The Dark Side of Virtualisation or 10 Reasons Not to Virtualise

Rik Ferguson
Director Security Research & Communication EMEA

Session ID: STAR-208

Session Classification: Intermediate

RSA CONFERENCE EUROPE 2012

Virtualisation Is A Good Thing™

Enabled server consolidation

Created more flexible environments

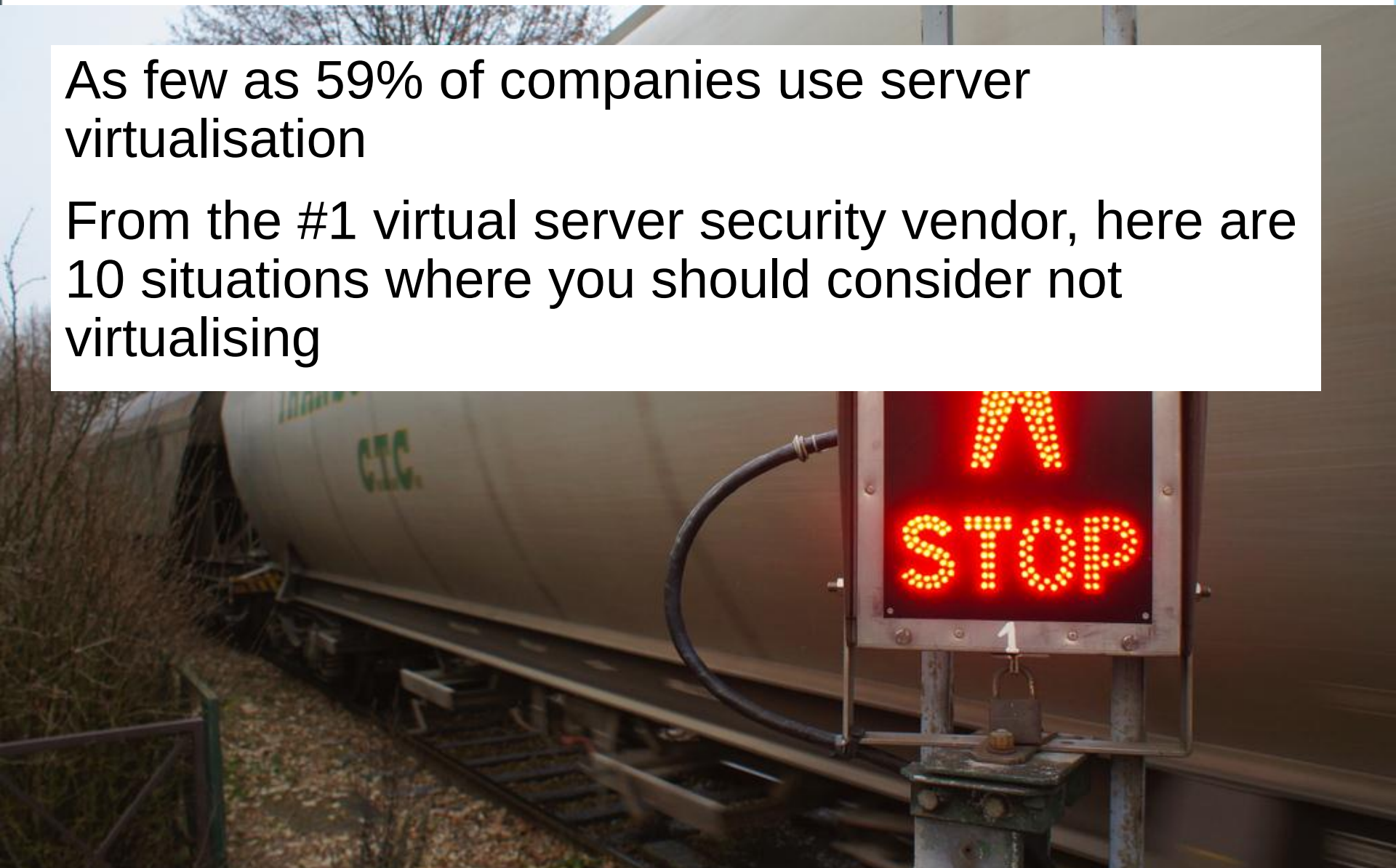
Saved companies a ton of money

Way less annoying than Jar Jar Binks

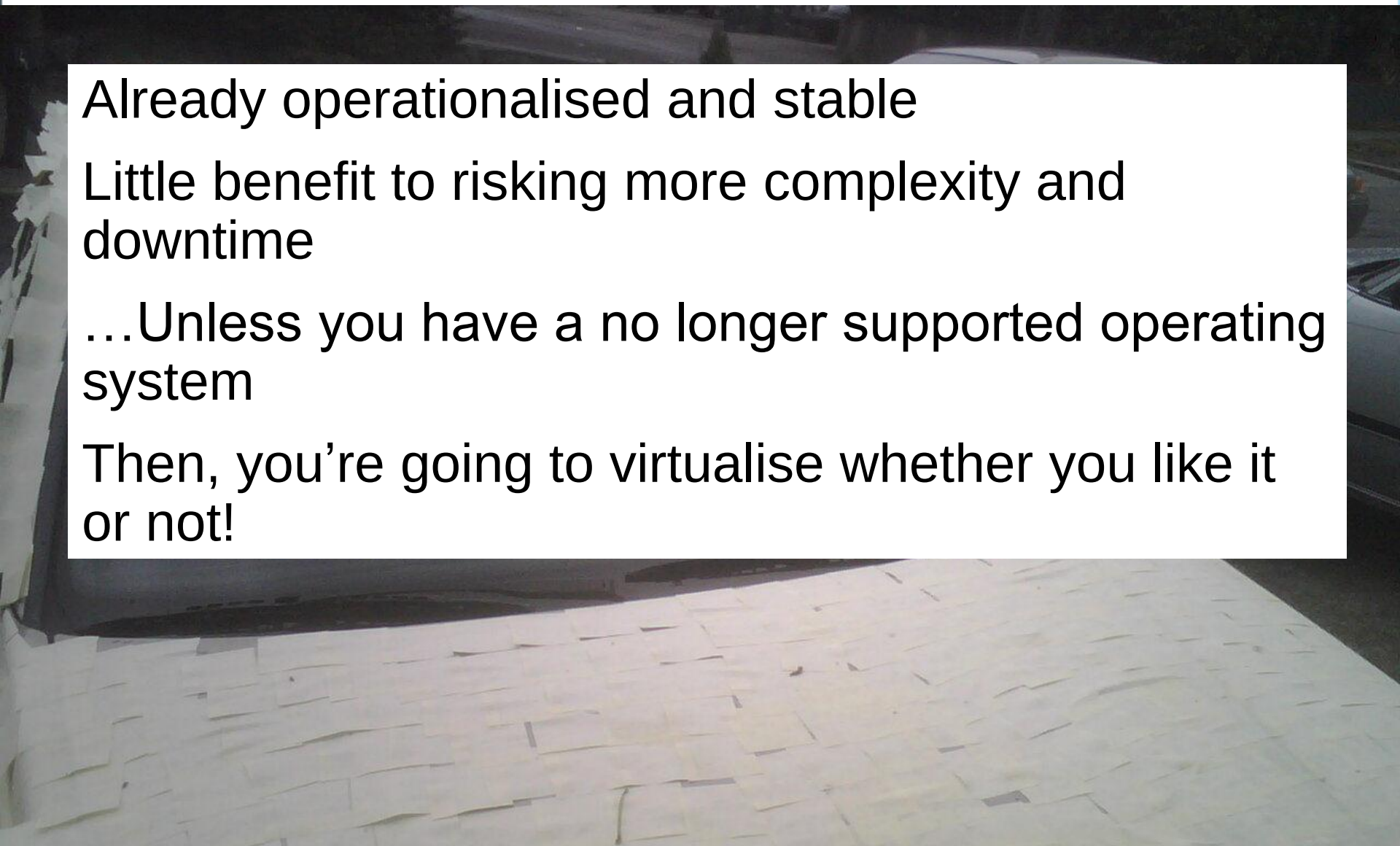
But…

As few as 59% of companies use server virtualisation

From the #1 virtual server security vendor, here are 10 situations where you should consider not virtualising



