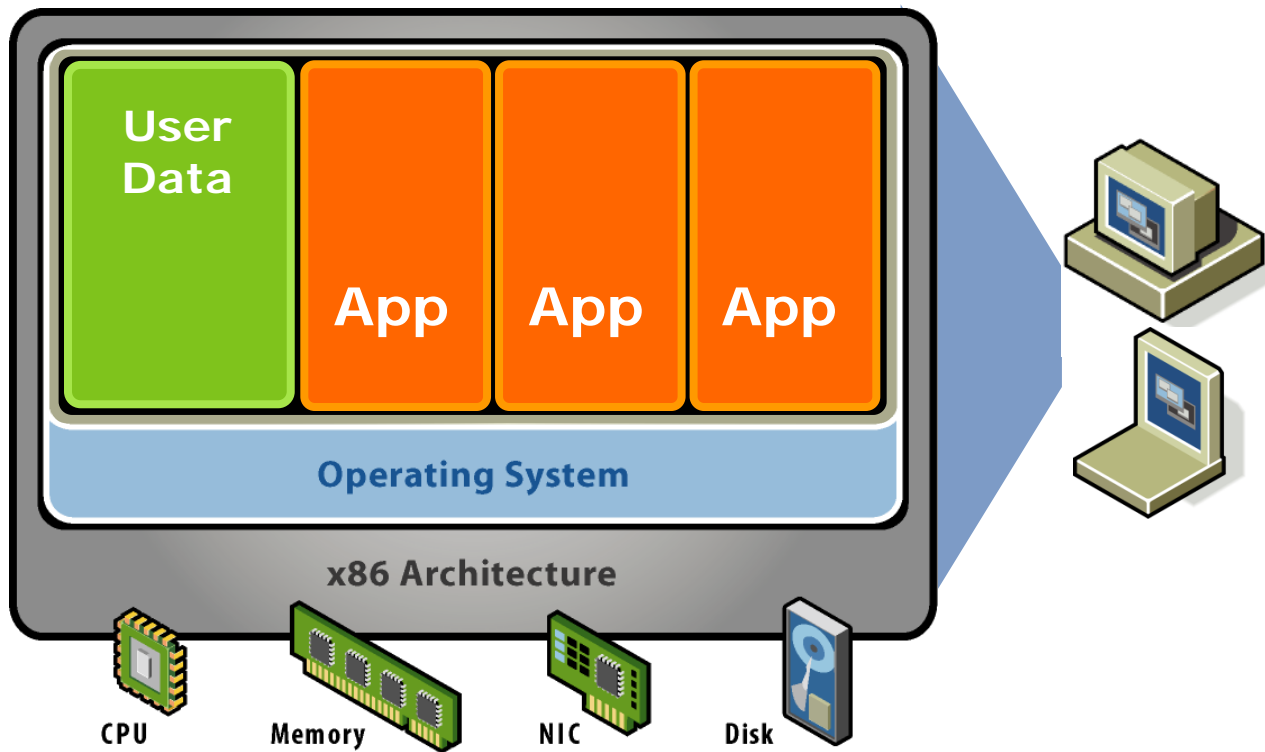




# Security in a Virtualized Mobile Environment

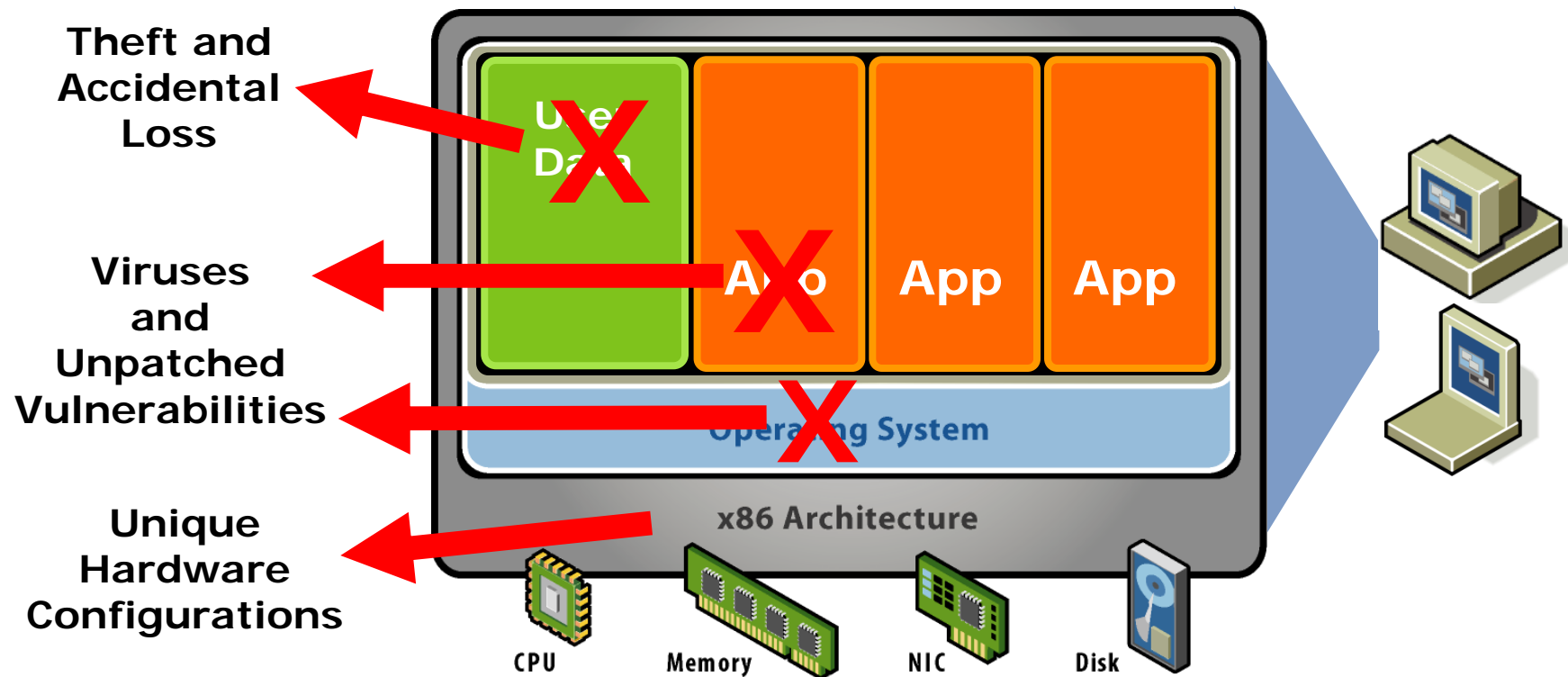
Jeff Umbarger  
Senior Systems Engineer – Public Sector  
[jumbarger@vmware.com](mailto:jumbarger@vmware.com)

