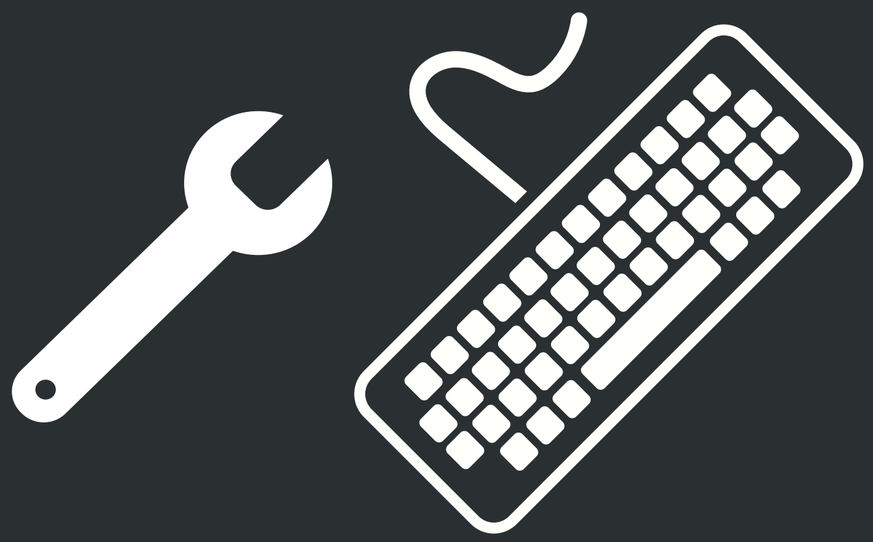
Windows Server 2003 End of Support

What does it mean? What are my options?



The Register®

TREND MICRO™

Windows Server 2003 End of Life- Why Care?

The next big vulnerability (Heartbleed/Shellshock) is looming

No more patches from Microsoft

Migration takes time; custom support is expensive

Painful experience from previous End of life (Win 2000 and XP)

TREND MICRO™

The Register®

What are we dealing with?

- Greater spending on security and risk management initiatives
- Attacks on businesses becoming more sophisticated highlighting traditional security no longer enough
- Now we have to deal with Windows Server 2003 End of Support in July 2015

The reality with Windows Server 2003

- **Most companies still have some 2003 Server within their estate**
  - Only 17% are 2003 free*
- **Why not just upgrade**
  - Regulations
  - Custom applications
  - Time needed for testing
  - Exploration of other options
  - Other priorities

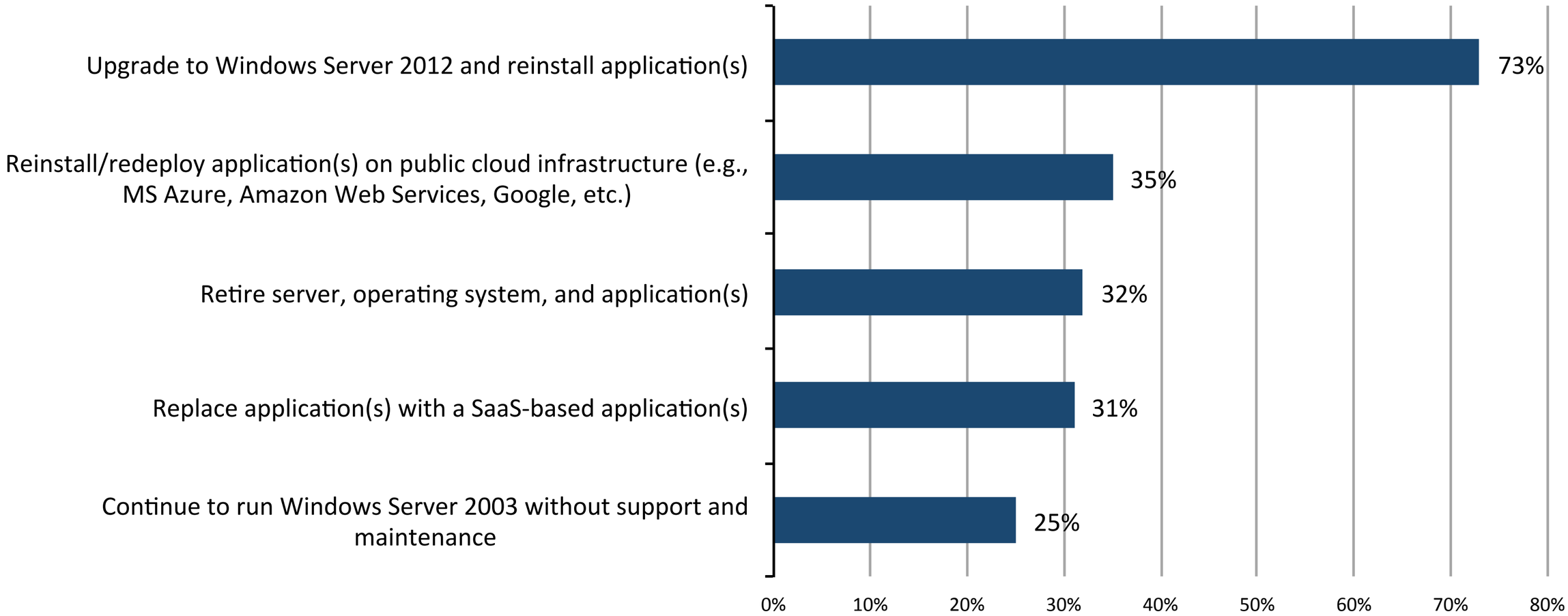
* Enterprise Security Group 2003 Server Usage Survey 2015