Static, Predictable Computing



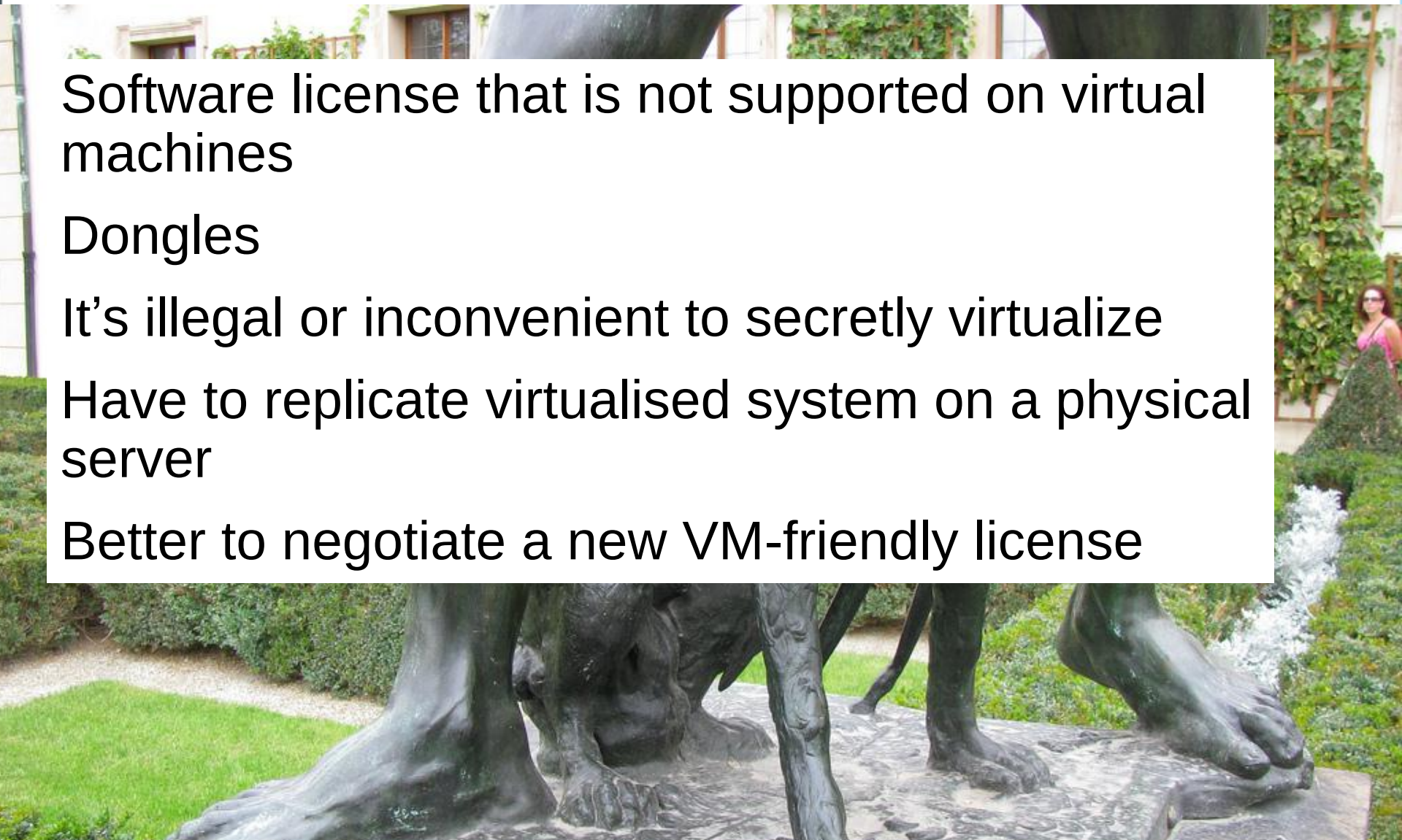
Already operationalised and stable

Little benefit to risking more complexity and downtime

…Unless you have a no longer supported operating system

Then, you're going to virtualise whether you like it or not!

Virtualization Unfriendly Licensing



- Software license that is not supported on virtual machines
- Dongles
- It’s illegal or inconvenient to secretly virtualize
- Have to replicate virtualised system on a physical server
- Better to negotiate a new VM-friendly license

It Just Won't Work Well

High I/O apps like databases or other things that require tuning to work with underlying hardware

Disk intensive workloads (use a pass-through not virtual HD)

Grid or distributed SMP that needs high speed interconnection

Hardware cards without virtualisation drivers (dongles too)

Graphics-intensive apps (especially high end video cards)