## Typical Laptop / Desktop Configuration



A “standard” desktop is a unique blob of user data, applications, OS, and hardware drivers blended together.

## Problem: Management is difficult on the Edge



Many individual devices must be patched, monitored, and secured – a difficult task, especially for remote users.

## Mobile Computing Challenges – Lack of Control

- Mobile Users require greater rights than desktop users
  - Need control of network configurations
  - Often need to connect USB devices
- Connections to dangerous networks
- Sensitive Data Residing on Laptops
- More susceptible to malware
  - Little or no control over Internet access
  - Difficult to patch and apply antivirus updates
  - Infected systems difficult to recover or “clean-up”

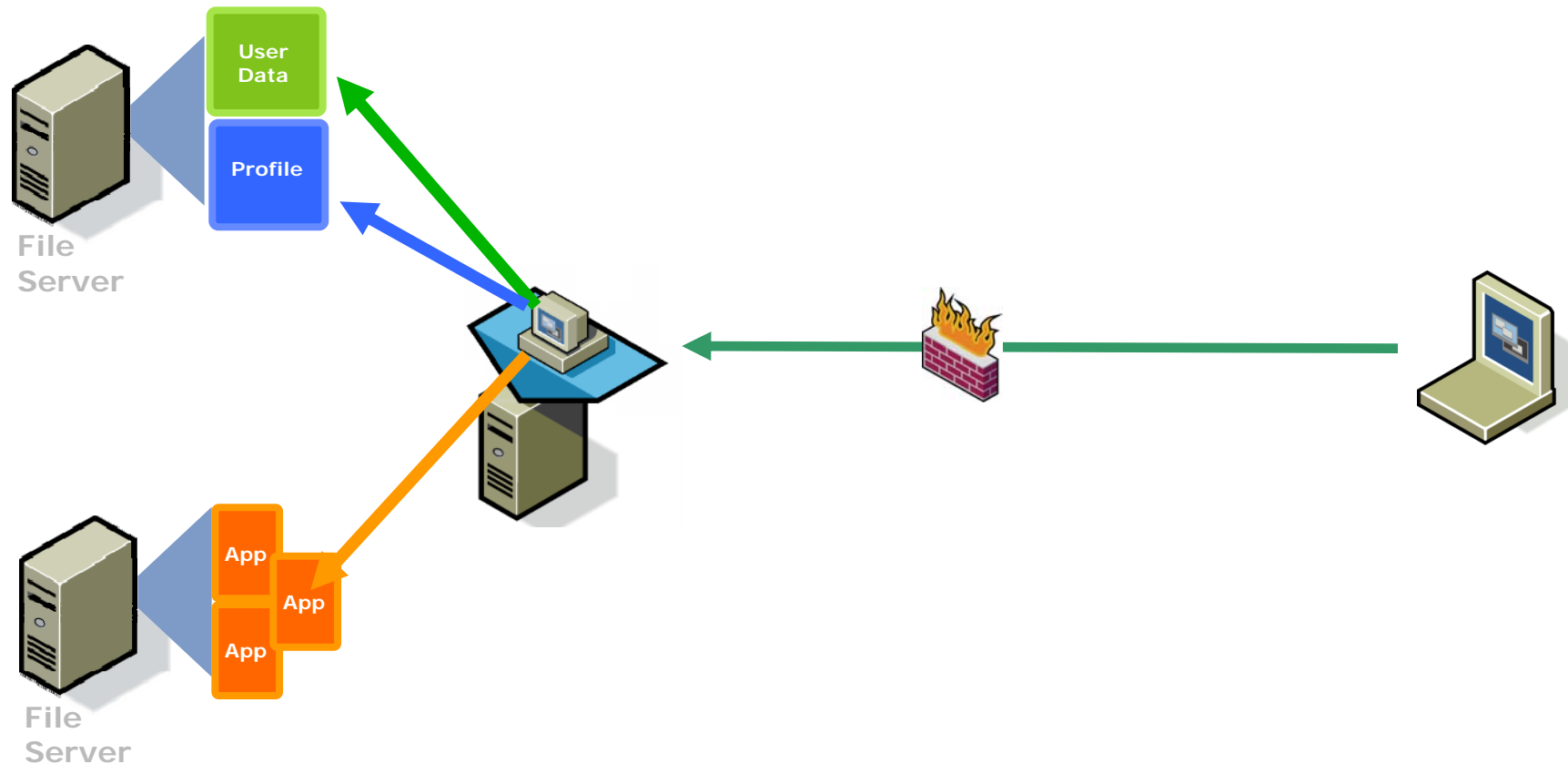
## How Virtualization Can Help

- Server Based Virtualization of Desktop Infrastructure (VDI)
- Client Side Solution – Assured Computing Environment (ACE)
- Application Virtualization



