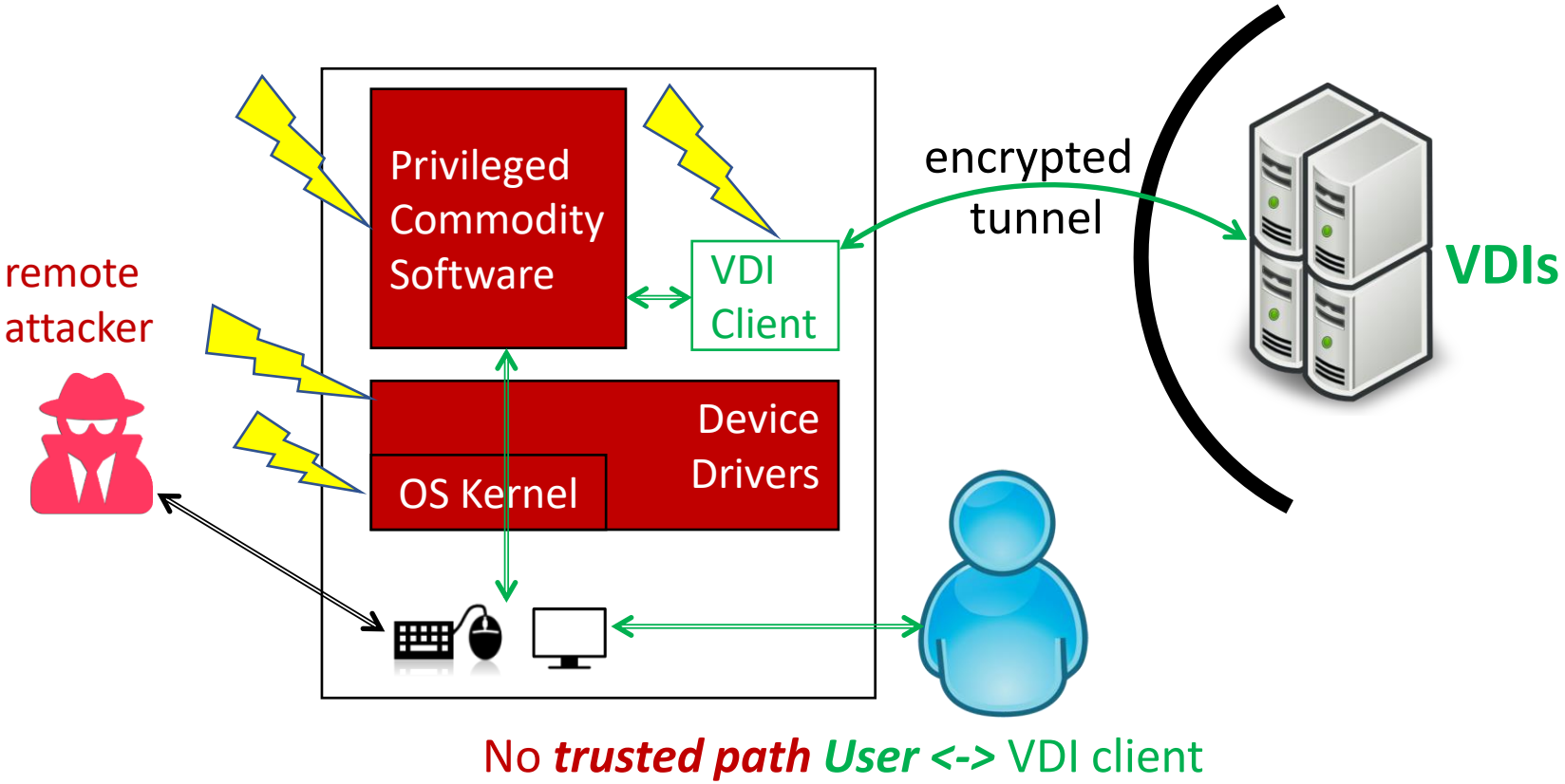


Attackers

- ***capture*** screen and view confidential data on VDIs
- ***capture*** user's keystrokes; e.g., passwords
- ***inject*** fake keystrokes to modify sensitive data
- ***corrupt*** VDI client process

Problem: No *End-to-End* Security to VDIs

***Huge untrusted code base → Many 0-day vulnerabilities* [1]**



Consequence:

Attackers have *same* VDI data accesses as the unsuspecting users,

despite *perfect network & VDI security*

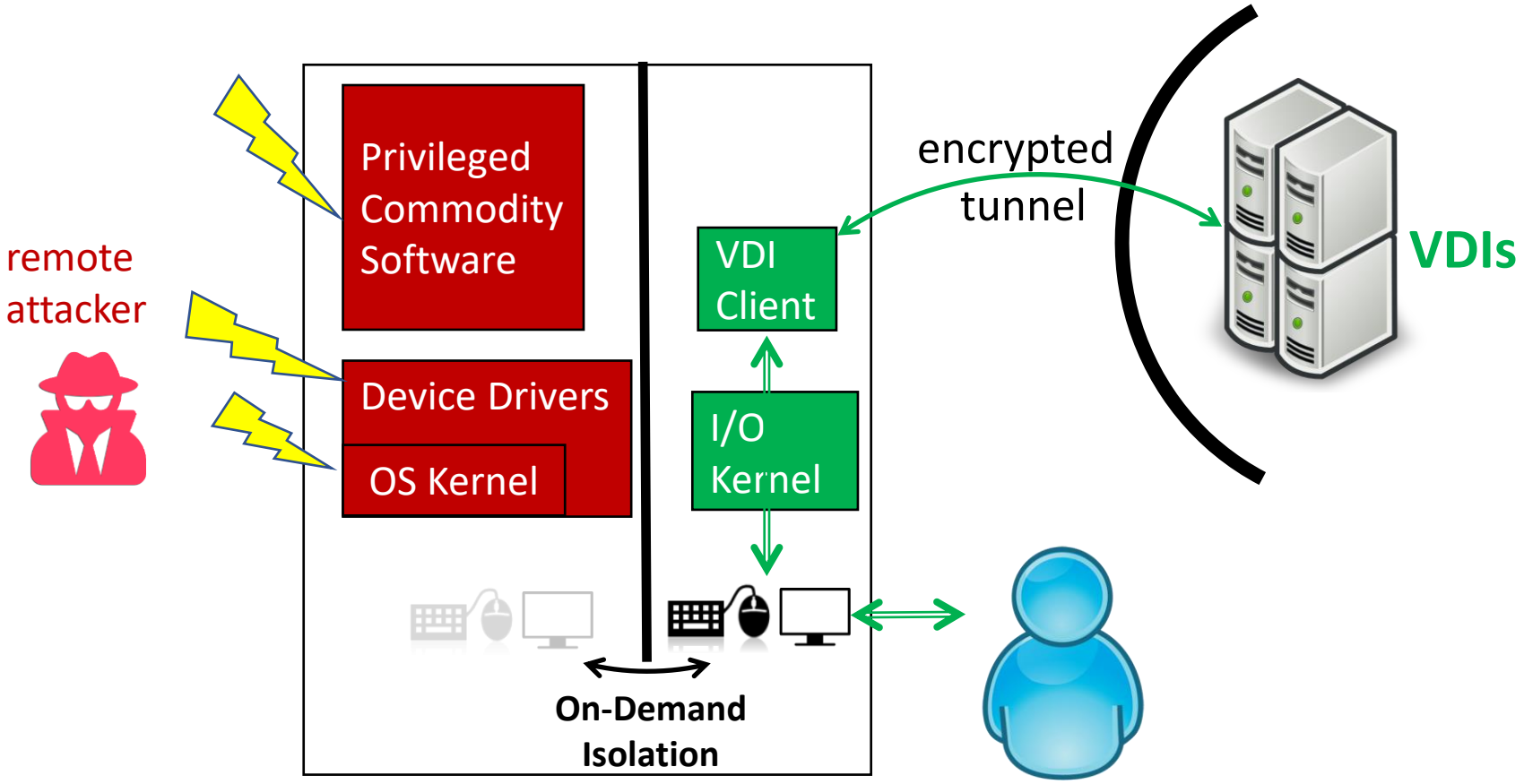
Inadequacy of Current Solutions

- Insecure
  - Antivirus Tools, Firewall – broken by undiscovered attacks
  - VPN – broken by local virus and malware
  - Bromium, Hysolate, Forcepoint Trusted Thin Client – broken by security flaws in huge code base

