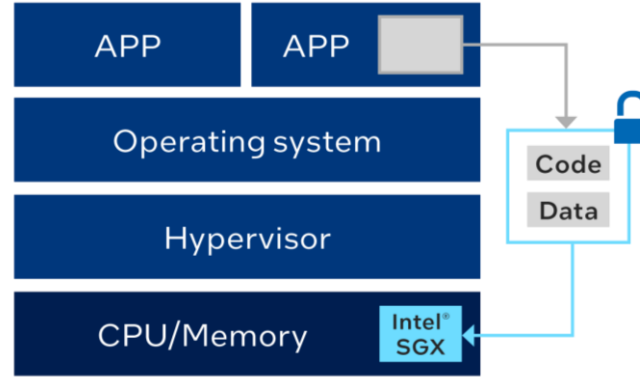
Tightening side channel protections with Intel SGX AEX-Notify

Scott Constable (Intel Labs)

Intel® Software Guard Extensions

- Intel® SGX is the **most deployed**, **researched**, and **updated** Confidential Computing technology in data centers today
- Delivers the **smallest potential attack surface** of any TEE available for the data center



Intel SGX for the Datacenter

2018: Intel SGX **first offered for the data center** with Intel Xeon-E processors

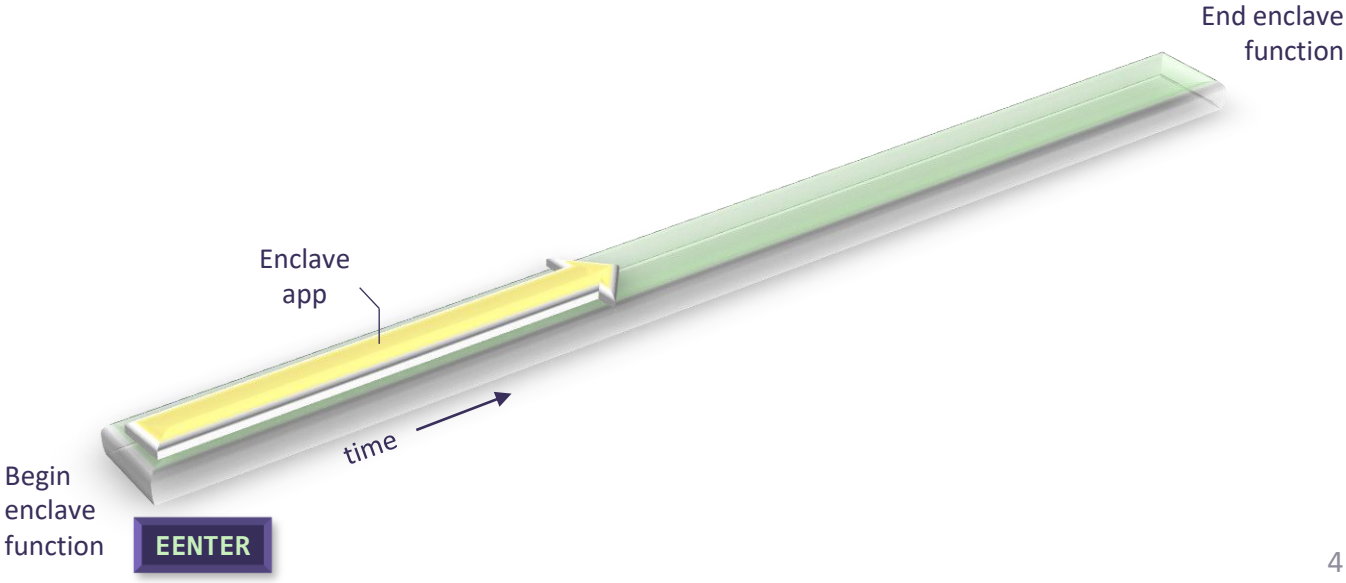
2021: Intel SGX offered on Intel 3rd Gen Xeon Scalable Processors (codenamed Ice Lake)