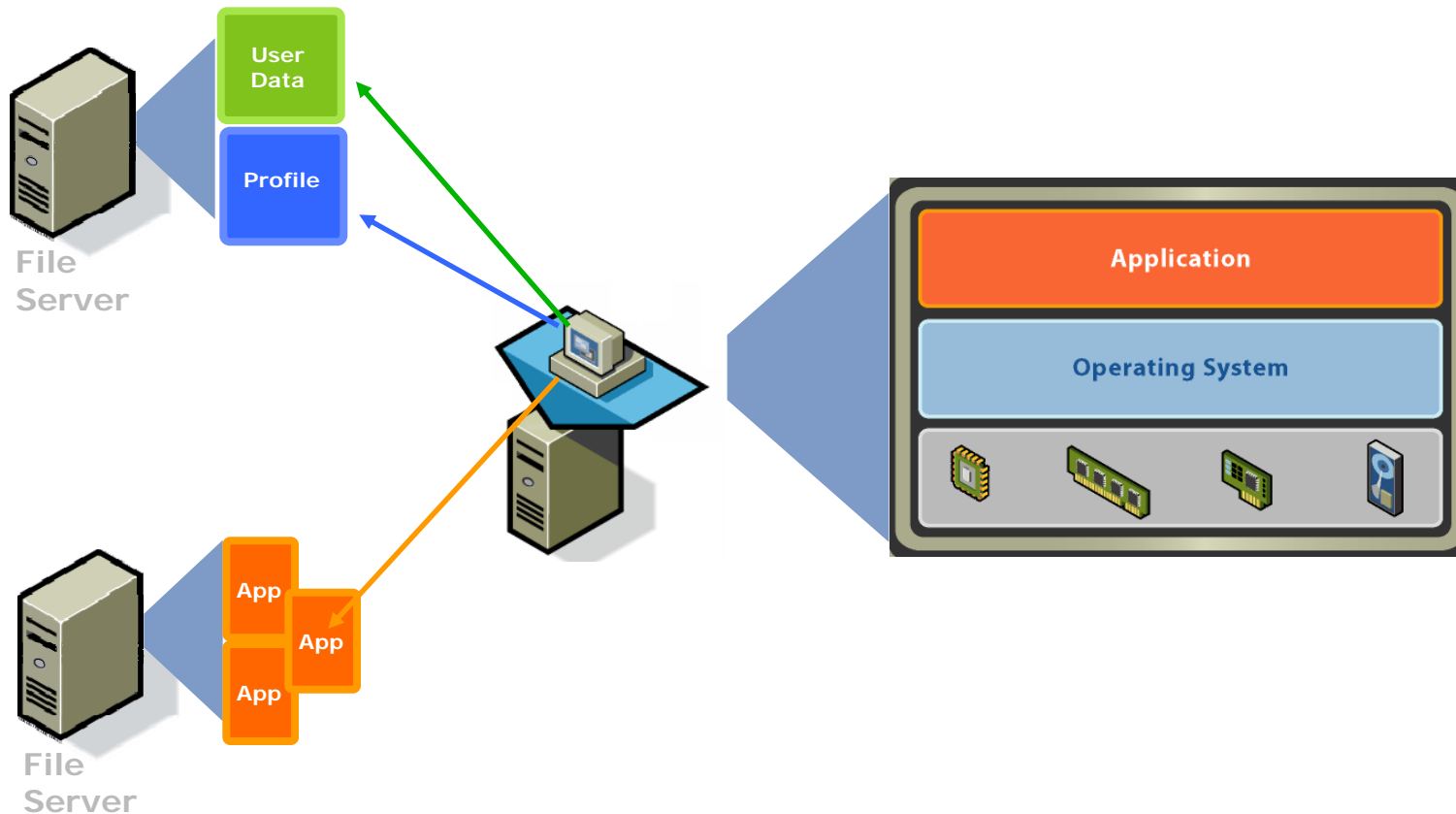
# Server-Based Virtualization of Desktops

## Server-based Desktop Virtualization



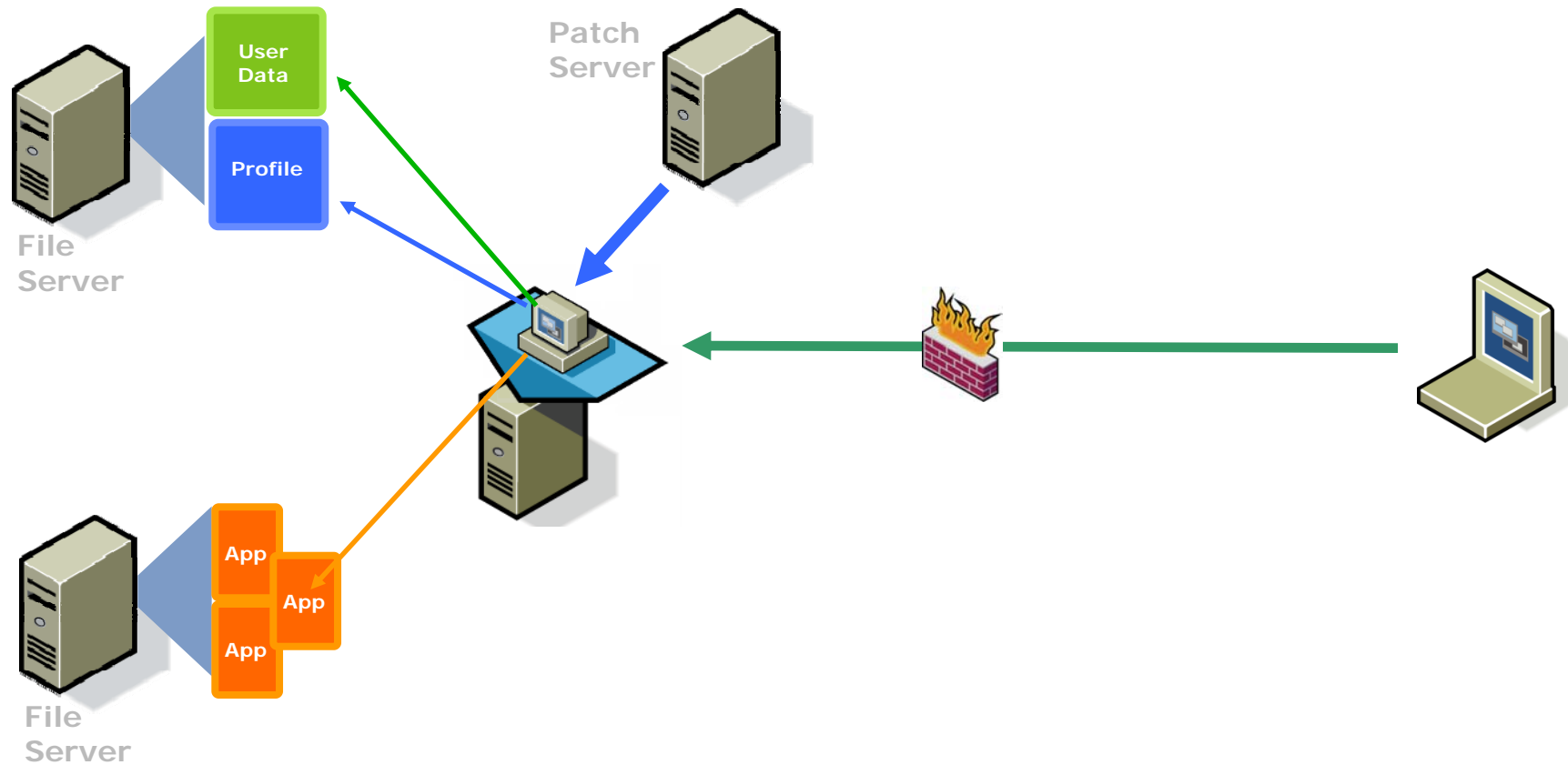
Moving the desktop to a virtualized image in the data center allows the complex components to be protected and componentized.