- Violate users' experience
  - Forcepoint Trusted Thin Client – very few local apps supported

- Incompatible with Enterprise Applications
  - Green Hills' *Integrity MultiVisor* – limited to embedded systems only

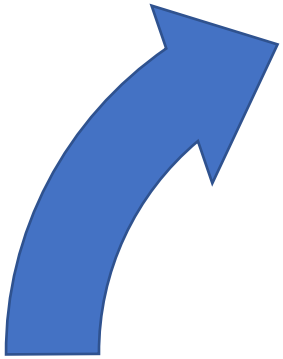
Our Solution: On-Demand Isolation

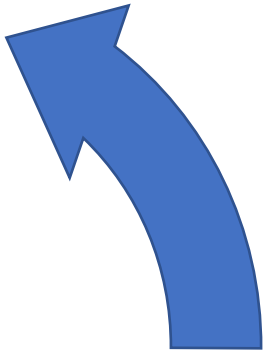


Security Guarantee:
Attackers ***can no longer break*** user's trusted path,
regardless of how they ***compromises other software***; e.g., OS, apps, users' tools

Advantages of Our Solution

- Usable security despite *any* commodity OS/apps 0-day flaws
  - commodity OS/apps will *always* exhibit 0-day flaws; see axioms of insecurity

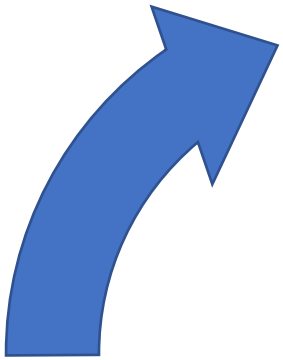


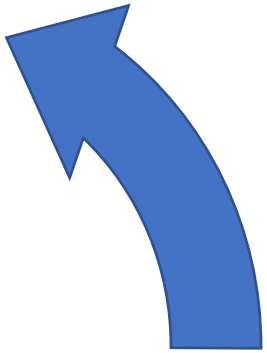


Security Guarantee:
Attackers ***can no longer break*** user's trusted path,
regardless of how they ***compromises other software***; e.g., OS, apps, users' tools

Advantages of Our Solution

- Usable security despite *any* commodity OS/apps 0-day flaws
  - commodity OS/apps will *always* exhibit 0-day flaws; see axioms of insecurity
  - maintain users' experience
    - users can process security insensitive data with commodity local tools/apps

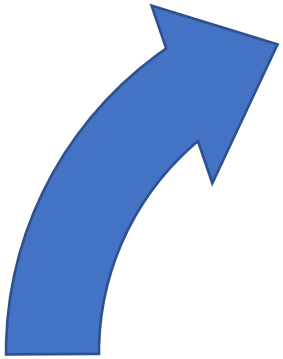


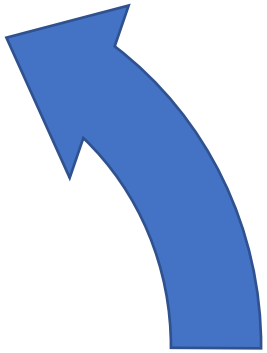


Security Guarantee:
Attackers ***can no longer break*** user's trusted path,
regardless of how they ***compromises other software***; e.g., OS, apps, users' tools

Advantages of Our Solution

- Usable security despite *any* commodity OS/apps 0-day flaws
  - commodity OS/apps will *always* exhibit 0-day flaws; see axioms of insecurity
  - maintain users' experience
  - reduce enterprise IT cost
    - eliminate IT administrative labor to maintain VDI security





Security Guarantee:
Attackers ***can no longer break*** user's trusted path,
regardless of how they ***compromises other software***; e.g., OS, apps, users' tools

Advantages of Our Solution

- Usable security despite *any* commodity OS/apps 0-day flaws
  - commodity OS/apps will *always* exhibit 0-day flaws; see axioms of insecurity
  - maintain users' experience
  - reduce enterprise IT cost

On-Demand Isolation:

- Security with mathematical proofs!

- Many more secure applications!

- Support PCs, laptops, mobile phones, tablets!

