A sane approach to virtualization security

Manu Namboodiri, Vice President of Marketing

BITARMOR

Virtualization and its promise

- **Virtualization**
  - Devices, networks, applications are being virtualized
  - Huge benefits in flexibility, cost savings
  - A paradigm shift in infrastructure management
- **But, the major benefits are yet to be realized**
  - Cost savings, scalability, automation
  - Self provisioning, higher user productivity
  - Business flexibility
  - Others we have not dreamed of yet
  - A paradigm shift in *business*

BITARMOR

Virtualization security

Is virtualization so fundamentally different that it requires a different approach to security?

Yes, we do.

Approaches to virtualization security
(the more things change, the more they remain the same)

Security

- Network-based and host-based firewalls, intrusion detection/prevention systems
- Host-based anti-malware prevention
- Device and disk encryption
- Vulnerability and configuration management and remediation
- Network access control
- Network and storage encryption solutions
- Network behavior analysis and monitoring
- Etc, etc, etc

Virtualization Security

- Virtual Network and virtual host-based firewalls, intrusion detection/prevention systems
- Virtual Host-based anti-malware prevention (for example, antivirus for the host or hypervisor)
- Virtual device/disk encryption
- Vulnerability ,configuration management and remediation for virtual environments
- Virtual Network and VM access control
- Virtual network and storage encryption solutions
- Virtual network behavior analysis and monitoring
- Virtual Machine isolation and segmentation
- Hypervisor security, prevent escape from the hypervisor
- Etc, etc, etc

BITARMOR

The problem with legacy
(this is how we have always done it)

- **Standard US railroad gauge – 4 feet 8.5 inches**
  - That's the way it was built in England!
- **Railroad based on standard tramway gauge**
  - Same tools and same people built both
- **Based on standard spacing for wagons**
  - Had to match existing rut spacing on the roads
- **First roads (and ruts) were built by Imperial Rome**
  - Ruts were from Roman war chariots

The United States railroads are of 4'8.5" gauge because of the width of the wagon wheels of Imperial Roman war chariots!

BITARMOR

The problem with legacy
(this is how we have always done it)