## Universal Operating System “Gold” Image



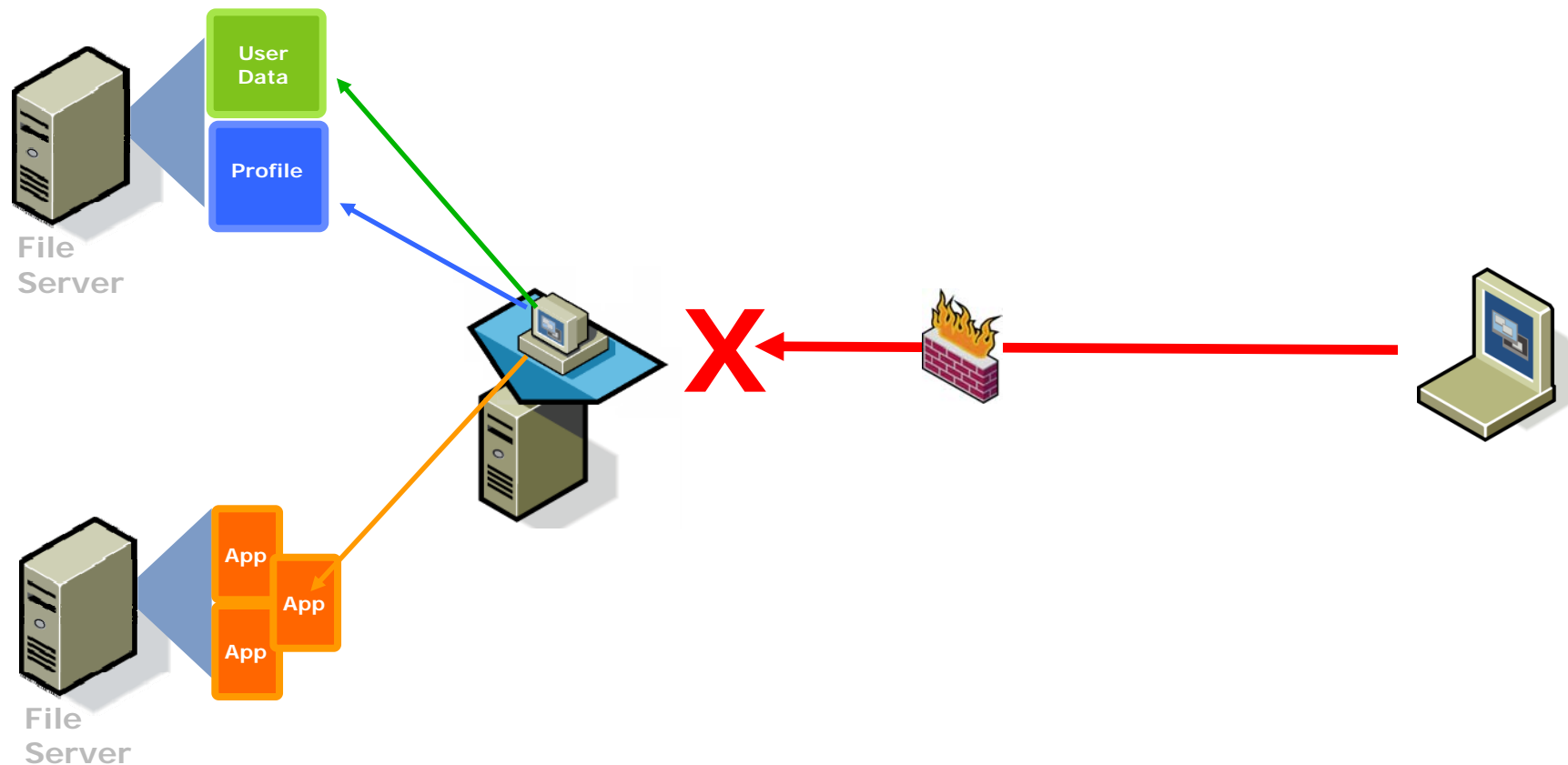
A single encapsulated hardware build for all users allows for better tuning and hardening of the underlying operating system.