Other solutions

Insecure

Antivirus,
Firewall

Hysolate,
Bromium

Forcepoint
Trusted Thin Client

Violate Users' Experience

Forcepoint
Trusted Thin Client

Incompatible with Enterprise Apps, Tools

Green Hills'
Integrity MultiVisor

Our solution

Secure by design,
Enable mathematically verified security

Maintains Users' Experience

Compatible with Enterprise Apps, Tools

Who Needs Our Solution?

(Limited to current VDI Markets)

- Large numbers of users need *secure remote* enterprise accesses
  - > **45 M** *enterprise employees* in > 7,000 enterprises globally [1]
    - most employees have 2~3 endpoints; e.g., PC, laptop, mobile phone, tablet
    - most employees work both on- and off-site
  - > **45 M** *government employees* in G-20 countries
  - Estimated **16.76 M** users on 2020-06-30 [1, 2, 3, 4]

- Other enterprises' employees
  - Rapid and steady *move to VDI*; e.g., ~$7B today, 16.5% CAGR [5]
  - Permanent shift to *secure remote access*; e.g., due to COVID-19

[1] HG Insights. Companies using "Citrix Virtual Desktops", "VMware Horizon", "Microsoft Windows Virtual Desktop". Count all companies have 10K+ employees as 30K. [Fetched on 2020-09-28]
[2] Citrix. Form 10-Q Quarterly Report. 2020-07-31. https://investors.citrix.com/financials/sec-filings/
[3] HG Insights. Companies using "Citrix Virtual Desktops", [Fetched on 2020-10-07]
[4] Citrix. Citrix Endpoint Management (Pricing). https://www.citrix.com/products/citrix-endpoint-management
[5] Allied Market Research. Cloud-based VDI Market Expected to Reach $10,154 Million by 2023. 2017

Go-To-Market Strategy

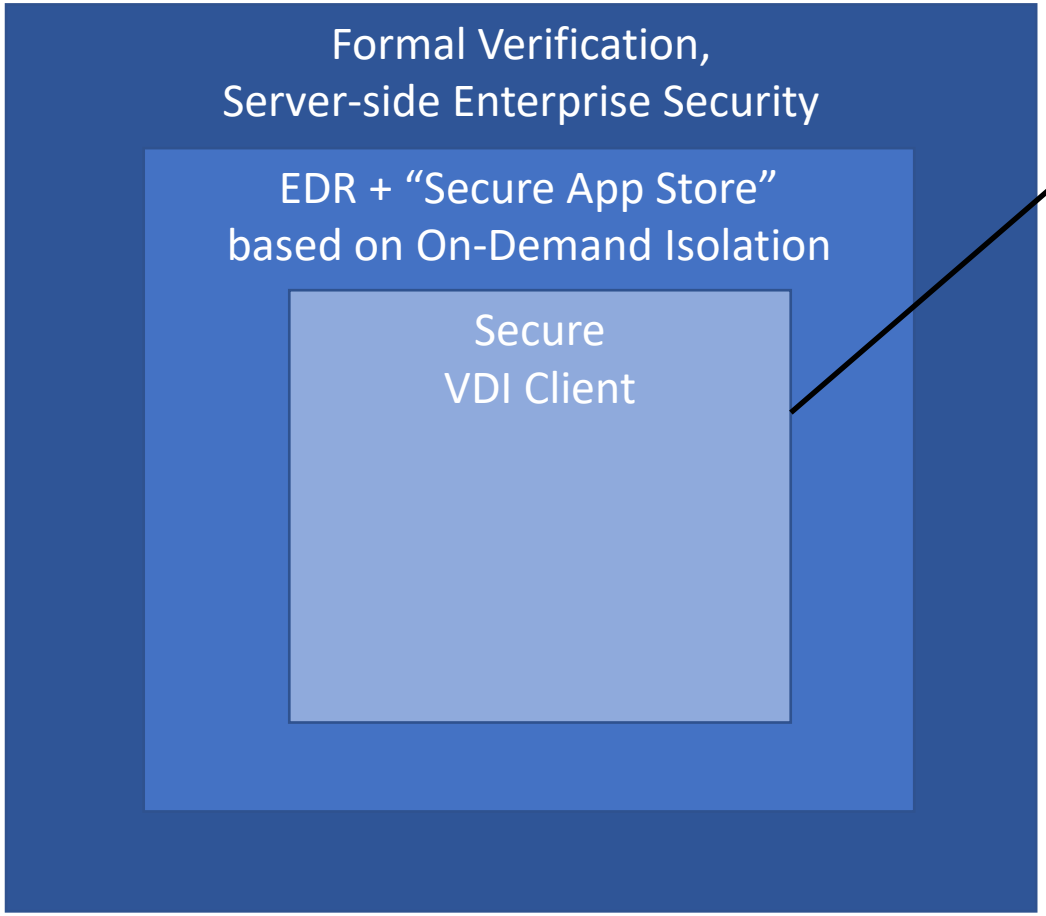
(Limited to current VDI Markets)