- Up to **1TB protected enclaves** for code and data
- Protected offload from enclaves to **HW accelerators**
- Achieved **broad software ecosystem support**

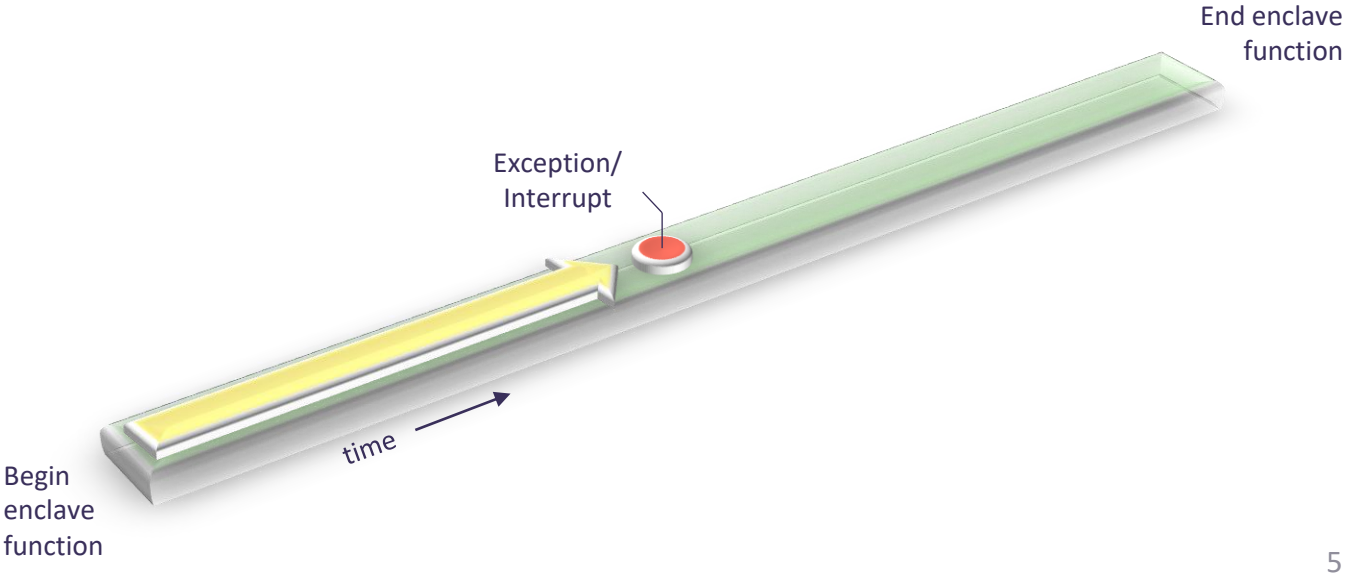
2023: Asynchronous Enclave Exit Notify (**AEX-Notify**) introduced on Intel 5th Gen Xeon Scalable Processors (codenamed Emerald Rapids)

- AEX-Notify is also **backportable to older server processors** via a microcode update