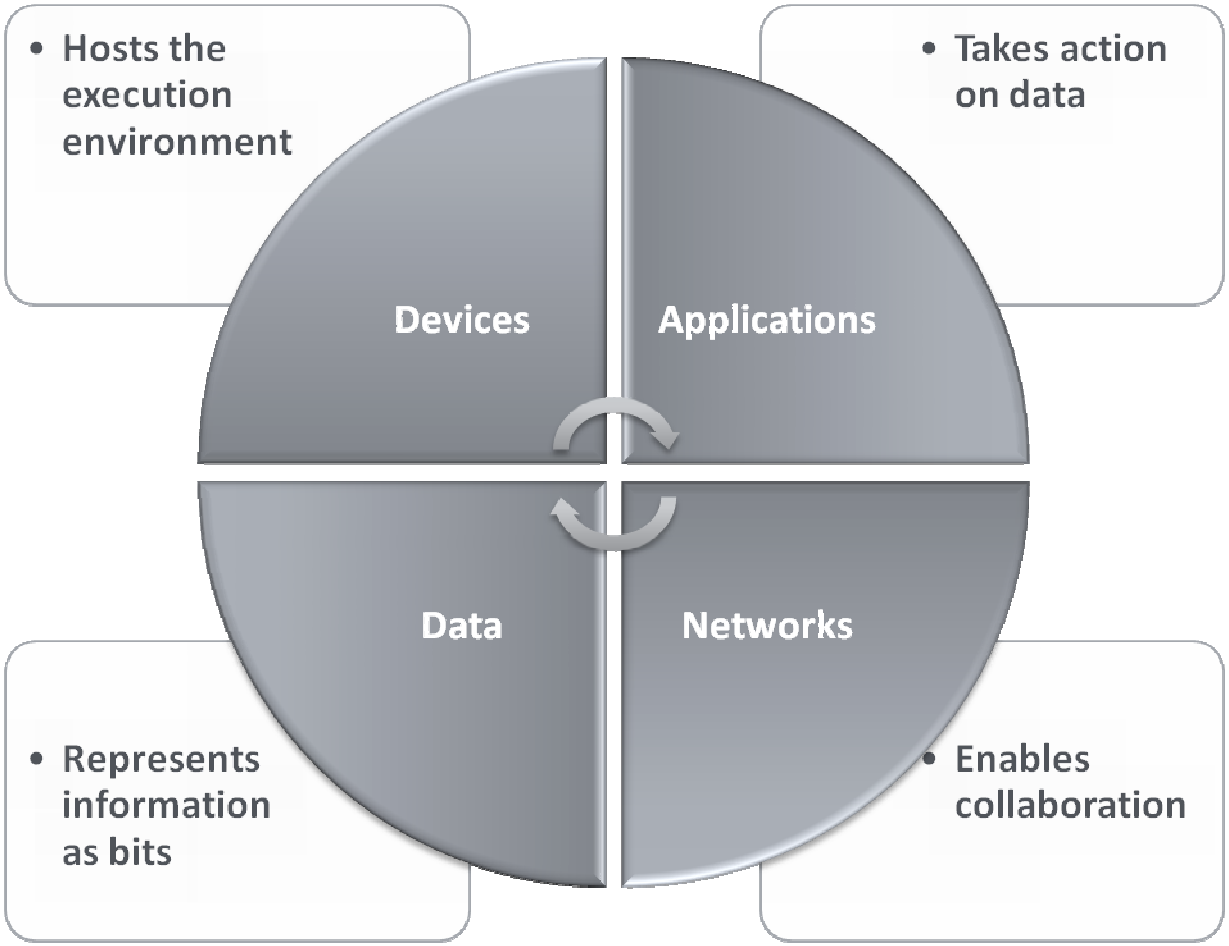
BITARMOR

Why we need to do things differently

1. The increased criticality of data in virtual environments
2. The inevitable co-existence of virtual and non-virtual environments