- For small and mid-size business: turn-key VDI solutions + IT security services
  - Reason 1: Satisfy great demand [1]
  - Reason 2: Solve the pain-point “Lack of staff or expertise in security” [2, 3]
  - Reason 3: Introduce in our solution to provide real security with a low cost

- For large business: Promote our secure VDI clients

[1] Allied Market Research. Cloud-based VDI Market Expected to Reach $10,154 Million by 2023. 2017
[2] Veeam. 2020 Data Protection Trends. 2020
[3] Gartner. The Managed Security Services Landscape Is Changing. 2020

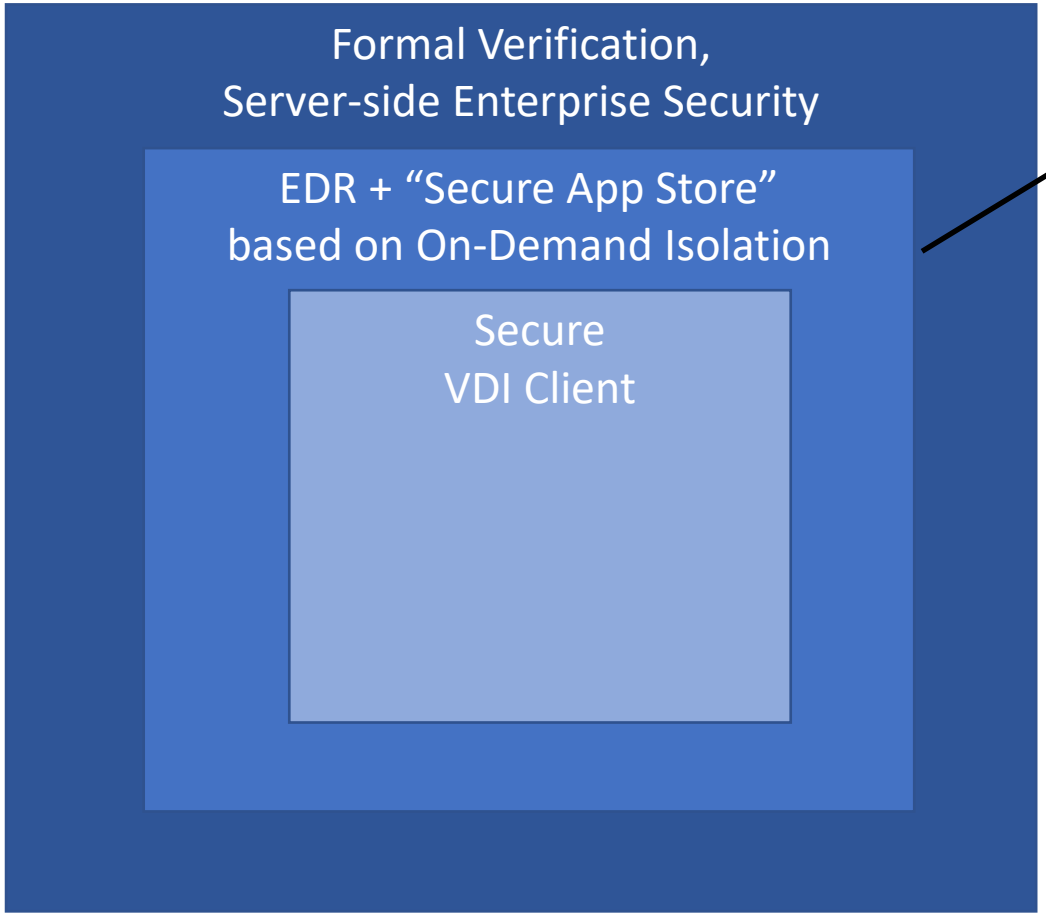
Future Plans



Short-term:

- Implement VDI client for PCs and laptops

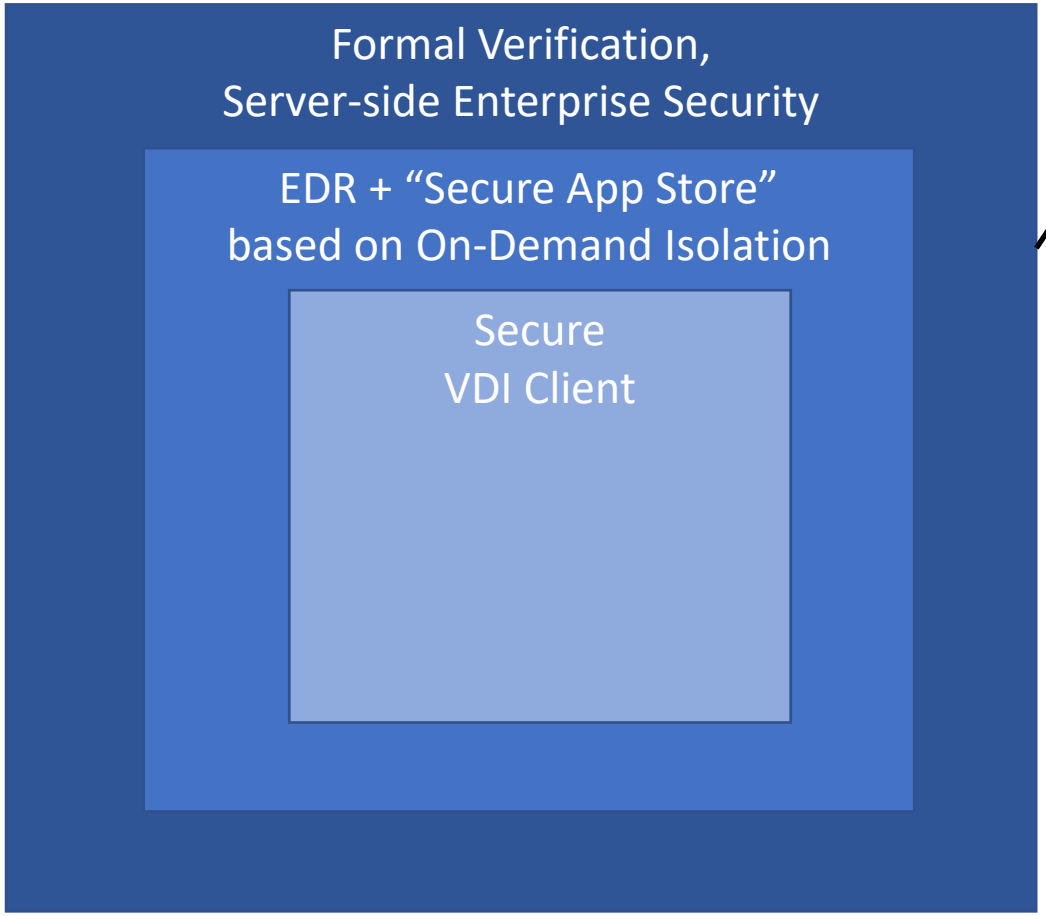
Future Plans



Mid-term:

- Implement VDI client for smart phones and tablets
- Establish an “App Store” based on our I/O Kernel and On-Demand Isolation
- Implement new Endpoint Detection and Response (EDR) approaches based on our tech

Future Plans



Mid-term:

- Complete mathematical verification of entire VDI client set
- Adopt our other secure solutions to protect server security

Level of Effort - Estimate

- Short-Term “Implement VDI client for PCs, laptops”
  - Timespan: ~1.0 year
  - No. of developers on I/O kernel and drivers for VDI client:
    2 (highly skilled) – 5 (average skilled)
  - No. of developers on VDI client: 2 - 3 (average skilled)
- Mid-Term
  - Timespan: ~ 2 – 2.5 years
  - No. of developers:
    6 (high skilled) – 12 (average skilled)
  - No. of developers on VDI client: 5 - 10 (average skilled)

Patents for On-Demand Isolation

- Current CMU Patents: 4
- Pending CMU Patents: 2