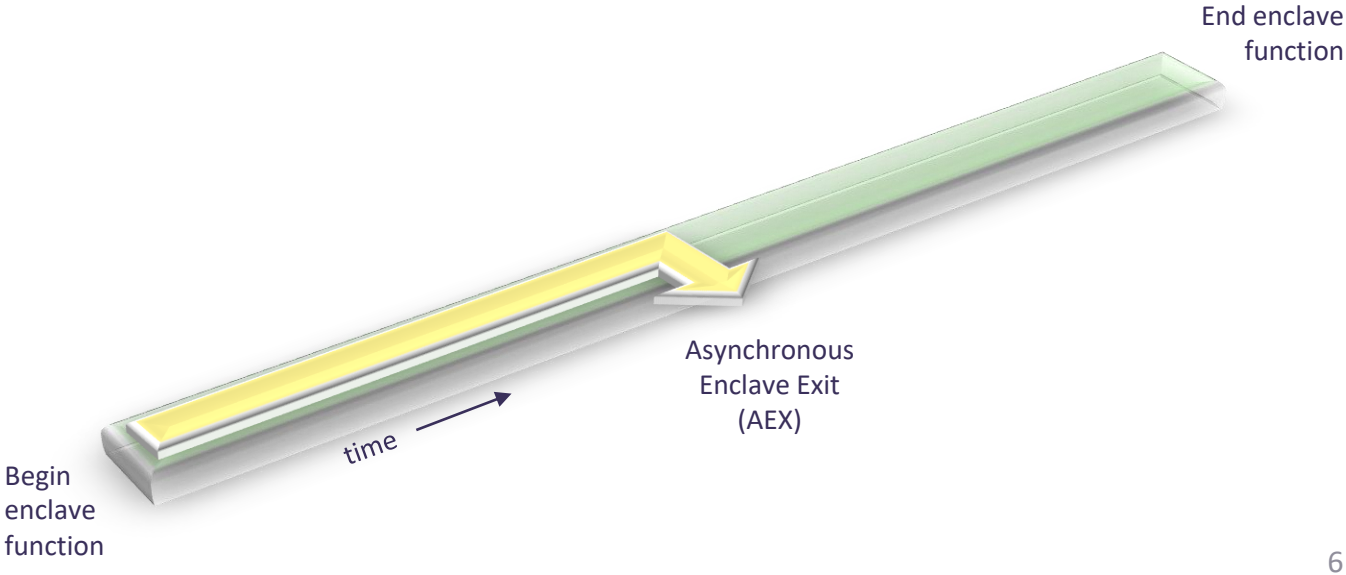
Entering and Exiting an Intel SGX Enclave



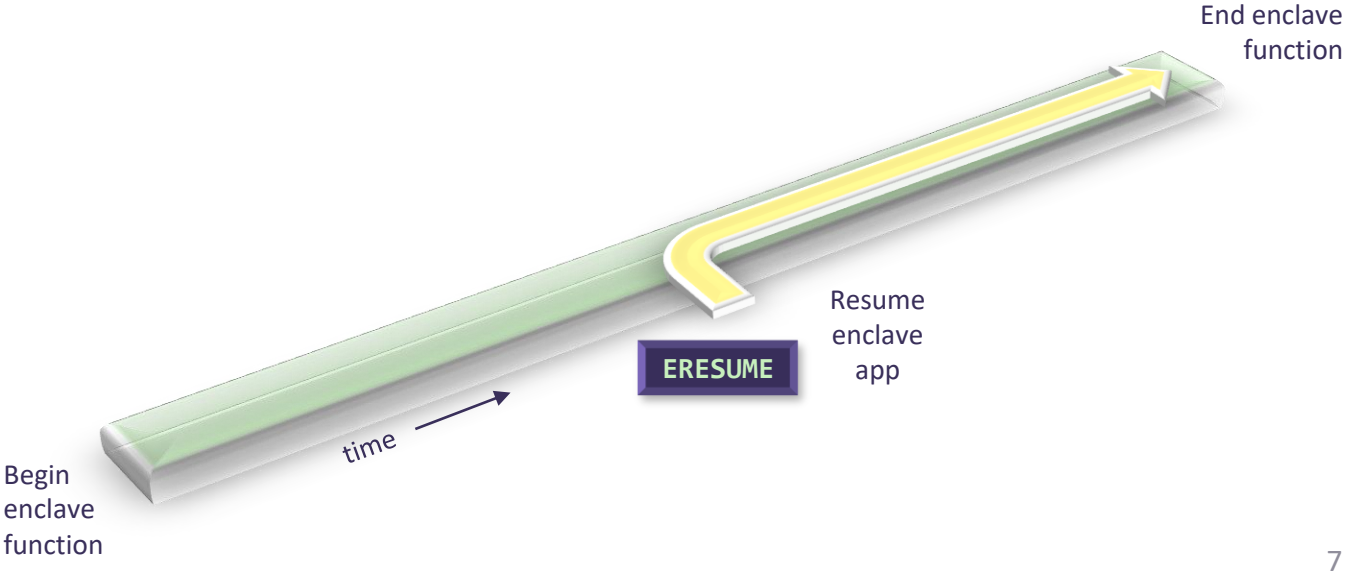
Entering and Exiting an Intel SGX Enclave



