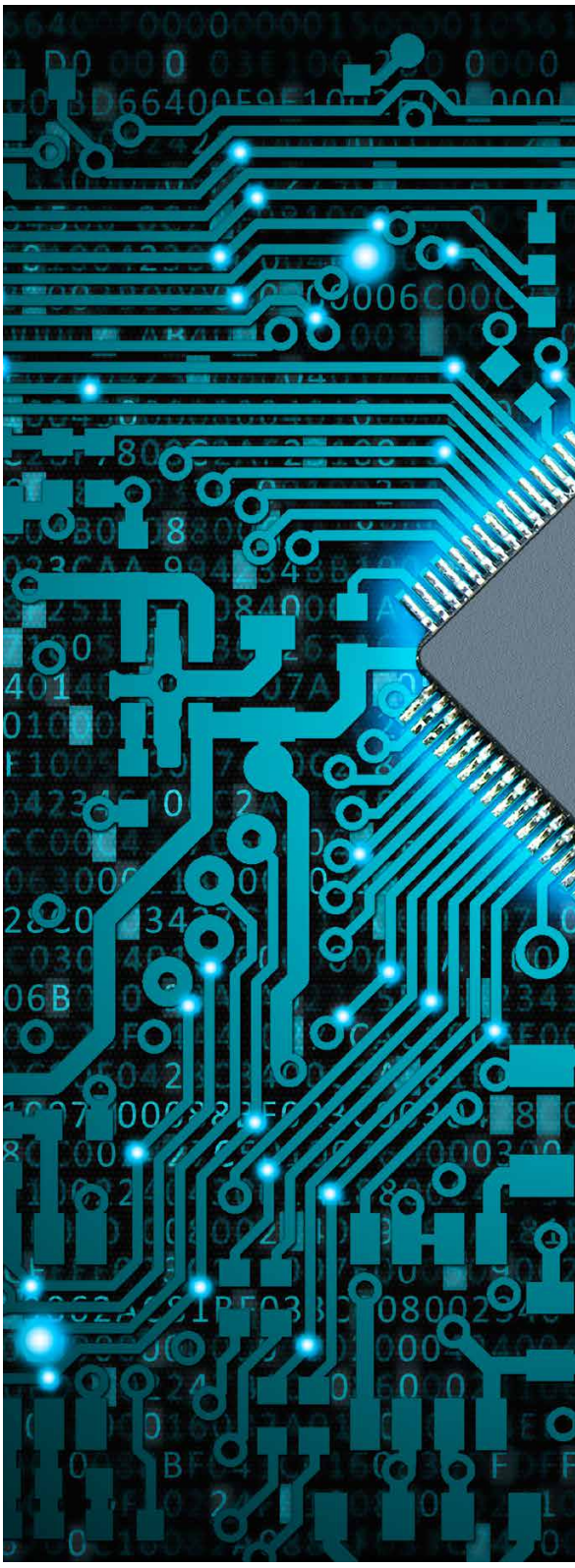
virsec

Solution Brief

SPECTRE AND MELTDOWN ATTACK PREVENTION

Patching vulnerabilities without compromising stability and performance



Spectre and Meltdown vulnerabilities—***microprocessor flaws present in virtually every server or application system throughout the datacenter and cloud***—have the greatest impact on enterprises systems seen in years. These flaws compromise isolation between multiple application processes, while also exposing data processed by the CPU. Shared environments and cloud services are most vulnerable, as these systems are designed to operate in multi-tenant environments while maintaining isolation between users. To avoid fallouts similar to WannaCry and Equifax, patching these flaws has become a priority with IT and security leaders.

Patching chip-level vulnerabilities is no simple matter. It requires installing fixes at multiple levels, resulting in an overwhelming IT initiative of updating everything from microcode to the kernel, operating system, hypervisor, libraries and more, and for every system affected. Operating system vendors and ISVs are collaborating with chip manufactures to help ensure the safety and security of customers' data and devices—updating OS security and helping drive distribution of microcode fixes. As these updates are installed, enterprises must ensure compatibility across applications, including custom-code, legacy technologies, and closed systems—a herculean effort that amounts to looking for the pink elephant.

