FROST & SULLIVAN

Hewlett Packard Enterprise

intel

Microsoft

A Webinar Executive Summary

Server Hardware Under Attack: Is Your Small or Midsized Business Protected?

MODERATOR:

Michael Suby
Vice President, Research
Frost & Sullivan

PANELISTS:

Robert Moore
Director of Server Software
& Product Security
Hewlett Packard Enterprise

Jason Lamb
Cloud / Software Defined
Infrastructure Technology
Solutions Specialist
Intel

Ryan Puffer
Program Manager –
Virtualization Security
Microsoft

Introduction

Recently, Michael Suby, Vice President, Research, Frost & Sullivan, hosted a timely webinar discussion, Server Hardware under Attack: Is Your Small or Midsized Business Protected? Robert Moore, Director of Server Software & Product Security, Hewlett Packard Enterprise; Jason Lamb, Cloud /Software Defined Infrastructure Technology Solutions Specialist, Intel; and Ryan Puffer, Program Manager –Virtualization Security, Microsoft, lent their expertise and insights as Suby conducted a deep dive into the state of server security today. The participants discussed how small and medium businesses are at a heightened level of cyber and business risk with aging servers running Windows Server 2008. The discussion did not end with the statement of a problem, but provided practical guidance on security resiliency.

IT Security Critical for Small and Medium Businesses

In an age of rampant and ongoing security breaches, a secure IT infrastructure and plan is important for all companies, but it's critical for small and medium sized businesses. Downtime is costly and lost server time can cost small businesses big money. It is also an unfortunate reality that often small businesses never fully recover from a serious IT issue or security lapse. In fact, according to The Denver Post, "Sixty percent of small companies that suffer a serious security breach will be out of business within the next six months." Companies of all sizes need to be diligent as new security attacks keep coming. In fact, it has been predicted that by 2021, cyber security threats will cost the global economy about 6 trillion dollars.

Hardware is the Playing Field

As noted in the graphic below, computer hardware is an emerging playing field for cyber warfare. One particularly destructive example of a hardware vulnerability is called Meltdown. Affecting Intel microprocessors, IBM POWER processors and some ARM based microprocessors, it is a rogue process that can potentially read all memory, even though unauthorized to do so. This security vulnerability, and others like it, is considered potentially "catastrophic" by security analysts…not to mention the business that have experienced the damage they can do. Several other hardware invasive processes are listed in the chart below:

Standup and Take Notice Circumstances

Cyber warefare taking aim at hardware vulnerabilities

- List of 'identified' vulnerabilities growing: Spectre, Meltdown, Foreshadow, Foreshadow-NG, Baseband Management Controller, and most recently, ZombieLoad

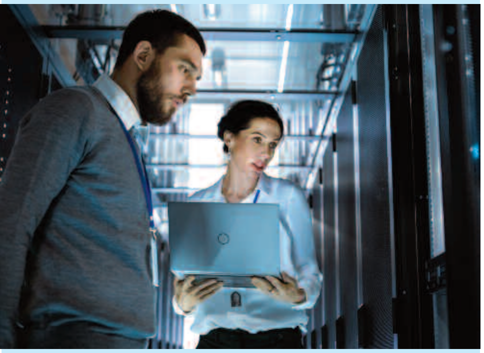
End-of-Support for Windows Server 2008/2008 R2 happens on January 14, 2020

- Complimentary provisioning of security updates ends
- Extra spending becomes the new standard

To address hardware server vulnerabilities, SMBs should contemplate the 'root of trust' that exists with their server hardware. Lacking assurance that the server firmware has not been compromised, adds to cyber risk as well as business risk associated with the operations supported by vulnerable servers.

Another complicating factor in IT security is the fact that breach detection can take time. According to FireEye, it can take up to 78 days to detect a security compromise. Meanwhile, the damage continues. And even if an organization does quickly detect an issue, if the "fix" is not a good one, it can happen again. In addition, the end of support for Windows 2008 will take place on January 14, 2020. This means there will be no more complimentary security updates, especially beneficial for smaller companies.

> *"Data is everywhere, not just inside firewalls. There are growing quantities of data in cloud edge data centers and on mobile devices. And now we have to verify and validate every device connected to a customer ID."*
>
> **– Robert Moore**
> *Director of Server Software*
> *& Product Security*
> Hewlett Packard Enterprise



Cloud Security Concerns

As the participants discussed, migrating to the cloud is not always a simple, optimal, or secure choice. There are often valid concerns about moving corporate data to the cloud as well as compliance, migration, and backup and recovery challenges. As Robert Moore, *Director of Server Software & Product Security, Hewlett Packard Enterprise*, stated, "Data is everywhere, not just inside firewalls. There are growing quantities of data in cloud edge data centers and on mobile devices. And now we have to verify and validate every device connected to a customer ID." So data security is also a growing issue.