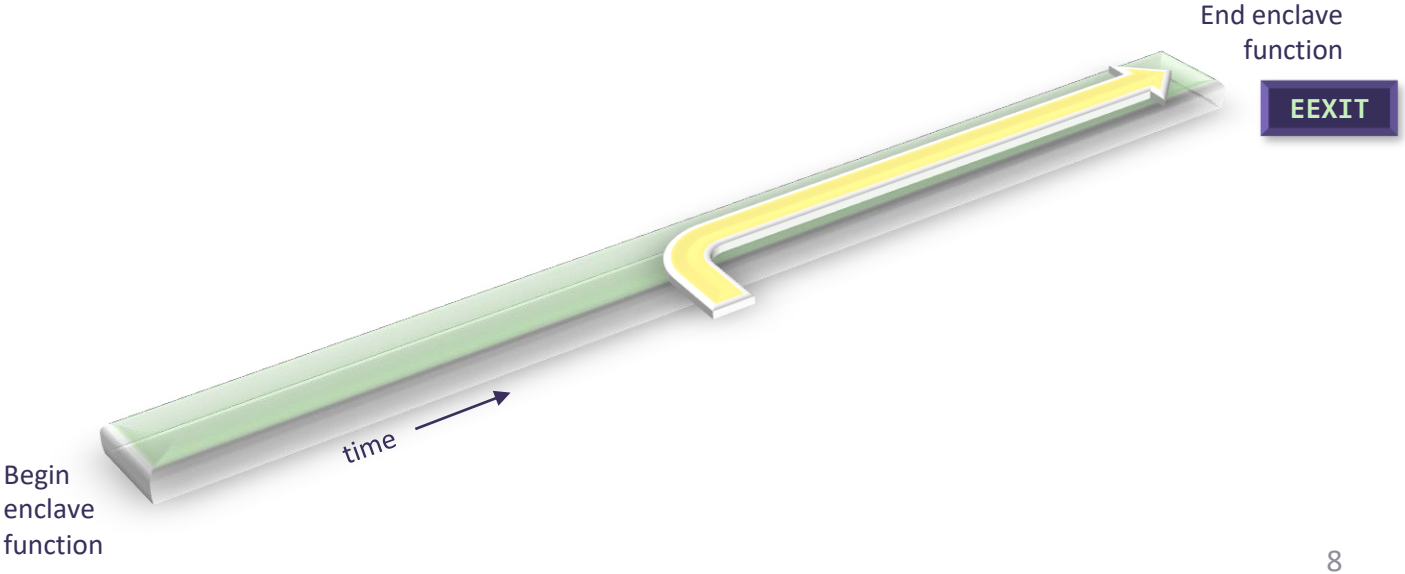
Entering and Exiting an Intel SGX Enclave