## Patch Management in the Data Center



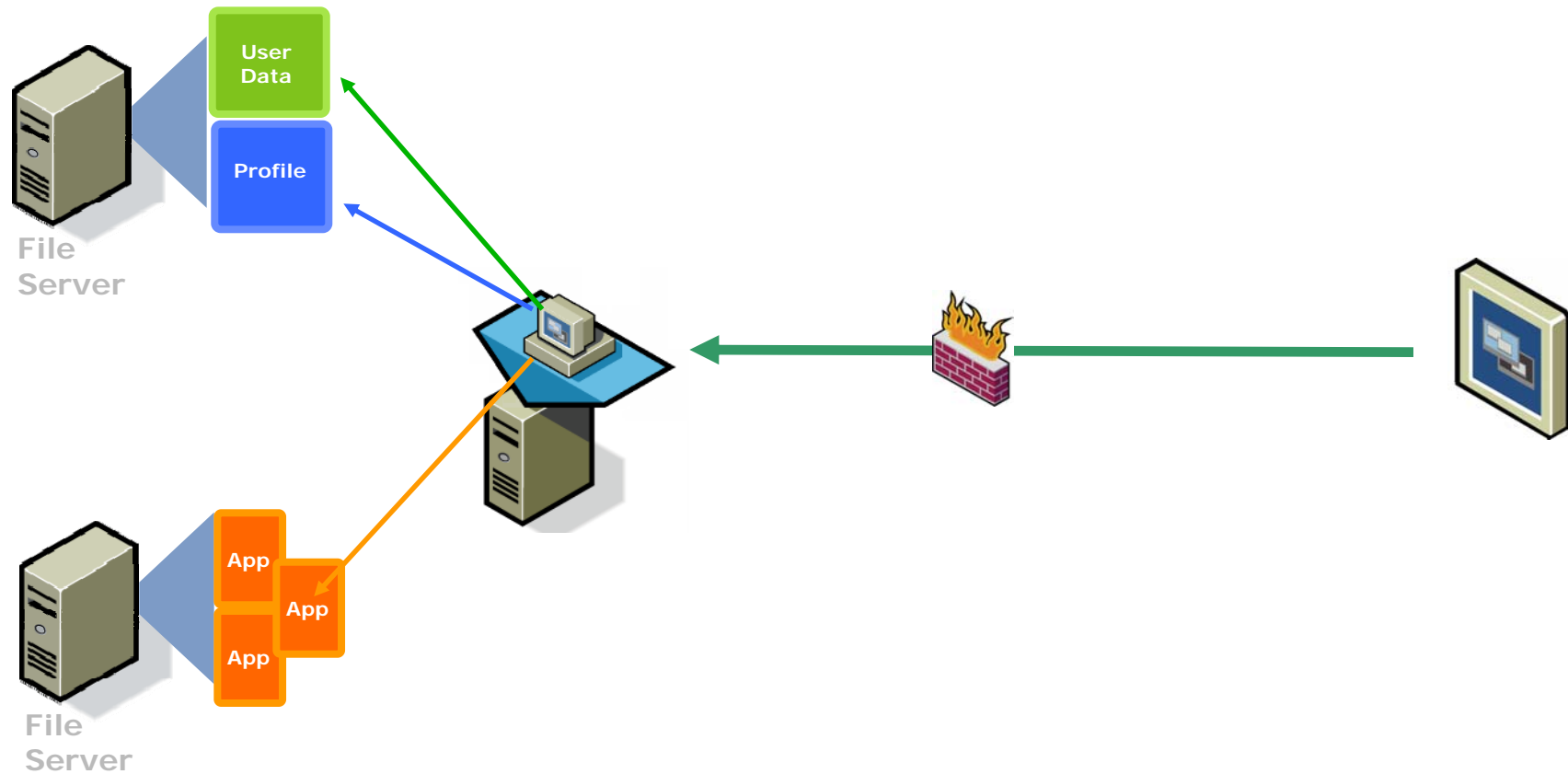
Patches can be delivered at data center network speeds, or virtual machines can be periodically destroyed and rebuilt cleanly.