Frost & Sullivan predicts that hybrid cloud (use of both public and private clouds for key services and data) and edge computing will continue to grow and that the Internet of Things (IoT) will create a mounting number of devices on premises and deployed remotely. But these advancements will come with big challenges, including security concerns, data storage issues, and the money and time it often takes to transfer and back up data safely. Leveraging the right mix of products and services will be an important ingredient for success. Of critical importance is having the foundation of resilient security in the servers that support critical business functions and process sensitive information. The industry thought leaders in attendance and moderator Michael Suby, *Vice President, Research*, Frost & Sullivan, offered the following recommendations about the current state of server components:

Recommendations for More Secure Servers

- As regulations continue to expand, look for servers built to be compliant with regulations
- Look for 'native data at rest' protection
- Look for a server that is agile, and ready for multiple cloud environments
- Look to improve performance and increase agility and pay attention to how the hardware and operating systems work together
- You need cutting edge products for your investment…solutions that will last a long time
- Consider your business relationship with partners and suppliers…they want security, too

Recommended Secure Server Feaures

☑ Immutable Authenticity Assurance

☑ Authoritative Alerts

☑ Simply Recovery to Trusted State

☑ Built Compliant

☑ Native Data-at-Rest Protection

☑ Step-up in Performance & Agility

It was agreed by all that as security regulations continue to expand, it's important to look for a server built to be compliant with regulations. As the discussion progressed, the following questions were also addressed:

How significant is the cyber security threat in the world today? Answers included:

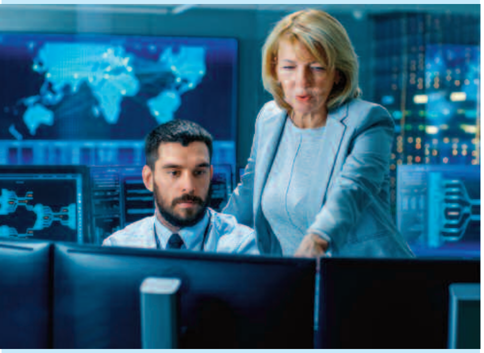
By 2021, cyber security threat costs to the global economy are predicted to be about 6 trillion dollars!

Research shows that there has been a significant increase in ransomware in the last two years.

Most hackers target smaller companies.

Personal mobility security concerns are paramount.

> *"We are headed toward encrypting everything. Constant research is needed."*
>
> **– Jason Lamb**
> *Cloud / Software Defined Infrastructure Technology Solutions Specialist*
> Intel



What are the latest threats and tools that hackers have been using?

Hackers are taking advantage of technology advances to push their hacks and AI gives them information about the right time and place to attack

Artificial Intelligence (AI) and machine learning (ML) are used to make sure Malware doesn't deploy until the virus or weapon reaches the target. AI gives perpetrators more information – such as the right time and place

Old style hacking, like "phishing emails" are utilizing a range of attack technologies to achieve bad ends

It was also noted that the perimeter firewall is not necessarily safe anymore as half of breaches take place inside a firewall. You need the right tools and equipment to detect this. The end goal is always to detect and recover

What do HPE, Intel and Microsoft do to protect and outsmart the hackers?

They work together to outsmart or stay ahead of them

HPE has hardware and software that verify information and credentials

Intel and Microsoft verify their own aspects of server

Intel has been working on solutions to mitigate side channel attacks

Jason Lamb, Cloud / Software Defined Infrastructure Technology Solutions Specialist, predicts that we are headed toward encrypting everything, and stated that constant research is needed

All three companies represented, Hewlett Packard Enterprise, Microsoft and Intel, are working together to make hardware and software security more effective and complete. Windows has big advances in better security hardware. This might include insulating certain information from other areas.

Virtualization can also add another layer of security. Requiring additional information to access areas of the operating system is a relatively new strategy; even if a perpetrator gets into the system they are not able to access certain information.

In closing, the participants gave their recommendations for secure server features. Jason Lamb of Intel stressed the importance of staying as up to date as possible, by using solutions and equipment that have the latest security features and the flexibility to accommodate new ones. All advised small and large companies to balance investments in data center technology with hardware and software upgrades, and reminded listeners that the right technology can provide critical security barriers.

About Hewlett Packard Enterprises

Hewlett Packard Enterprise is a global technology leader focused on developing intelligent solutions that allow customers to capture, analyze and act upon data seamlessly from edge to cloud. HPE enables customers to accelerate business outcomes by driving new business models, creating new customer and employee experiences, and increasing operational efficiency today and into the future. Visit us at www.hpe.com.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 40 offices on six continents. Learn more at www.frost.com.