Entering and Exiting an Intel SGX Enclave



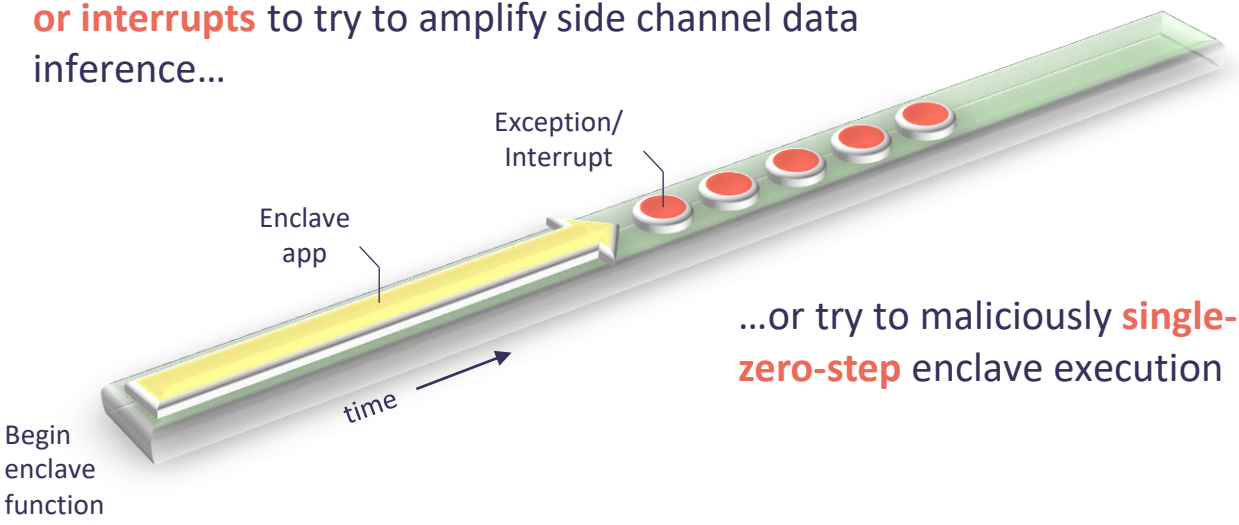
Entering and Exiting an Intel SGX Enclave



What if the OS/VMM is malicious?

What if the OS/VMM is Malicious?

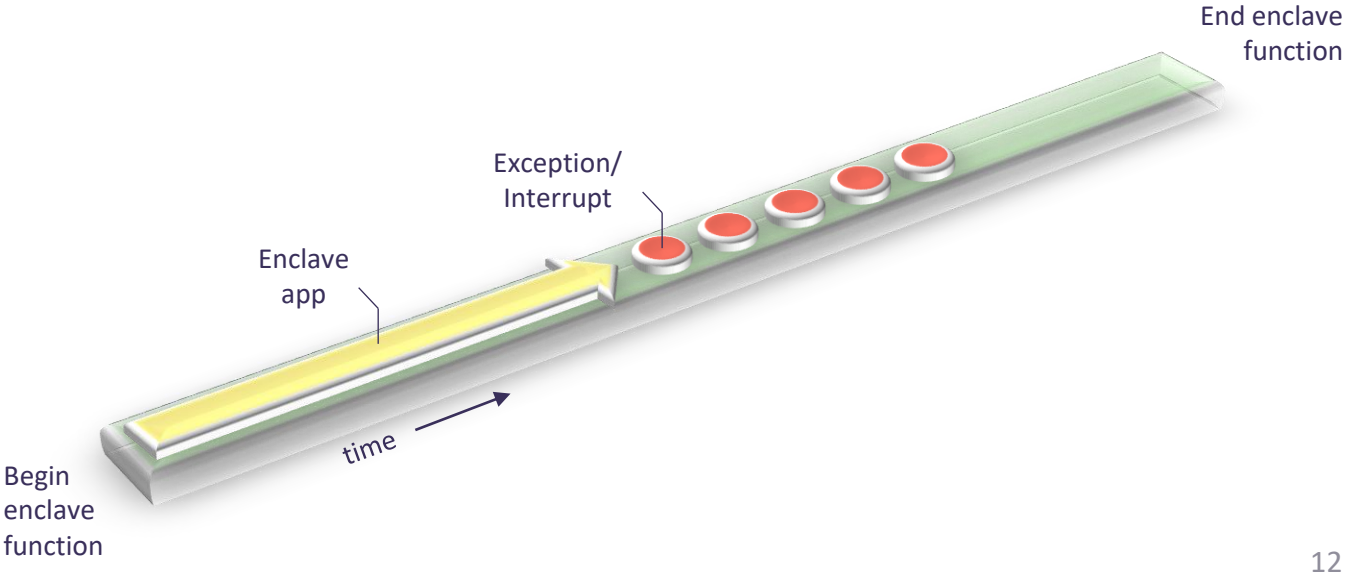
The OS/VMM might induce frequent **exceptions or interrupts** to try to amplify side channel data inference…



