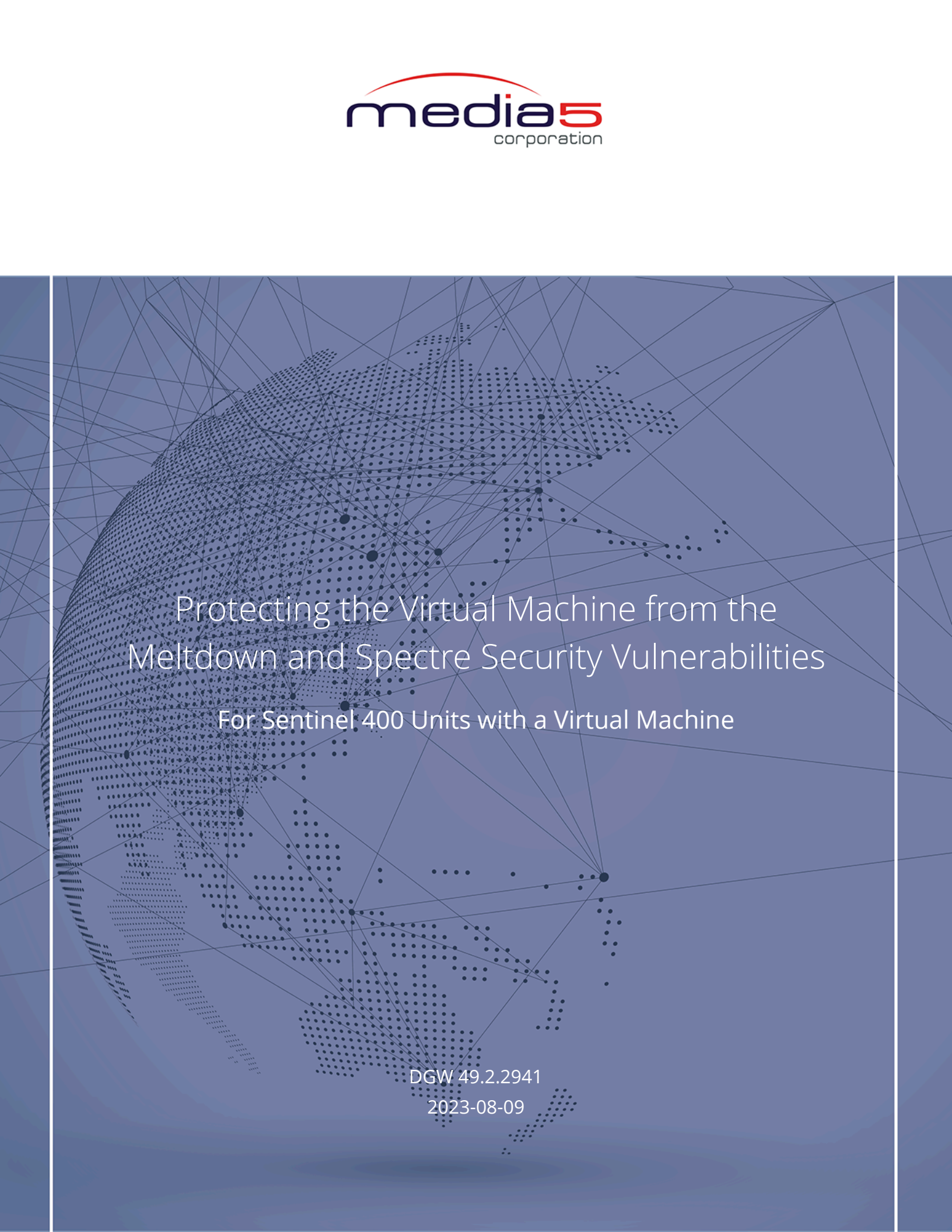


The background of the slide is a dark blue field with a complex, abstract pattern of thin white lines and dots, resembling a network or a stylized globe. The lines and dots are more densely packed on the left side, creating a sense of depth and movement.

Protecting the Virtual Machine from the Meltdown and Spectre Security Vulnerabilities

For Sentinel 400 Units with a Virtual Machine

DGW 49.2.2941
2023-08-09

Table of Contents

What are the Meltdown and Spectre Security Vulnerabilities	3
Is my VM vulnerable to Meltdown and Spectre?	3
Is all the System Vulnerable?	3
How to Protect my VM against Meltdown	4
How to Protect my VM against Spectre	4
Copyright Notice	5

What are the Meltdown and Spectre Security Vulnerabilities

These vulnerabilities allow a non-privileged process to read sensitive data in memory, thus accessing privileged information from the kernel or other processes.

A Virtual Machine (VM) running inside the Sentinel 400 **may** be vulnerable to Meltdown (CVE-2017-5754) and to the two variants of Spectre (CVE-2017-5753 and CVE-2017-5715).

For more information on these vulnerabilities:

- [https://en.wikipedia.org/wiki/Meltdown_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability))
- [https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability))

Is my VM vulnerable to Meltdown and Spectre?

Your Virtual Machine (VM) is only vulnerable if it allows running third-party/rogue applications or scripts.

For example:

- A restricted user who has shell access can run malicious software.
- A user surfing the Net from within the VM can unknowingly run malicious Javascript from his browser.

You can consider your VM non-vulnerable if your VM is a secured and closed system that does not allow running rogue code (i.e. the vulnerabilities cannot be exploited), unless an attacker finds other vulnerabilities to break into your VM.

Is all the System Vulnerable?

The DGW firmware in the Mediatrix system, by itself, is not vulnerable since it does not allow running rogue code:

- <https://www.media5corp.com/media5-statement-meltdown-spectre-vulnerabilities/>

But it is theoretically possible, for a Virtual Machine compromised by the Spectre vulnerability, to read memory outside the Virtual Machine and access sensitive data of the Mediatrix system. The best protection against this is to secure your VM, to make sure there is no known means an attacker can use to break into your VM.

Media5 also recommends to always keep your Sentinel 400 up-to-date with to the latest DGW firmware version.

How to Protect my VM against Meltdown

Linux kernels have a new feature called KPTI (previously known as KAISER) that protects against Meltdown.

If your Virtual Machine is vulnerable, Media5 recommends that you upgrade your kernel to a version that supports KPTI, and enable it.

For more information on KPTI: https://en.wikipedia.org/wiki/Kernel_page-table_isolation

IMPORTANT: Enabling KPTI may impact the performance of your Virtual Machine.

How to Protect my VM against Spectre

There are different mitigation techniques against Spectre:

- Mitigation #1: A microcode update from the CPU vendor for better control over the branch speculation. Also need an updated kernel to enable these new features (IBRS and IBPB).
- Mitigation #2: Different techniques (like "retpoline" and "LFENCE") that require recompiling the kernel, packages and applications.

As the time this document was written, Mitigation #1 could not be applied, as Intel had not yet released a microcode update for the CPU of the Sentinel 400.

If your Virtual Machine is vulnerable, Media5 recommends applying Mitigation #2. See [https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)#Mitigation](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)#Mitigation) for more details.

IMPORTANT: Mitigation techniques against Spectre may impact the performance of your Virtual Machine.

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



media5corp.com