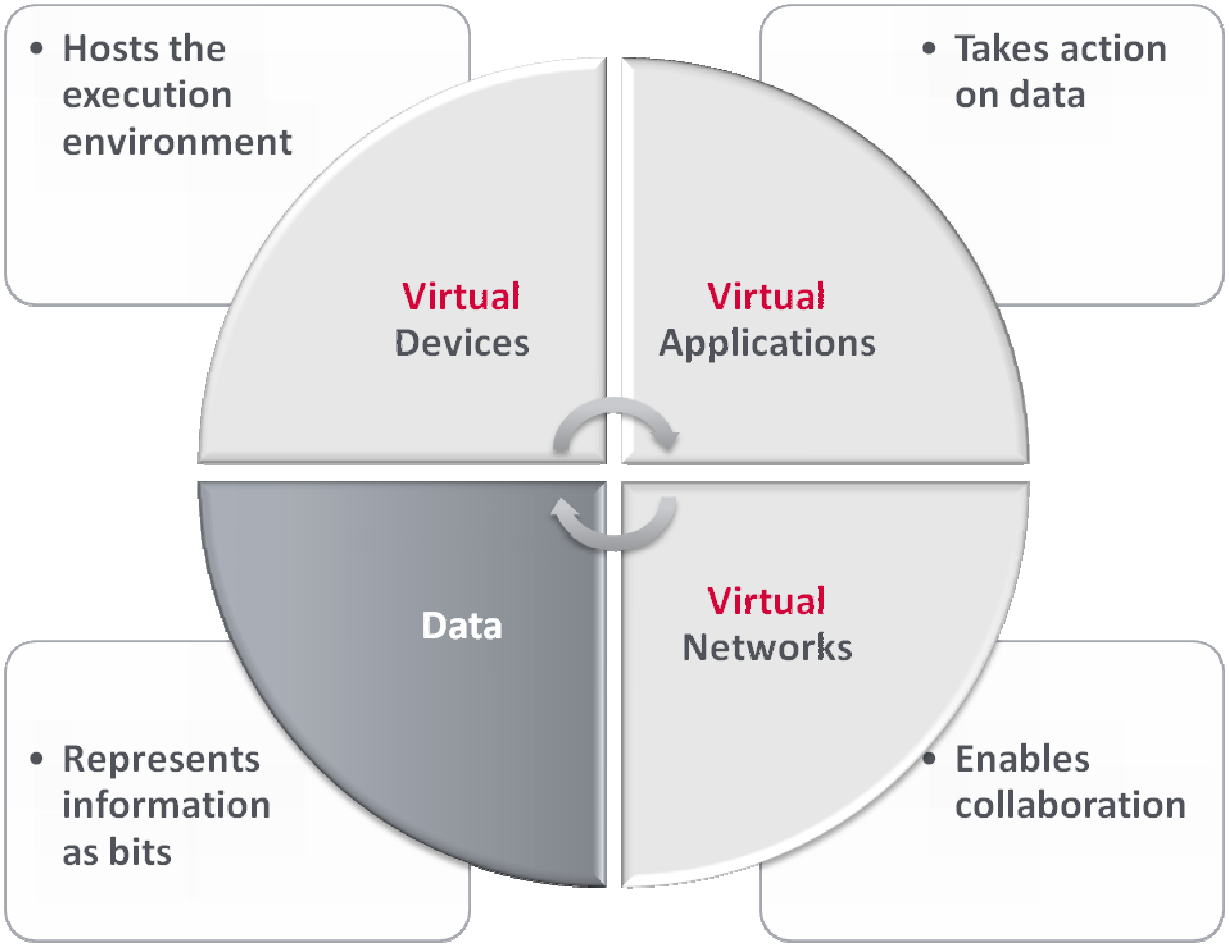
BITARMOR

Back to basics – the computing environment

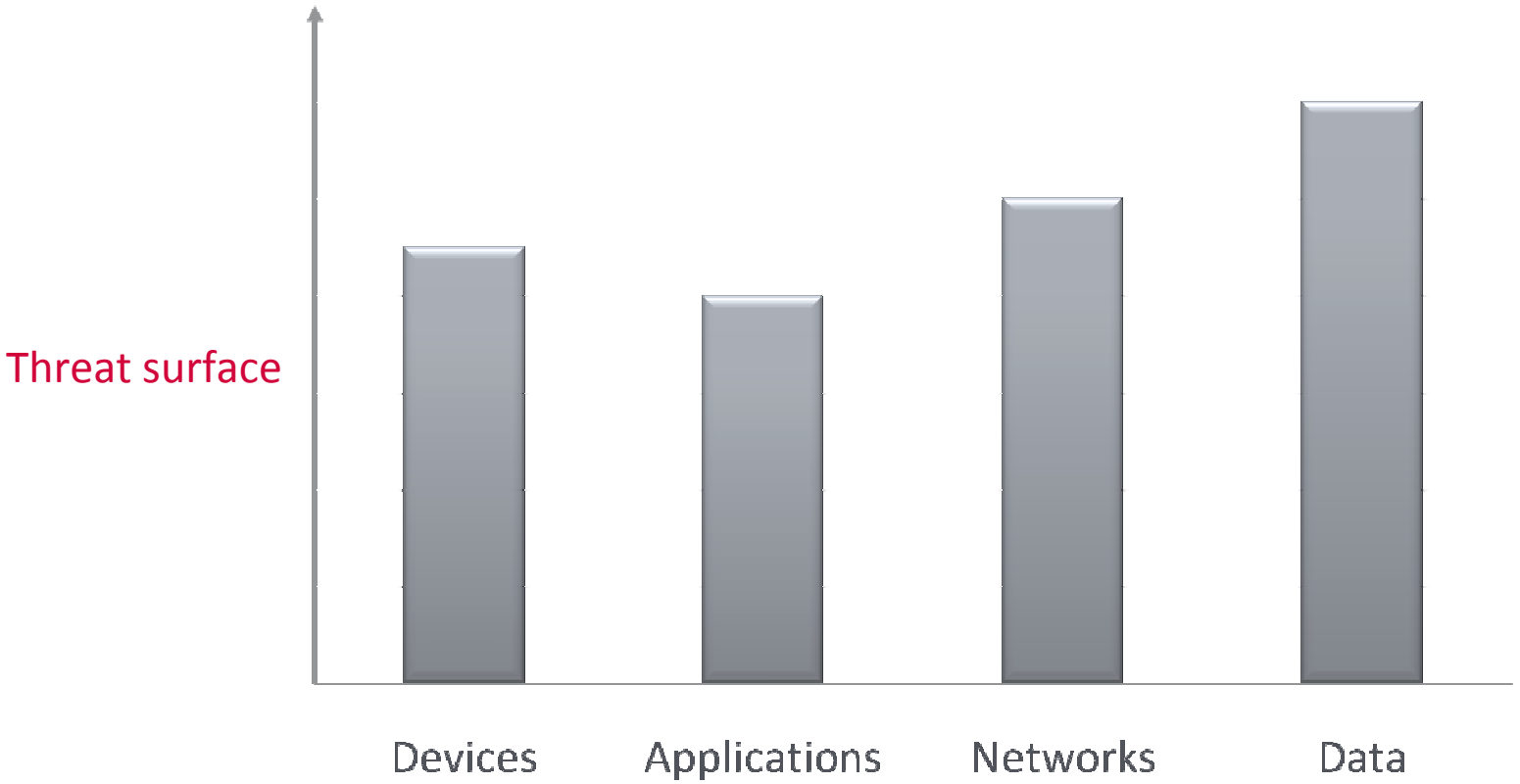