## Access Control



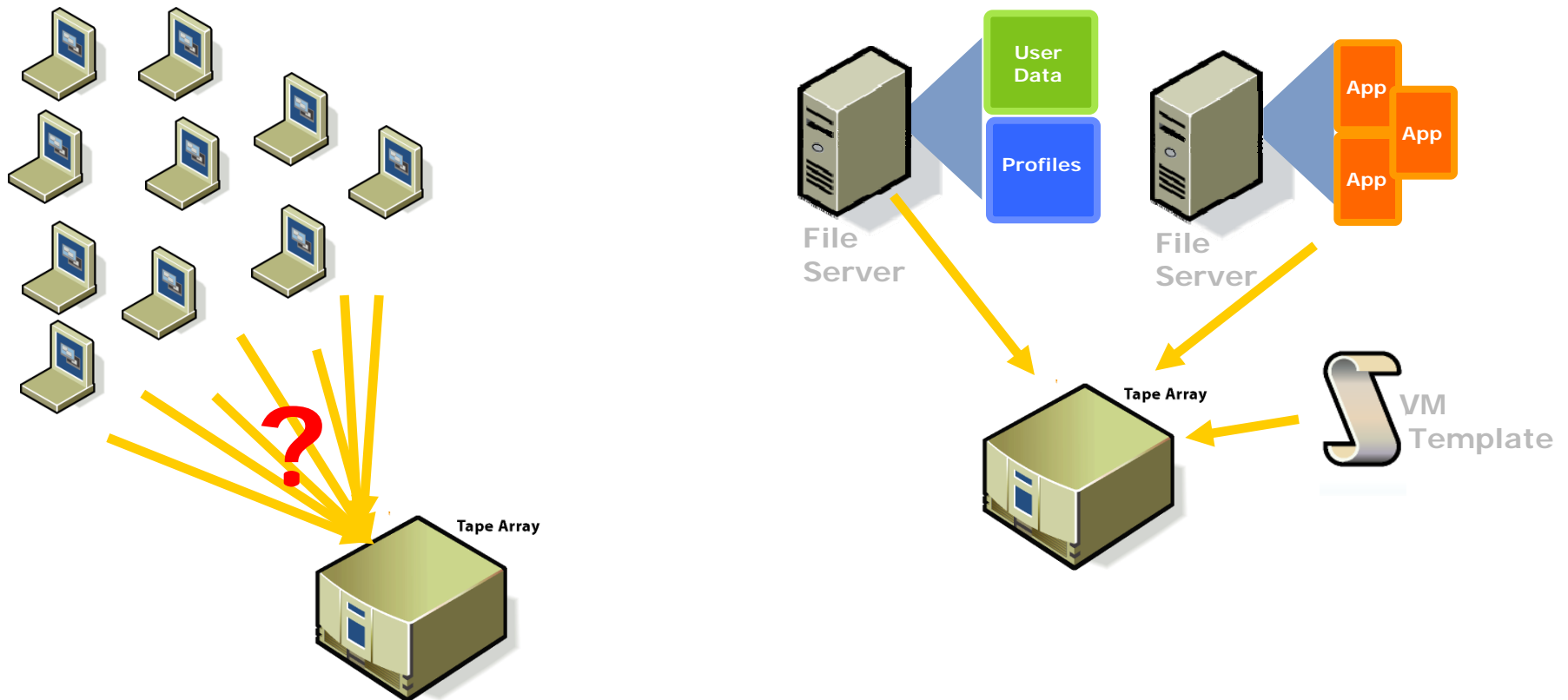
Controlling access to the virtualized desktops provides further protection to applications and user data.

## Elimination of Complex Devices at the Edge



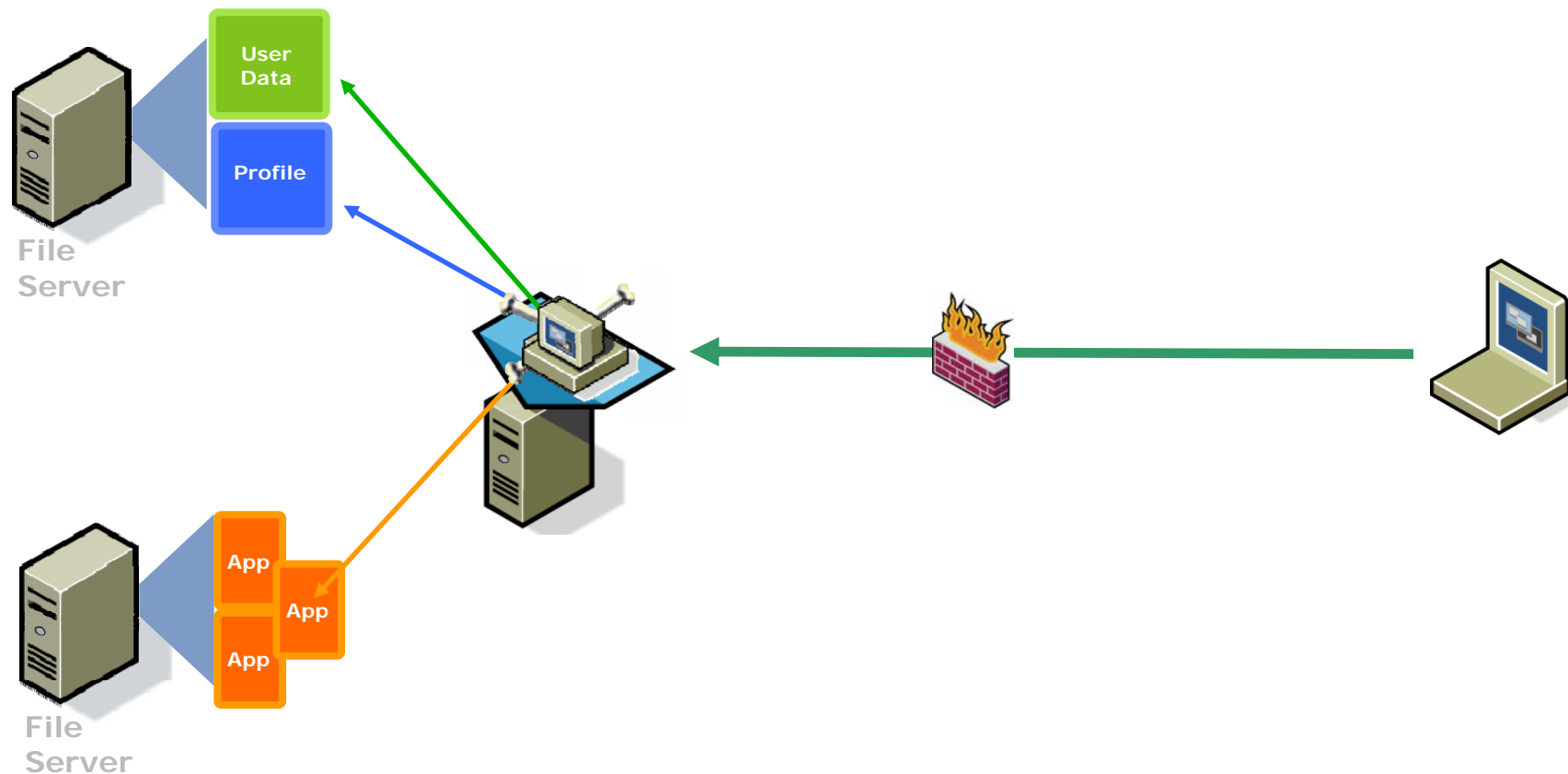
Users can be issued tamper-proof thin clients with no moving parts to complete the solution.