TREND MICRO™

The Register®

Windows Server 2003 Migration Plans

What are your organization's plans for upgrading from and/or migrating off of its Windows Server 2003 systems? (Percent of respondents, N=497, multiple responses accepted)

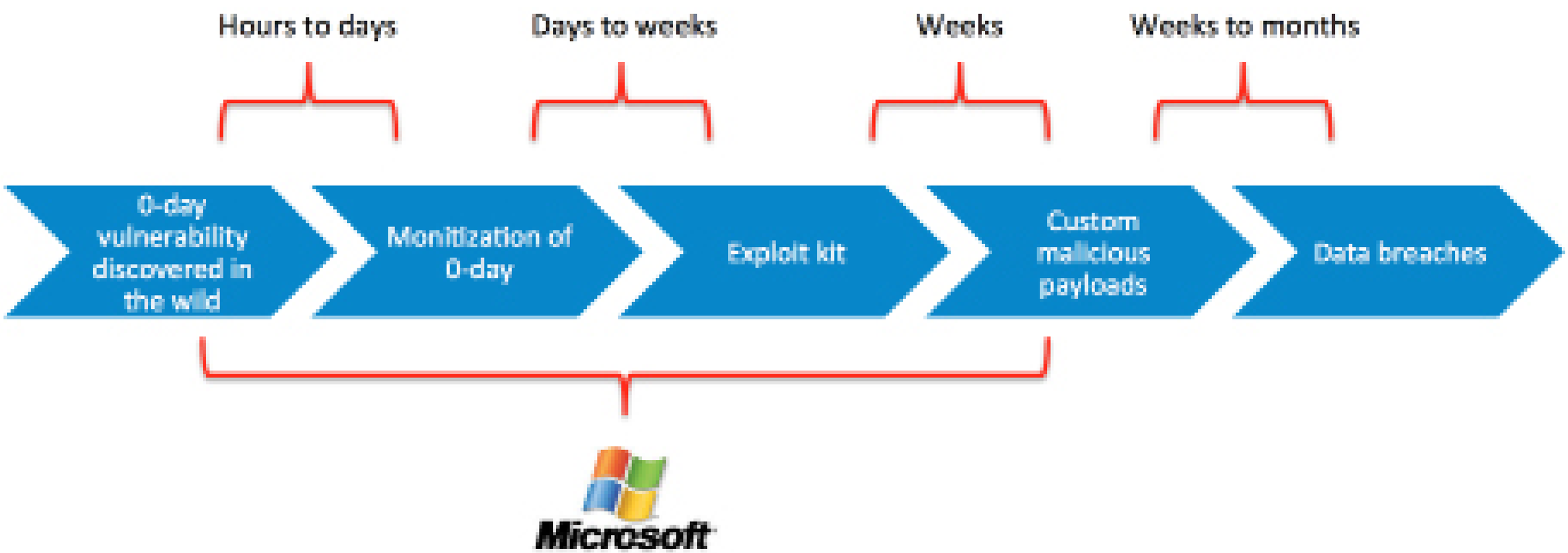


* Enterprise Security Group 2003 Server Usage Survey 2015

TREND MICRO™

The Register®

Main Risks with EOS:Exploitation of unpatched vulnerabilities



TREND MICRO™

The Register®

Compensating Controls

- **Microsoft support agreement**
- **Server configuration hardening**
  - MS, NIST, NSA . . .
- **Network security controls**
  - Network segmentation, ACLs, firewall rules
  - Virtual patching