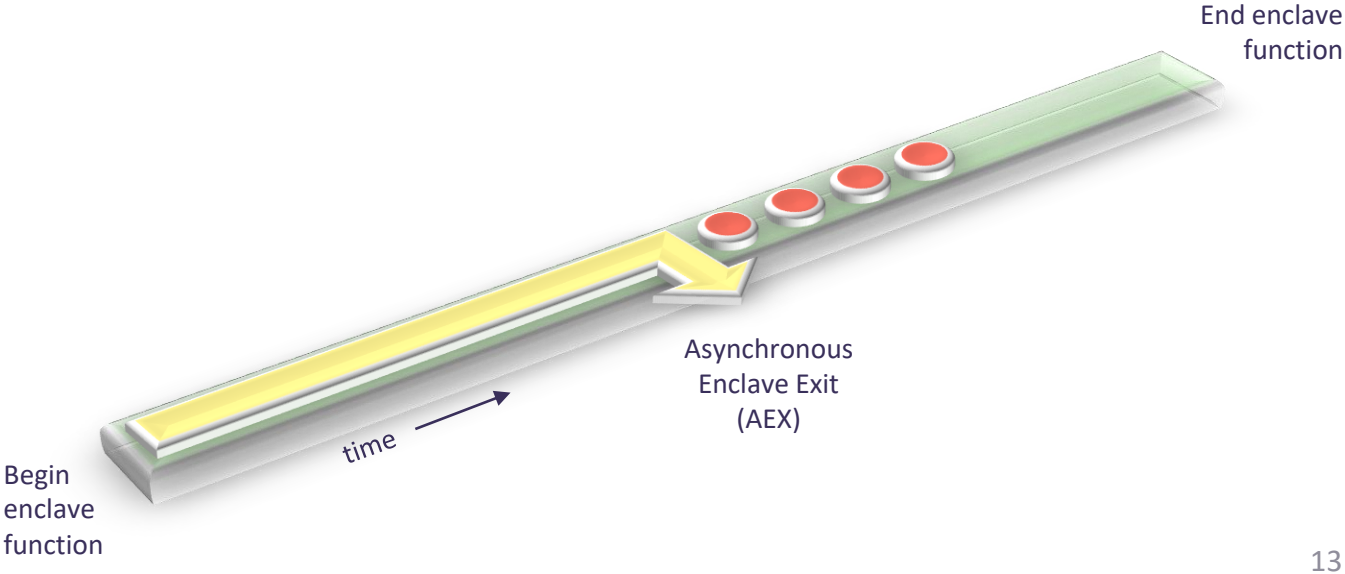
…or try to maliciously **single-step** or **zero-step** enclave execution

How can AEX-Notify help?

How can AEX-Notify Help?