While there is industry-wide concern about the risks posed by Spectre and Meltdown, enterprise IT teams are wary about deploying available patches released by manufacturers. Recent microcode re-designs have introduced critical application anomalies in functions and slowed response times. Uncommon error messages, difficulty logging on to servers and issues with admin consoles have also been reported. Additionally, new microcode updates for processor flaws have caused a high number of chip reboots, and some organizations have experienced as much as a 30% drop in overall application performance. Clearly, organizations need to rethink their approach to solving the Spectre and Meltdown problem.

Full Coverage Virtual Patching

Virsec is uniquely capable of solving the problems associated with patching Spectre and Meltdown, without requiring any hardware changes or software, kernel or microcode patches. Virsec Security Platform is

What Businesses Require

- Full Coverage Virtual Patching
- Continuous Real-time Defense
- Coverage for All Variant Types
- Ensured Compatibility, Stability and Performance

the first application security solution that protects against known and unknown attacks posed by Spectre and Meltdown, while maintaining application stability, compatibility and performance. Built on patented **Trusted Execution™** technology, the solution preemptively patches vulnerabilities at the binary level to minimize risk and prevent advanced memory-based threats, fileless malware, and unknown or zero-day attacks in real time. The Virsec solution also uniquely protects against cartographic operations on kernel memory commonly associated with Meltdown. With Virsec, companies can patch microcode flaws and ensure defense against future business crippling attacks without an urgency to upgrade systems.

Continuous Real-time Defense

Virsec Security Platform provides ground-breaking application and microcode defense that prevents advanced and uncommon attacks on enterprise applications. The platform defends web applications, compiled code and binaries by analyzing code as it executes in memory, allowing it to uncover vulnerabilities in process functions introduced by users or malware. Using Trusted Execution, the solution can effectively instrument and protect code on the fly at the lowest level, as binaries are fetched from main memory for execution. The platform ensures application integrity and closes down windows of exposure to the most sophisticated types of attacks including existing and new variants of Spectre and Meltdown.

Trusted Execution eliminates risks associated with Spectre and Meltdown. It deterministically protects against speculative execution abuse using an instruction translation approach that does not require modification to the application or disruptive changes to the kernel or microcode. This unique approach reliably identifies instructions that perform user-controlled memory reads and prevents instructions from accessing out-of-bounds memory during speculative execution—as seen in Spectre variant 1 attacks. Trusted Execution also prevents mis-training of branch predictors—as seen in Spectre Variant 2 attacks. It also disables side-channel attack code and terminates attacker-launched processes to block exploitation using Meltdown. Trusted Execution enables the detection and prevention of current Spectre and Meltdown exploits in real time as well as future attack variants that will inevitably appear.

Attack Mitigation Delivered

Spectre Variant 1

(Protect User & Kernel Space)

- Identify instructions vulnerable to out of bounds access
- Fence vulnerable instructions so they don't execute out of order
- Intercept processes with "spy" functionality
- Monitor hit rate of "malicious" instruction(s)
- Terminate processes that execute malicious instruction(s) beyond threshold

Spectre Variant 2

(Protect User & Kernel Space)

- Identify instructions vulnerable to branch mis-prediction
- In-Line patching with "Retpoline" or "Un-train" code
- Intercept processes with "spy" functionality
- Monitor hit rate of "malicious" instruction(s)
- Terminate processes that execute malicious instruction(s) beyond threshold

Meltdown Variant 3*

(Protect User & Kernel Space)

- Intercept processes with "spy" functionality
- Monitor hit rate of "malicious" instruction(s)
- Terminate processes that execute malicious instruction(s) beyond threshold
- Terminate processes that experience run time exceptions beyond threshold
- Terminate processes that execute transient instructions beyond threshold