- **Enhanced server monitoring**
  - Log events, profiling, forensics, network connections . . .

Server Compensating Controls

- **Application controls**
- **Advanced malware detection/prevention**
  - Server-based or server- and network-based
- **File integrity monitoring/control**
- **Host Based IPS – Virtual Patching**
- **Trusted hardware execution (TPM, TXT, etc.)**

The Bigger Truth

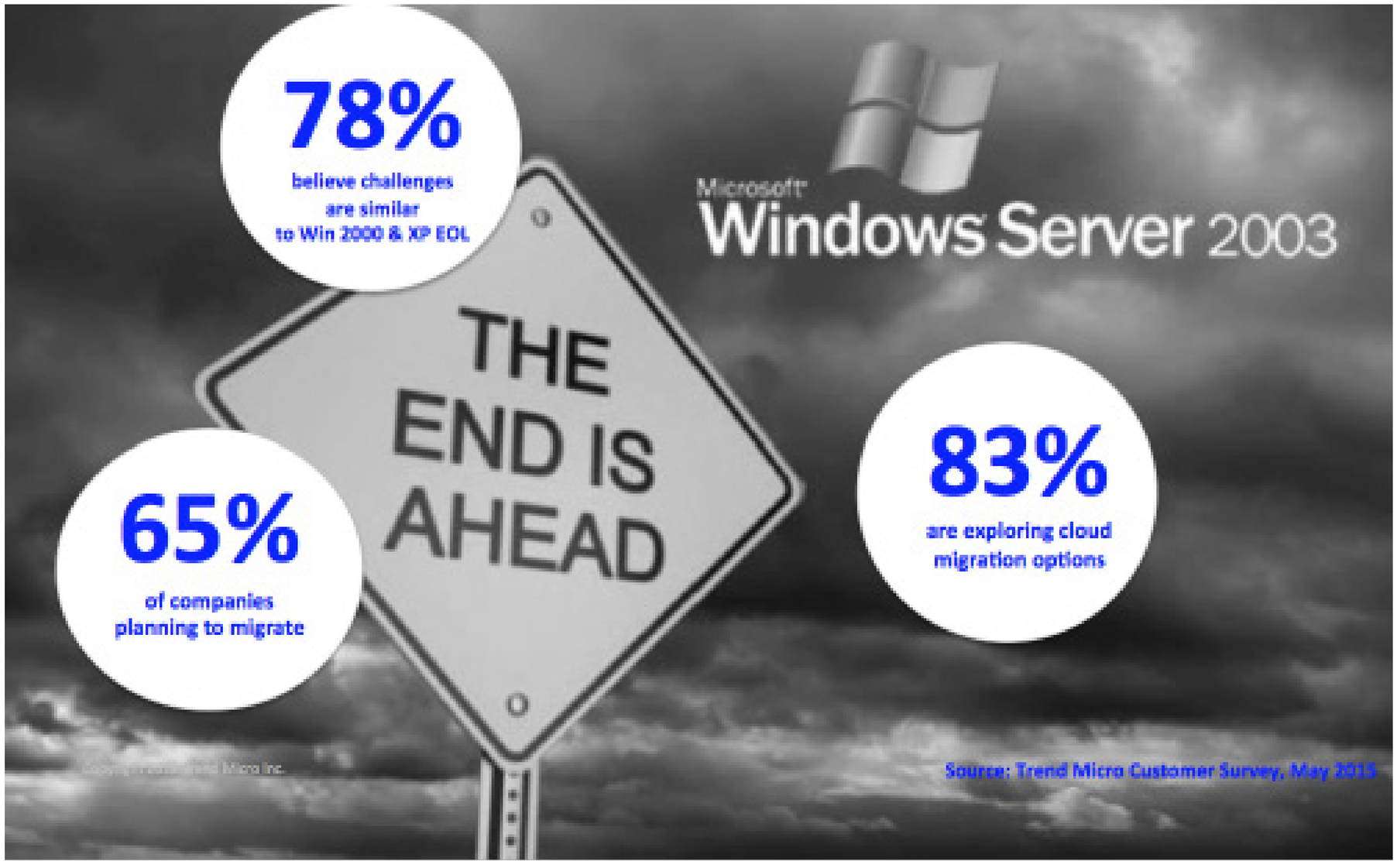
- **CISOs face a W2k3 server headache**
  - Time-consuming migrations
  - Security vulnerabilities
- **Organizations must do something**
  - Migrate or
  - Compensating controls
- **Keys to success**
  - Thorough strategy for security efficacy and operational efficiency