## Data Security - Backing Up



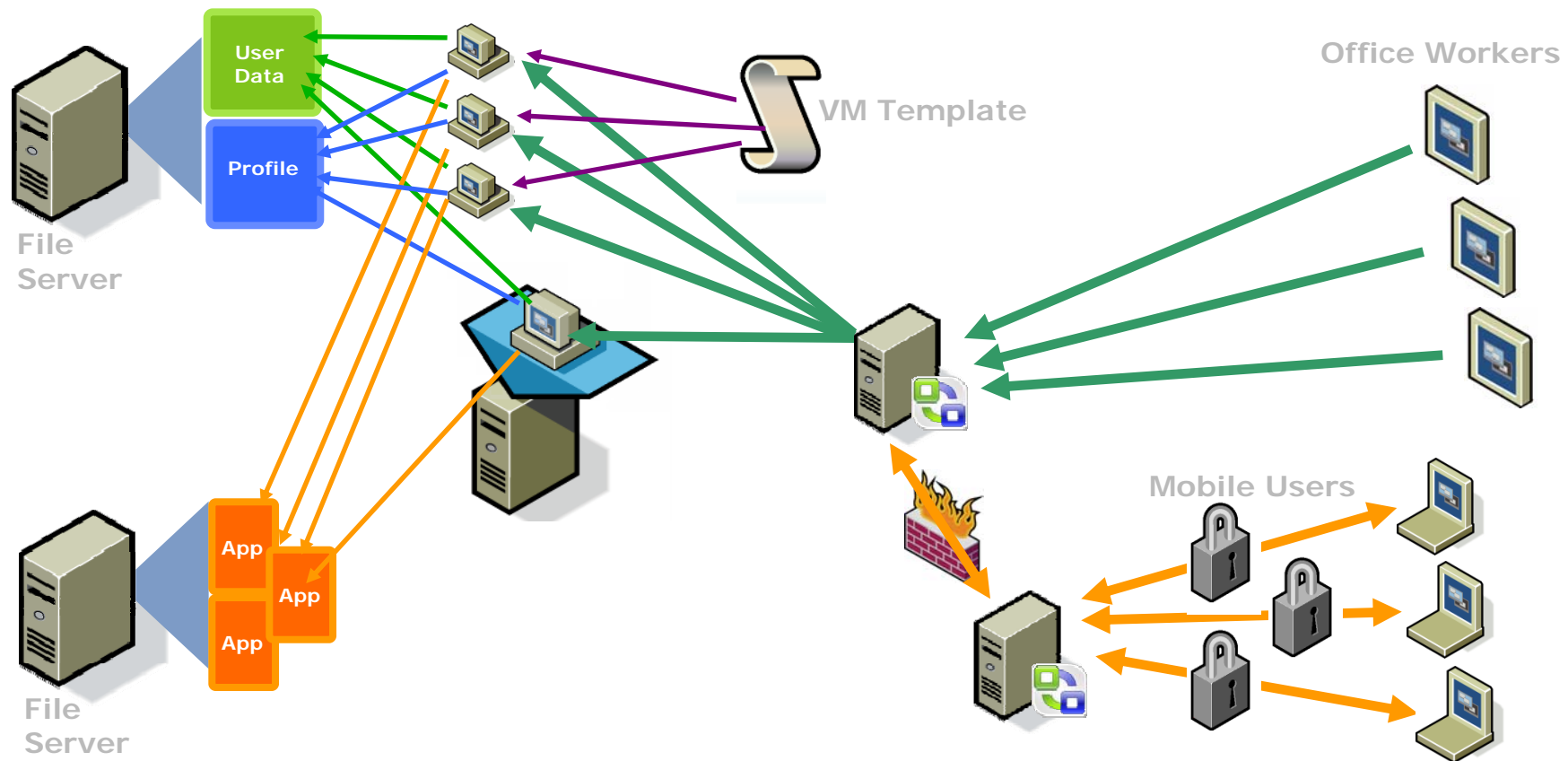
With a fully virtualized desktop, backups are not only simplified, they're actually possible.

## Easy Recovery from Infection



An infected VM can be easily restored to a clean state from a snapshot or new VM.

# Complete Server-Based Virtualization



All components are completely componentized and segmented, allowing for solid security measures at each step.



# **Secured Client-Side Virtualization of Desktops**

# Secured Client-Side Virtualization



**Link a VM to a specific device**



**Encryption of the Virtual Disk**

**Phone home or deactivate**



**Block devices to secure data**



**Control network access of the VM**



**Central Management of Security Policies**



Secure Virtual Machines can be overlaid on a insecure or unmanaged device.

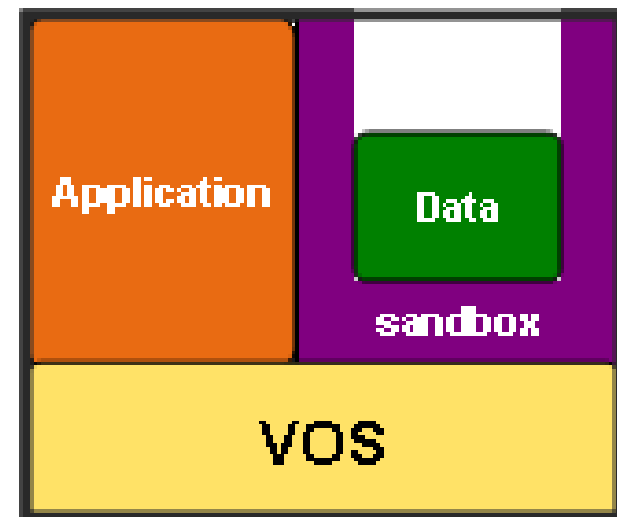
## Portable Client-Side Virtualization



The client device and it's unsecured OS become irrelevant – the VM is the true working environment.