BITARMOR

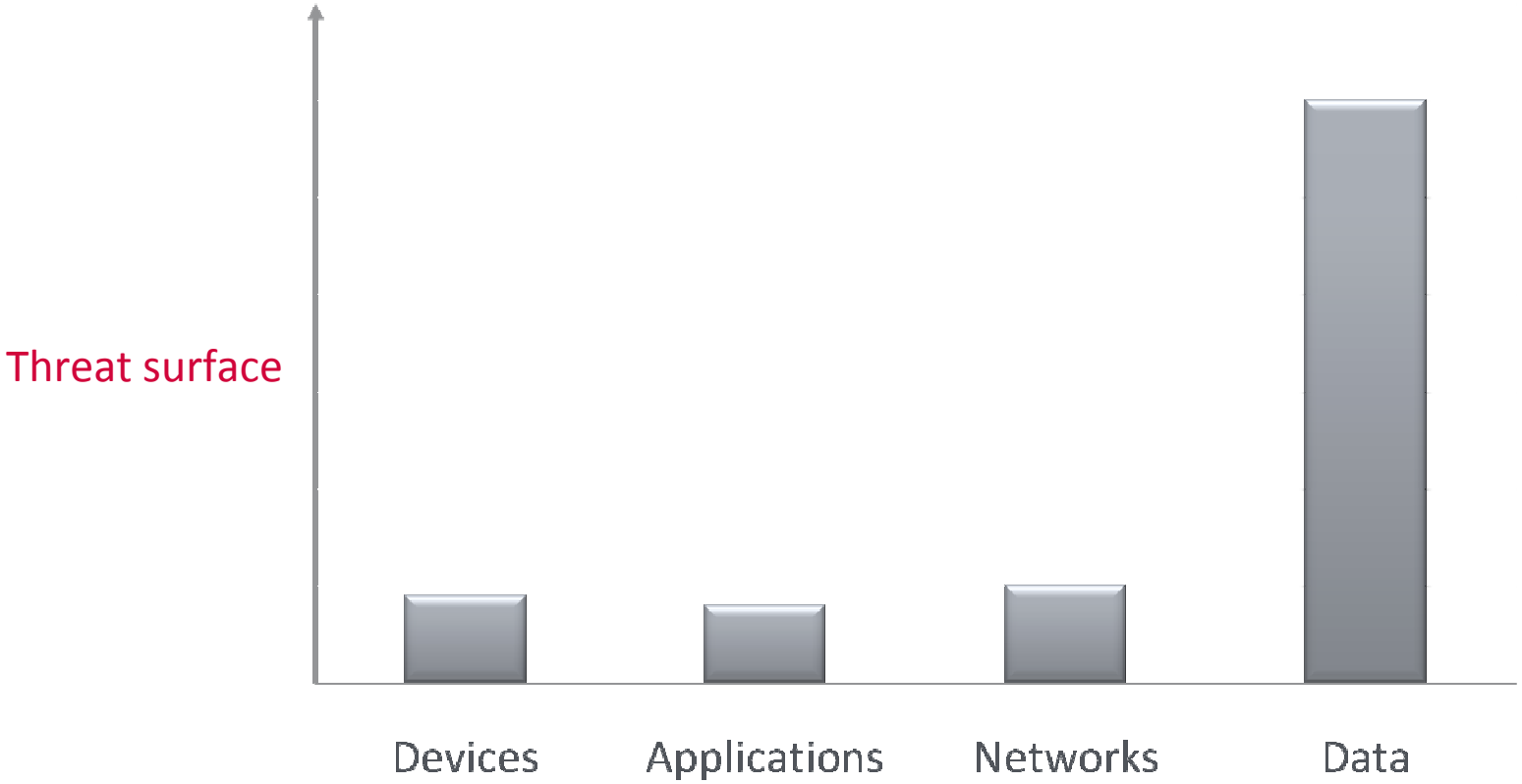
Virtualization – the computing environment