What Steps should be taken:

- **Catalogue your server estate and identify servers running Microsoft Server 2003**
- **Catalogue applications running on Microsoft Server 2003**
  - Identify application owners
  - Understand application dependencies
  - Understand application migration priorities and risks
- **Identity migration pre-requisites for each application**
- **Migrate those that can easily migrate to Windows Servers 2008 or 2012**
- **Build project plan with App owners if not easily migrated**
  - Where possible, redesign older applications that cannot be migrated
  - Replace/retire applications that can't be migrated to newer application where possible
  - Build mitigation solutions for applications that can't be migrated from Server 2003 or replaced

What Steps should be taken:

- **Mitigation requirements**
  - Protect future Server 2003 vulnerabilities from exploitation
  - Have an anti-malware solution that will continue to support 2003 Server
  - Monitor Servers for any suspicious or Malicious changes / activity
- **Mitigation options:**
  - Use a host based Intrusion Prevention Solution that uses IPS rules to stop unpatched vulnerabilities from being exploited over the network
  - Utilise an anti-malware solution that will continue to support the identification and blocking of malicious files targeting 2003 Server operating system for an extended period.
  - Utilise File Integrity Monitoring and Log Inspection to provide information of changes to the servers or high severity logs that might indicate suspicious or malicious behaviour on that 2003 Server.
- **Utilise extended period of 2003 Server protection to seek and appraise alternative applications to replace those that cannot be migrated quickly before July 14th 2015**
  - Re-engineer existing application
  - Buy in new application
  - Write new application



TREND MICRO™

The Register®

Trend Micro Deep Security: A Proven Security Solution

- History securing end of life platforms (Win XP and 2000)
- Protection for short (July 14) and longer term (migration)
- Comprehensive security controls
- Physical, virtual and cloud environments

TREND MICRO™

The Register®

How Deep Security Helps

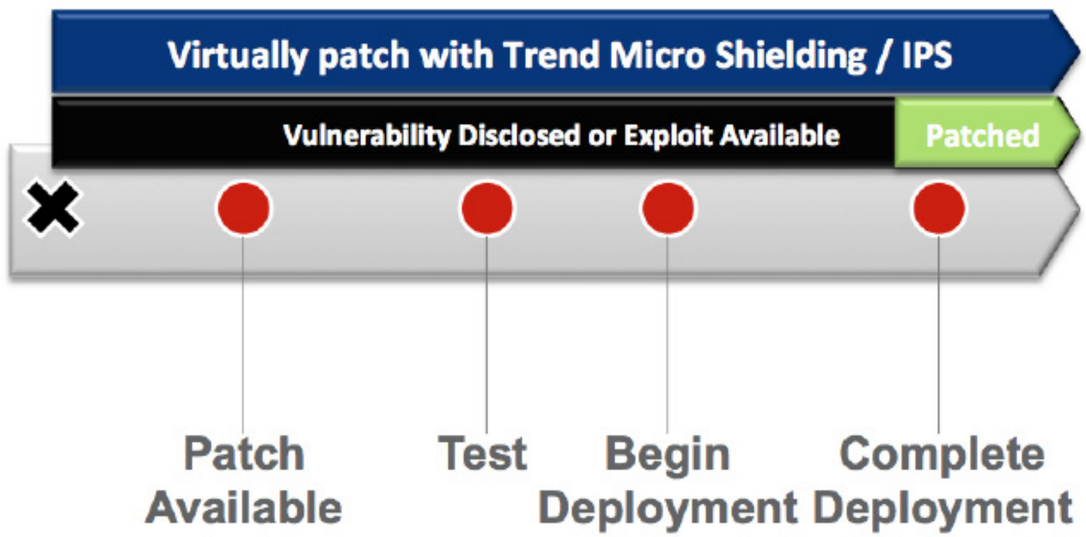
- **Network security**
  - -Virtual patching through Intrusion Detection & Protection (IDS/IPS)
- **System security**
  - - Integrity monitoring, enabling the discovery of unplanned or malicious changes to registry and key system files
- **Anti-malware**
  - - Protect vulnerable systems from the latest in threats