**Does not require a victim process*

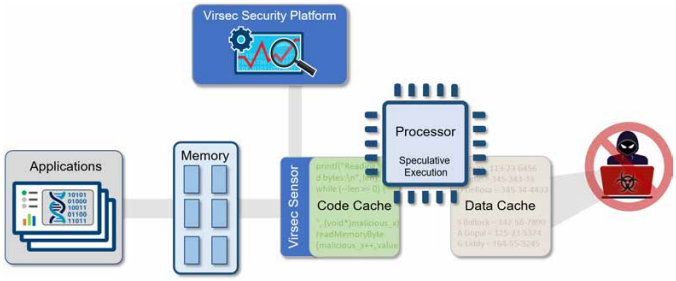


Figure 2: Virsec Spectre/Meltdown Defense

Coverage For All Attack Variants

Implementing Spectre and Meltdown fix is essential to reduce exposure of sensitive information processed by the CPU. Failure to put protective measures in place can be detrimental to business. With Virsec, IT can effectively protect applications and the data behind them, as they run on vulnerable CPUs or operating systems. Virsec provides coverage across most systems, including legacy technologies and closed ICS/SCADA environments. With Virsec, organizations can reduce the risk of data exposure by extending protection where vendor patches are not commonly available or have not been installed.

	Virsec Security Platform	Microcode Patch	Operating System Patch
Spectre Variant 1	✓		
Spectre Variant 2	✓	✓	✓
Meltdown	✓	✓	✓
Unknown Variants	✓		

Ensured Compatibility, Stability and Performance

Virsec enables IT teams to patch Spectre and Meltdown flaws without sacrificing stability and performance. Enterprises are freed from the potential for performance degradation or system reboots, and requirements to recompile code. Virsec's preemptive patching capability has been tested to run on vulnerable processor and operating system technology to patch binaries, while maintaining application compatibility and reliability. While chip and OS vendors have released patches updating microcode and operating systems, updates to microcode are risky and can render a computer unusable. Microcode updates are also prone to unintended consequences that can impact system performance and introduce instability for many environments and that has been an issue in the effort to address Spectre and Meltdown risks. The Virsec solution operates between the application and process memory to effectively protect applications and data as they run on vulnerable CPUs, while also allowing IT to maintain acceptable performance levels without compatibility or stability concerns.

Virsec Security Platform

Virsec Security Platform secures the entire application perimeter from memory to the web as attacks happen, identifying OWASP Top 10, advanced targeted attacks, and unknown threats without signatures, DAST/SAST integration and additional emulators and intelligence services. With Virsec, enterprises can effectively harden applications from the inside to prevent malicious activities, while ensuring application integrity, API enforcement and continuous authorization in the face of a threat.

Virsec Security Platform complements existing security solutions and increases the value of your entire security investment. It provides additional defense to harden the application against advanced attacks that bypass traditional security defenses like WAFs and IPS. With each attack or threat detected, the platform ensures attack attribution with detailed forensic data captured during execution. This data can be easily leveraged by existing firewalls, access control solutions, application delivery controllers and cloud-based security services to prevent subsequent attacks from ever reaching the server.

The platform can detect malicious exploits on first attempt and effectively mitigate attacks instantly. It identifies compiled-code tampering, such as DLL injection attacks within code segment, and memory corruption. Additionally, Virsec's unique

deterministic approach to threat detection requires no managed tuning. It automatically seals vulnerabilities preemptively and enables unsurpassed accuracy in threat detection with true zero-day defense—ensuring visibility into evasive threats, rapid time-to-protection and minimized risk.

Key Capabilities	Virsec Security Platform	RASP	WAF
Microcode Protection	✓		
Web Application Protection	✓	✓	✓
Fileless, Memory-based Attack Protection (on binaries)	✓		
Server-side File System Protection	✓	✓	
Automatic Defense Against Evolving Attacks	✓		✓
Advanced Non-Signature-Based Protection	✓		
Definitive, No-False-Positive Technology	✓		

About Virsec

Based in San Jose, California, Virsec was founded on the belief that a new model is required to counter today's advanced threats. The company is led by industry veterans who have driven one of the world's top processor teams, and created innovative technology in network security, embedded systems and real-time memory systems. The team has broad leadership experience at companies including AMD, Cisco, Palo Alto Networks, Juniper, Dell, NextGen, BMC Software, ForcePoint, as well a long list of high-growth start-ups.

More information can be found at www.virsec.com.

virsec®

226 Airport Parkway, Suite 350 • San Jose, CA 95110

Email: info@virsec.com • Phone: (877) 213-3558 • Web: www.virsec.com • Twitter: virsecsystems