Threat surface of computing elements

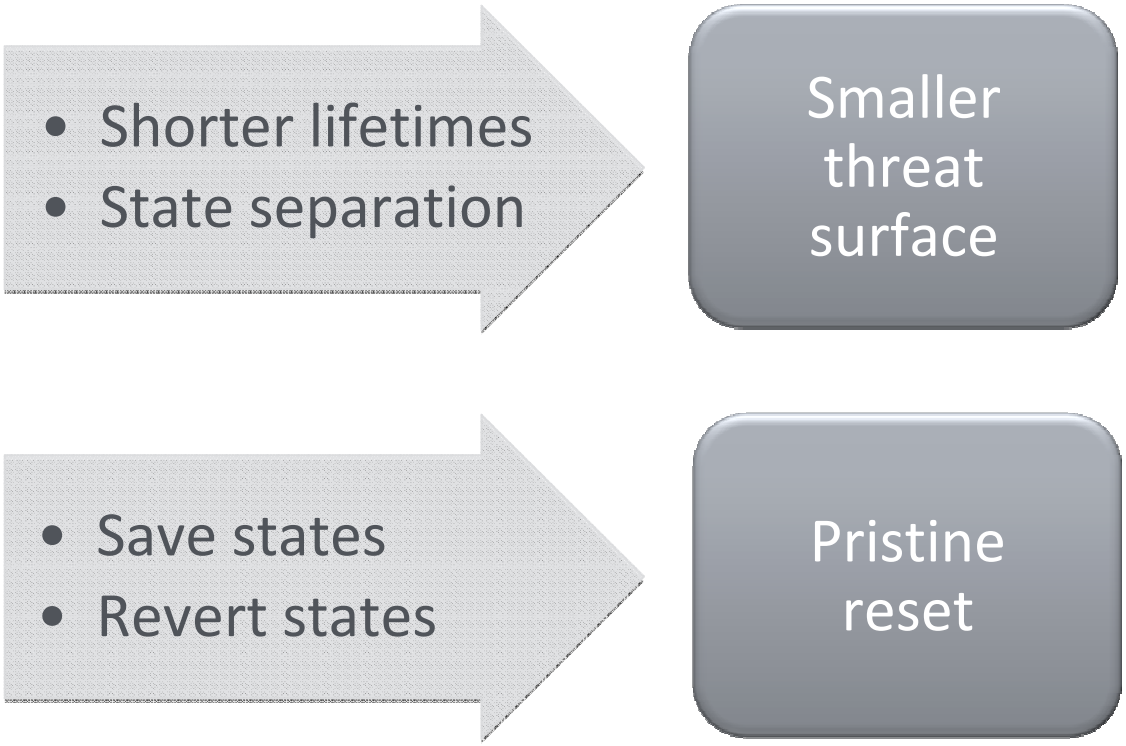


Threat surface of virtual computing elements

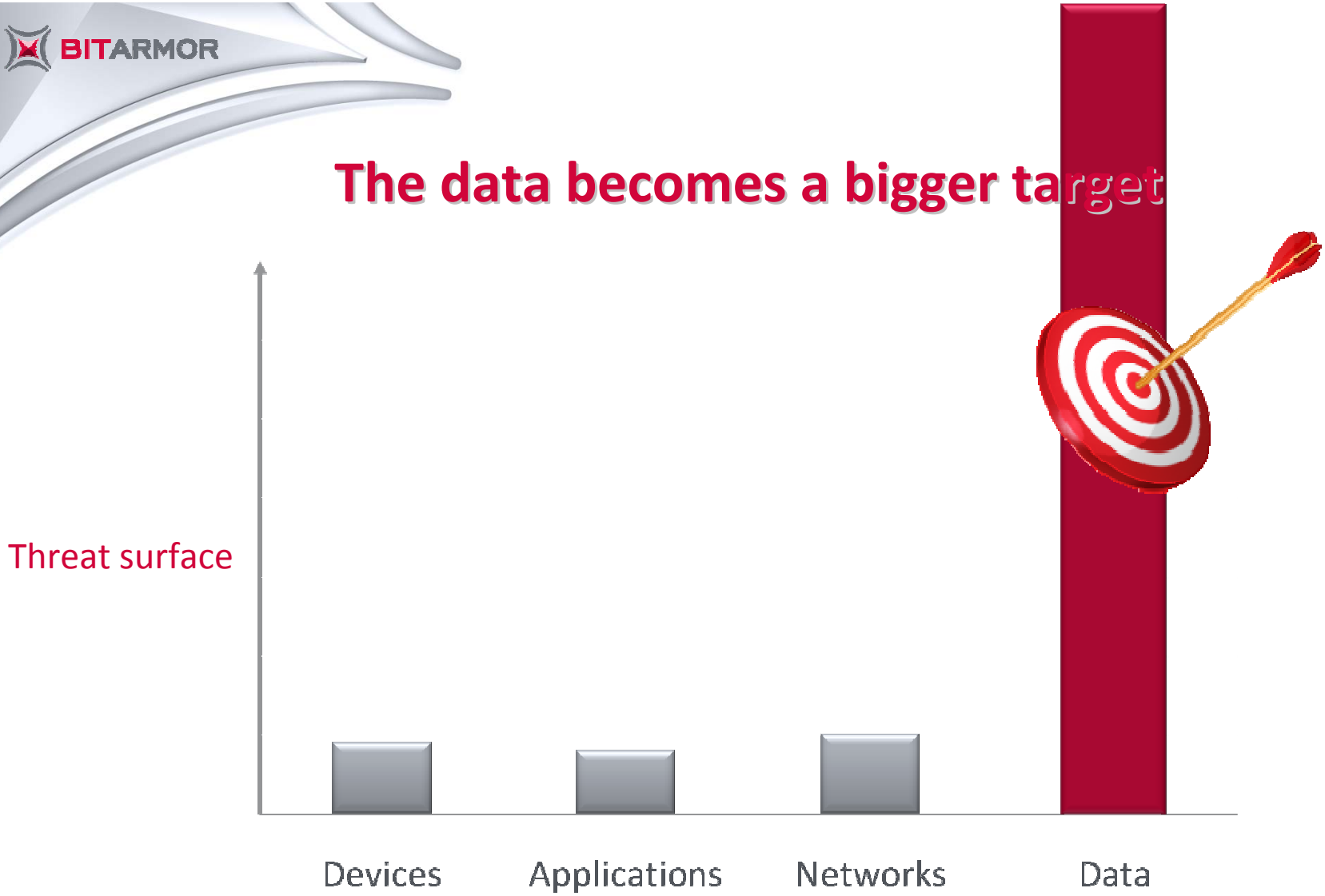


BITARMOR

Impact to infrastructure security



The data becomes a bigger target



Approaches to virtualization security
(the more things change, the more they remain the same)

Security

- Network-based and host-based firewalls, intrusion detection/prevention systems
- Host-based anti-malware prevention
- Device and disk encryption
- Vulnerability and configuration management and remediation
- Network access control
- Network and storage encryption solutions
- Network behavior analysis and monitoring
- Etc, etc, etc

Virtualization Security

- **Virtual** Network-based and host-based firewalls, intrusion detection/prevention systems
- **Virtual** Host-based a… alware prevention (for example, antivirus… st or hypervisor)
- **Virtual** device …
- Vulnerabil… agement and rem…
- **Virtual** Netv… ntrol
- **Virtual** network … ncryption solutions
- **Virtual** network behavior analysis and monitoring
- **Virtual** Machine isolation and segmentation
- **Hypervisor** security, prevent escape from the hypervisor
- Etc, etc, etc