TREND MICRO™

The Register®

Virtual Patching

- Reduce risk of exposure to vulnerability exploits – especially as you scale
- Save money avoiding costly emergency patching
- Patch at your convenience
- Secure out-of-support platforms (Windows Server 2000, 2003)



TREND MICRO™

The Register®

System Security

Integrity Monitoring: Monitor critical systems, files, keys and users

- Monitoring for changes across operating systems, application files, registry keys, users, groups, and ports
- Alerting to identify any changes
- Custom trusted baseline system and whitelisting to reduce noise
- Complete logging for audit and compliance, with event forwarding to SIEM

TREND MICRO™

The Register®

Anti-malware with Web Reputation

Protection from viruses, bots, and bad code

- Real-time protection, based on global threat intelligence from the Smart Protection Network
- White or black list domains and URIs
- Prevent access to known command & control (C&C) sites
- Event alerting and reporting
- Ability to forward events to SIEM

TREND MICRO

The Register®

What Deep Security Enables

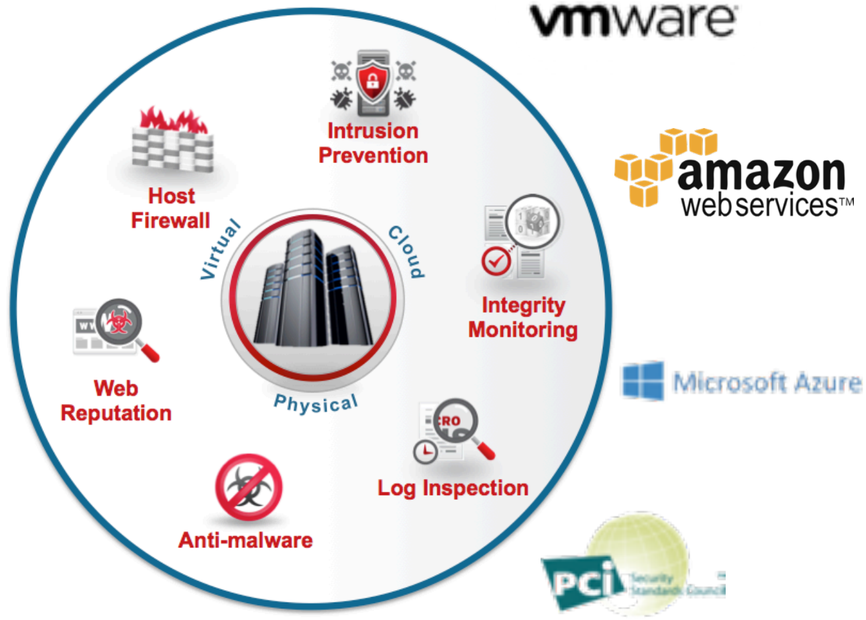
- Automated Security
- Centralized Management
- Enhanced System Performance