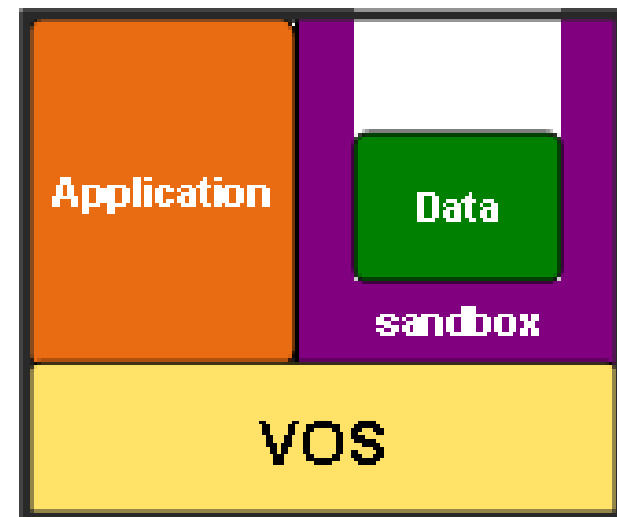
## Application Virtualization

- Applications are encapsulated in their own container
- Each application is separated from other applications and the operating system
- Application virtualization intercepts file and system calls between the application and the OS

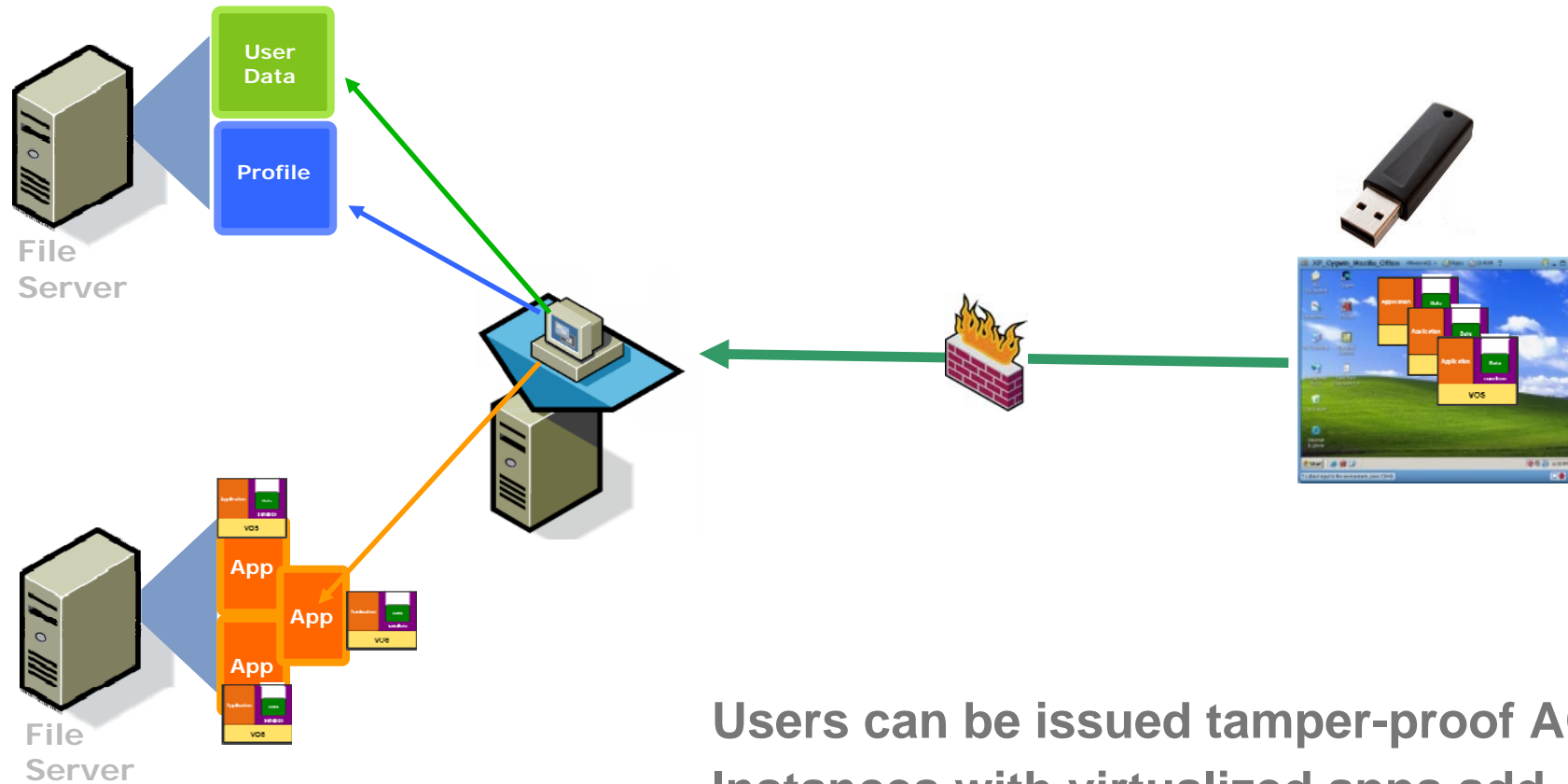


## Security Benefits of Application Virtualization

- > Single App to Patch
- > No need to “install” software on systems
- > Can be run as a usermode application with no admin rights
- > Can be run from a central location



# Integrated VDI, ACE, and App Virtualization Solution



Users can be issued tamper-proof ACE Instances with virtualized apps add network access only through VDI instance to complete the solution.

## Conclusion

- > There are many challenges associated with securing mobile environments
- > Virtualization provides multiple options to help
  - Moving the desktop to a virtualized image in the data center allows the complex components to be protected and componentized.
  - Assured Computing Environments Provide the ability for secure virtual machines to be overlaid on a insecure or unmanaged device.
  - Application Virtualization provides the ability to separate applications from the OS for better control



# Security in a Virtualized Mobile Environment

**Q&A**