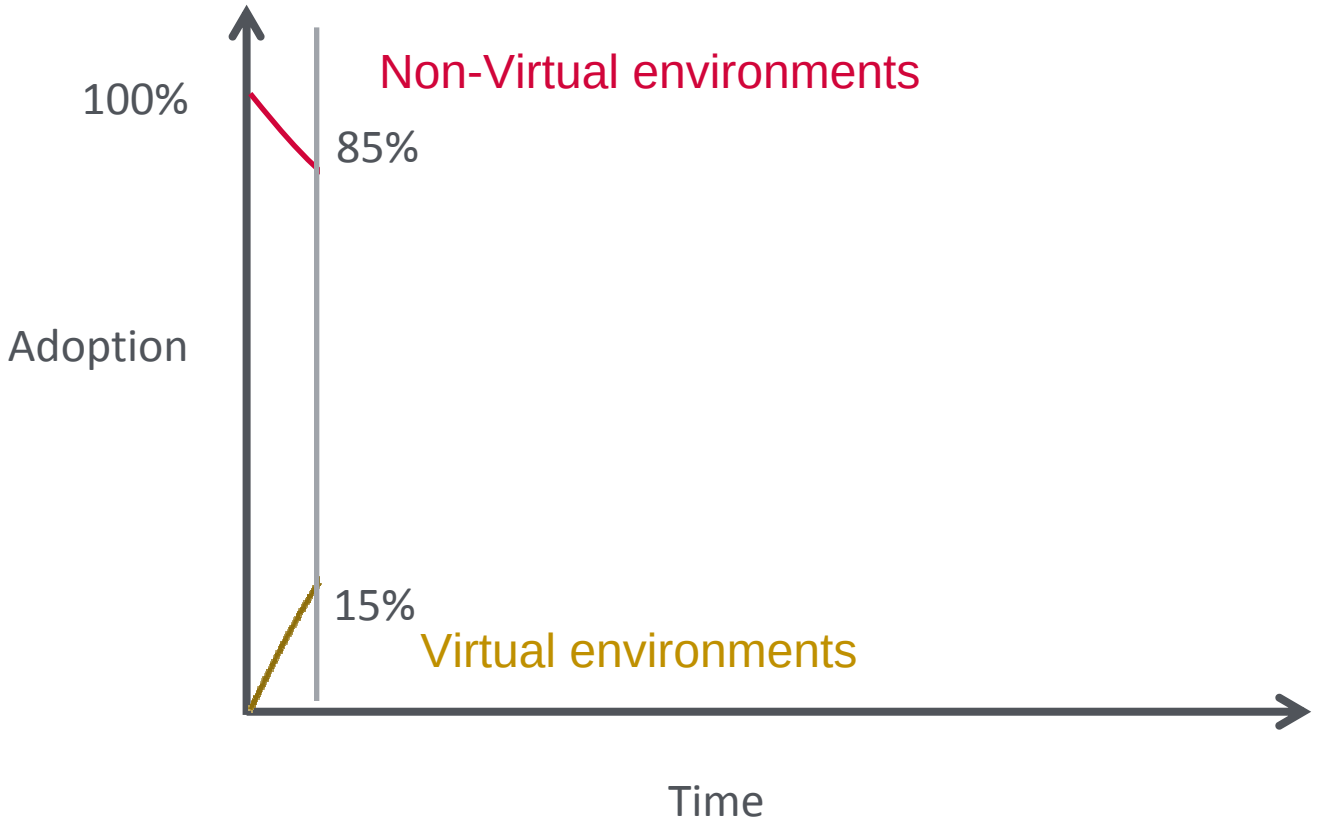
BITARMOR

Are we focusing on what is important?

Why are we spending inordinate resources to protect the ephemeral virtual infrastructure while we pay little heed to protecting the long-lived data itself?

Growth of virtualization

The co-existence and duplication dilemma



Approaches to virtualization security
(the more things change, the more they remain the same)