VM vendors are getting better are supporting special cases

Time Drift

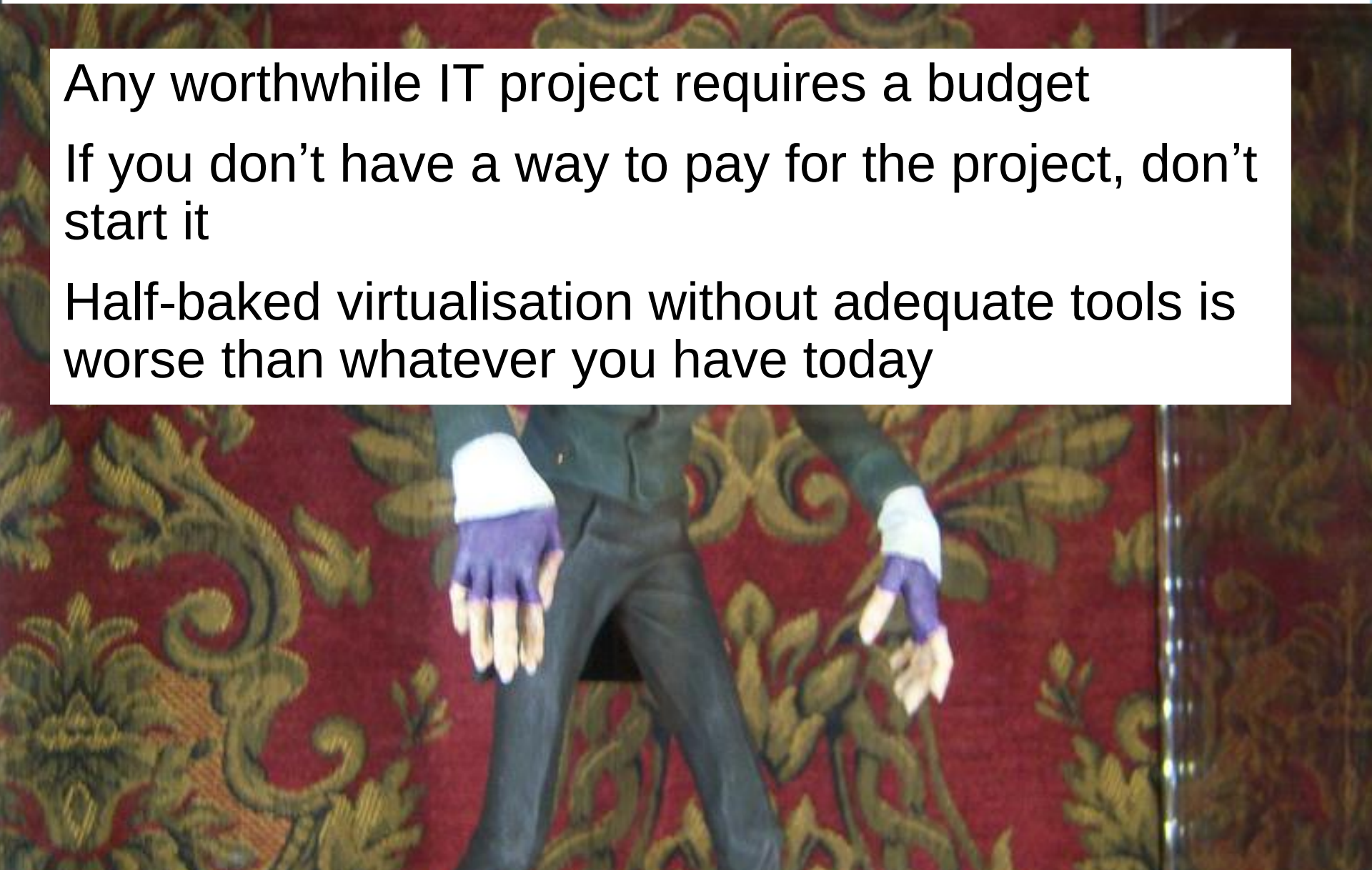
VMs store time apart from physical host

VM clock diverges from physical clock over time

If very small amounts will hurt apps, don't virtualise

Financial real-time trading, some industrial control systems

You Work for a Cheapskate

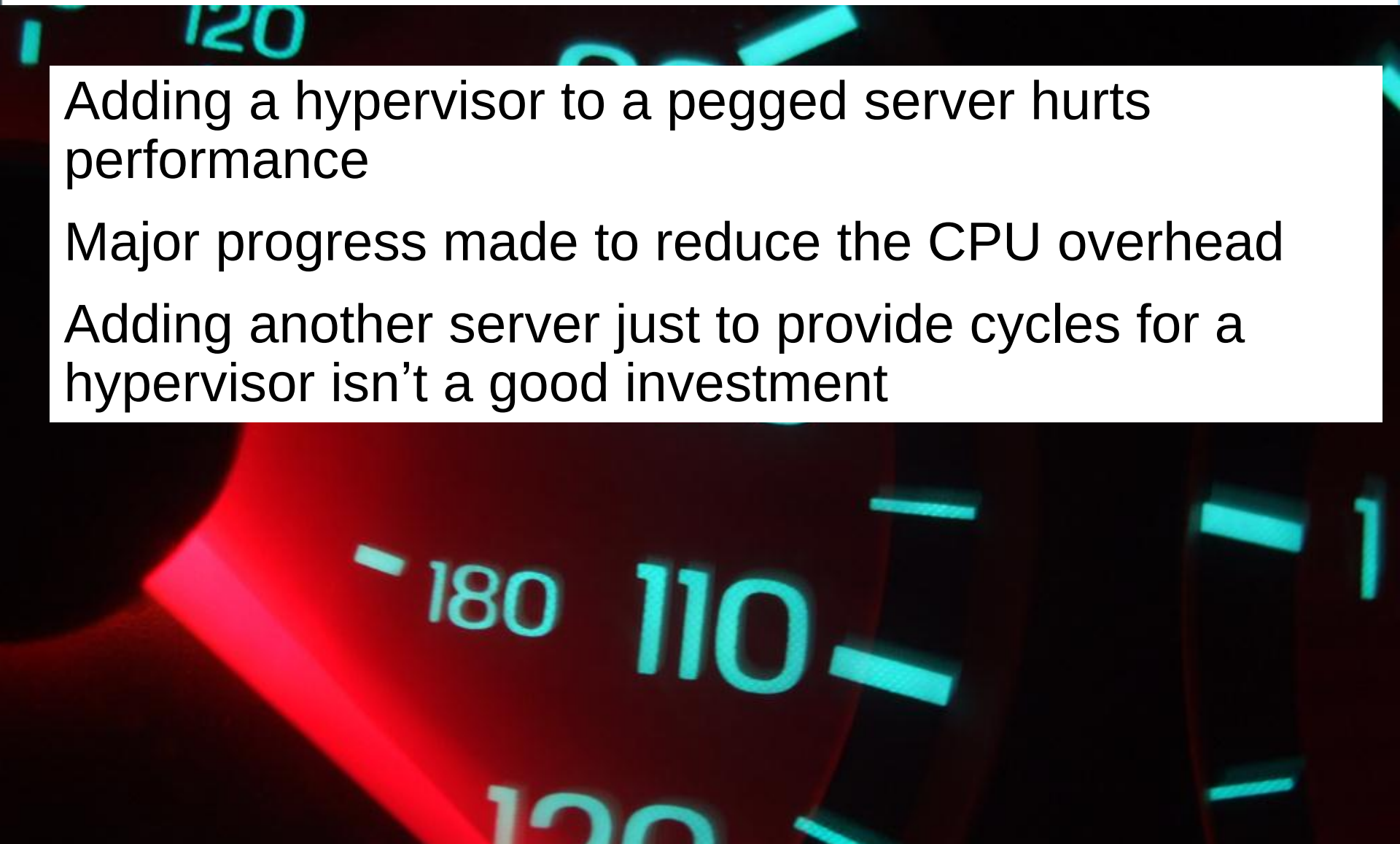


Any worthwhile IT project requires a budget

If you don’t have a way to pay for the project, don’t start it

Half-baked virtualisation without adequate tools is worse than whatever you have today

Running Servers at High Capacity



Adding a hypervisor to a pegged server hurts performance

Major progress made to reduce the CPU overhead

Adding another server just to provide cycles for a hypervisor isn't a good investment

No safe way to manage encryption keys

Key management is easy on physical servers

Virtual secure workloads move around

Encryption key management for physical servers won’t work

Not secure to store passwords or certificates on individual VMs

Policy based encryption key management required

App clustering for failover

Virtualisation platforms offer high availability for VMs

Older mission critical apps have HA already

Example:

- Microsoft Cluster Services with a shared disk will break in private clouds that allow VMs to automatically move around

If the VM platform provides HA, your apps shouldn't

Vice versa

To save money on VDI

Servers cost more than cheap desktops

You still have to buy a PC or tablet or thin client – and manage and secure it too

Virtual desktops are great for security and compliance, but they are not a lower cost option for all types of employees

They *are* more efficient for some types of employees (call center, line workers, etc.)

Virtualization platform components

Situation:

- Virtualisation platform and hypervisors rely on Active Directory or DNS servers
- AD or DNS is virtualised
- Hypervisor won’t start because it’s waiting for AD
- AD won’t start because it’s waiting for VM
- Pain

Can your virtualisation management software (vCenter, etc.) run on servers it manages?

The complete list

When you have static, predictable computing needs

When you can’t get a virtualisation friendly license

When it just won’t work very well

When time drift will hurt your apps

When you work for a cheapskate

When you’re already running servers at high capacity

When you don’t have a way to manage encryption keys

When you use clustered apps with built in failover

When you want to save money on all desktops by virtualising them

When you are running virtualisation platform components

How can you apply this knowledge?

- Identify the reasons you are virtualising
- Identify those systems that are appropriate and more importantly those that are not
- Build an integrated management platform
- Apply consistent *integrated* security across physical, virtual and cloud environments

That said...