TREND MICRO™

The Register®

Trend Micro Deep Security Advantage

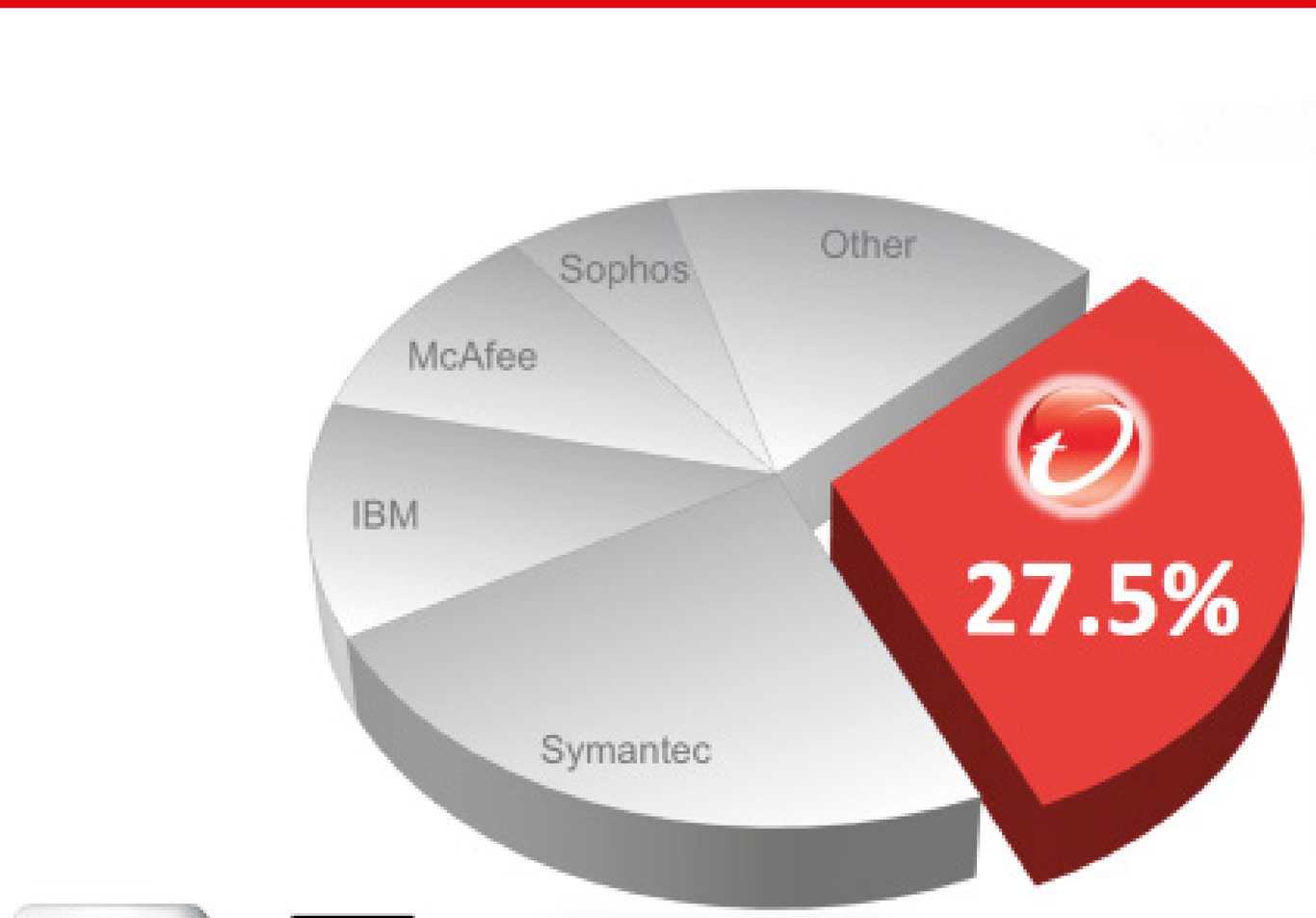
- Securing end-of-life platforms (Windows XP, 2000, 2003)
- Protect newer platforms after migration (Windows 2012, Azure and AWS)
- Protecting vulnerable Windows & Linux servers with virtual patching
- Automation of security across virtualization & cloud environments
- Highly efficient, comprehensive set of security controls



TREND MICRO™

The Register®

#1 Corporate Server Security Market Share1



CITRIX ready
VCE
EMC² VSPEX LABS VALIDATED
CISCO PARTNER Technology Developer
vmware PARTNER TECHNOLOGY ALLIANCE
amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER
Microsoft Partner
Gold Application Development

Source: IDC Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares, Figure 2, doc #250210, August 2014

TREND MICRO™

The Register®

Links

- Windows Server 2003 EOS and security support
- Windows Server 2003 after July - Blog

TREND MICRO™

The Register®