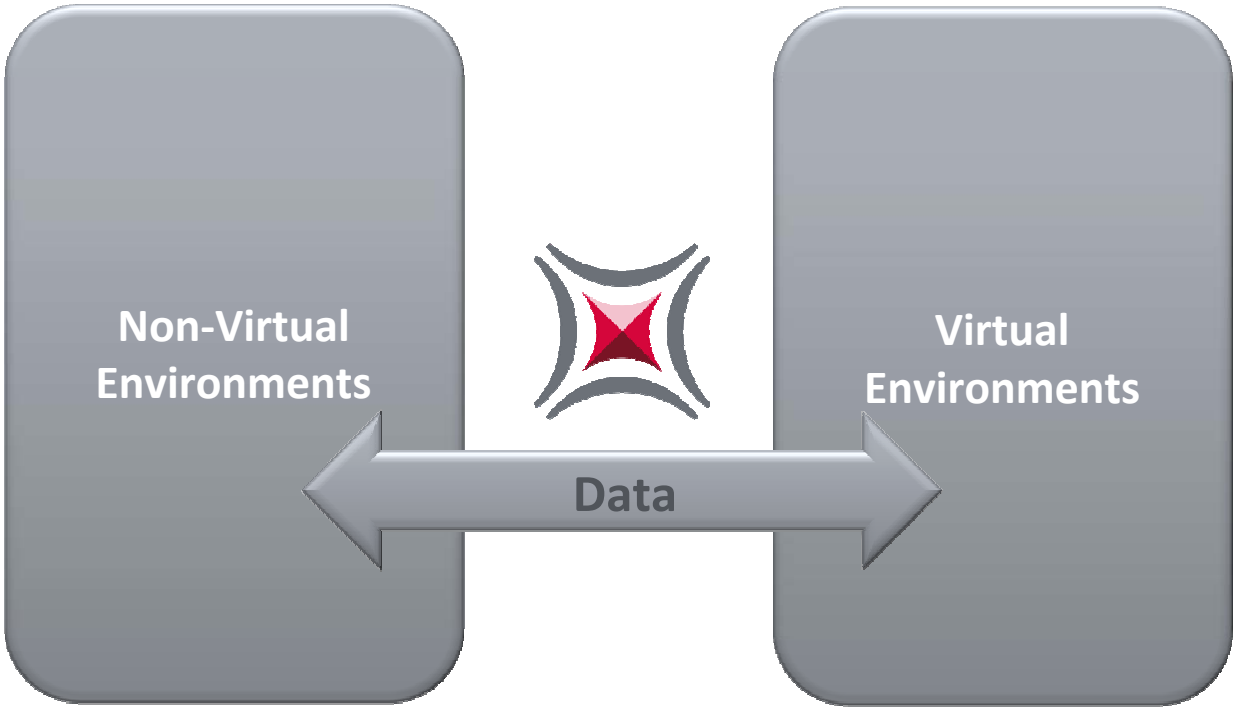
Security

- Network-based and host-based firewalls, intrusion detection/prevention systems
- Host-based anti-malware prevention
- Device and disk encryption
- Vulnerability and configuration management and remediation
- Network access control
- Network and storage encryption solutions
- Network behavior analysis and monitoring
- Etc, etc, etc

Virtualization Security

- **Virtual** Network-based and host-based firewalls, intrusion detection/prevention systems
- **Virtual** Host-based a… alware prevention (for example, antivirus… st or hypervisor)
- **Virtual** device …
- Vulnerabil… agement and rem…
- **Virtual** Netv… ntrol
- **Virtual** network … ncryption solutions
- **Virtual** network behavior analysis and monitoring
- **Virtual** Machine isolation and segmentation
- **Hypervisor** security, prevent escape from the hypervisor
- Etc, etc, etc

Approaches to virtualization security
(the more things change, the more they remain the same)

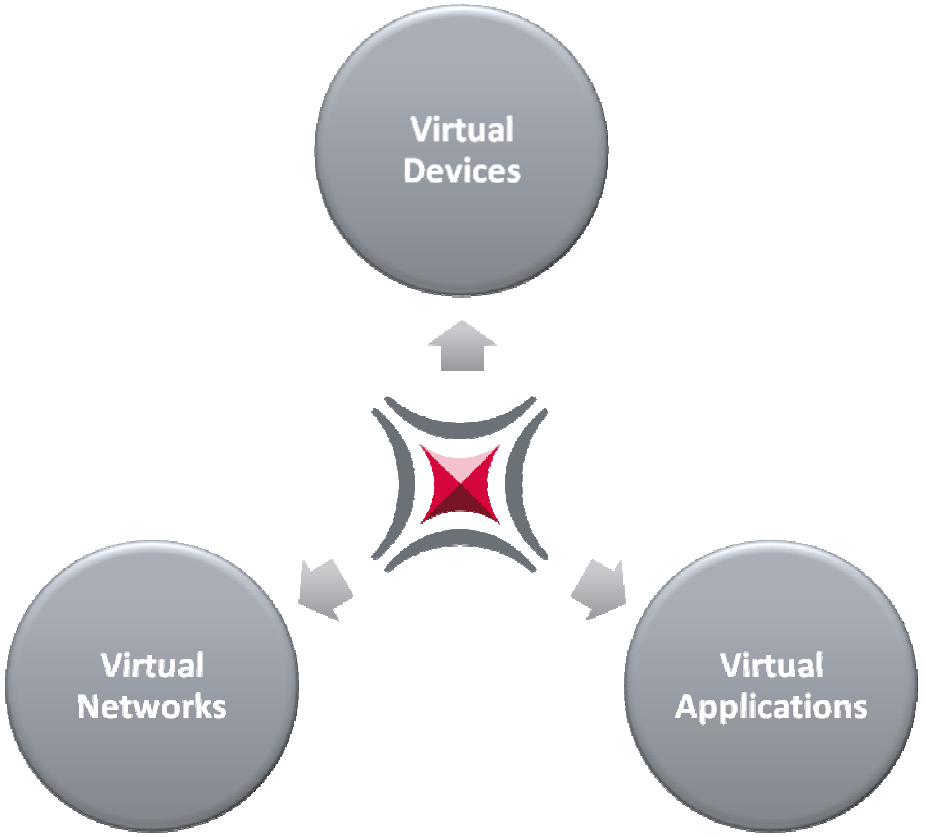


The only element that traverses between non-virtual and virtual environments is – DATA!

Protect the data, persistently!

The sane way to secure a dynamic virtual environment

- **The data**
  - Is the only element that cannot be virtualized
  - Has a longer lifecycle than virtual devices, networks and applications
  - Is the only element that moves between the virtual and non-virtual spaces
- **Device/perimeter-centric products not effective**
  - An **information-centric** approach is the **right** solution



BITARMOR

Example Scenarios

- **Desktop virtualization environments**
  - Accessing data on file shares, SharePoint, saving data locally, using a USB device
- **Application streaming**
  - Offline access to data, data in file shares/ SharePoint, data being emailed, leak prevention
- **Mixed environments**
  - Sharing data between virtual and non-virtual environments

About BitArmor

Smart Tag technology – an information-centric approach

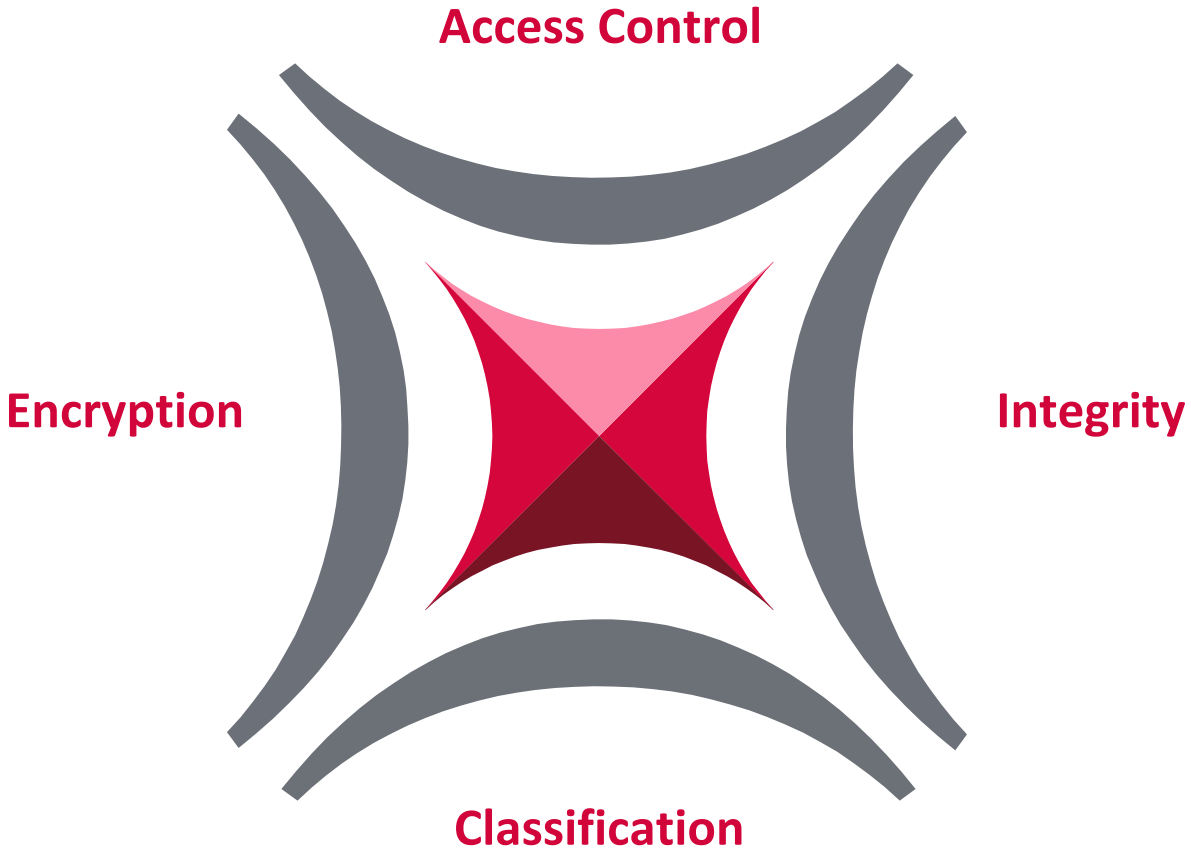
The BitArmor Smart Tag™

Protect data wherever it goes

- ***A unique information-centric security approach***
  - Attach protection policies to data itself
  - Policies travel with the data, giving you complete and continous protection

The BitArmor Smart Tag™

Protection policies that stay with the data



BitArmor
Solves Critical Data Protection Problems

- **BitArmor DataControl**
  - Protects data wherever it goes – inside and outside the organization
- **A single, integrated, data-protection solution**
  - Full disk encryption for laptops
  - Smart Tag enabled, ***persistent*** file encryption
    - Removable media protection
    - Email attachment protection
    - Network file share protection
- **The BitArmor No-Breach Guarantee™**
  - The industry's only guarantee against data breaches!

BITARMOR

Thoughts on evolving nature of security
(and what security is not)

- **Security is not about restricting data movement**
  - Security is about enabling secure sharing of data
  - Security should enable the business and not be a hindrance
- **Security is not about protecting devices/networks**
  - Security is about protecting sensitive data
- **Security is not just an IT problem**
  - If you, as the CISO, don't have buy-in from the business, you are toast

BITARMOR

Recommendations

- **Let virtualization "Be all it can be"**
  - Virtualization provides an opportunity for business to be responsive and dynamic as never before
  - Security should be an enabler, not a hindrance
- **Protect the infrastructure, but focus on data**
  - Basic virtual infrastructure protection is essential, but let's not go overboard
  - Take advantage of statelessness and reset
  - Let data move about, but let it remain protected at all times – i.e. persistent and information-centric protection.