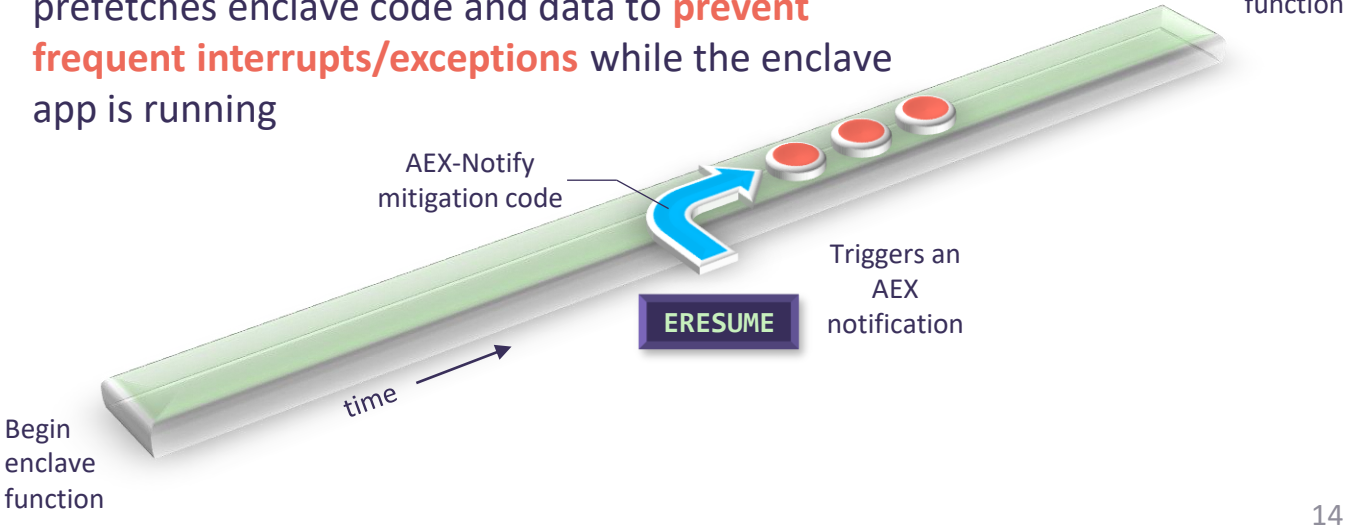


How can AEX-Notify Help?

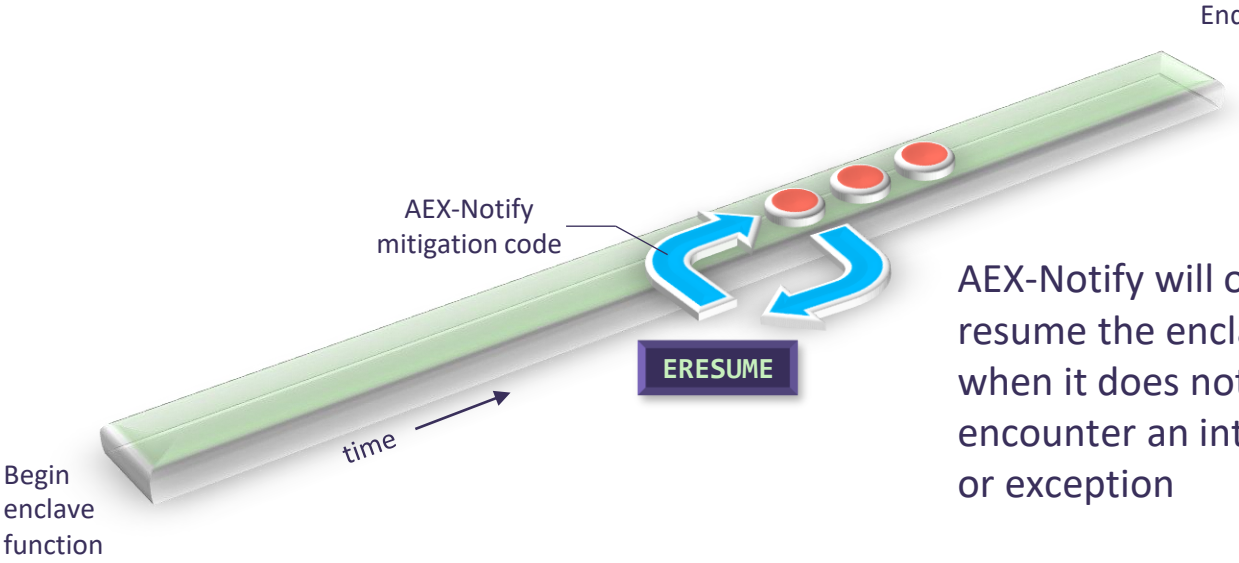


How can AEX-Notify Help?

AEX-Notify preemptively triggers exceptions and prefetches enclave code and data to **prevent frequent interrupts/exceptions** while the enclave app is running



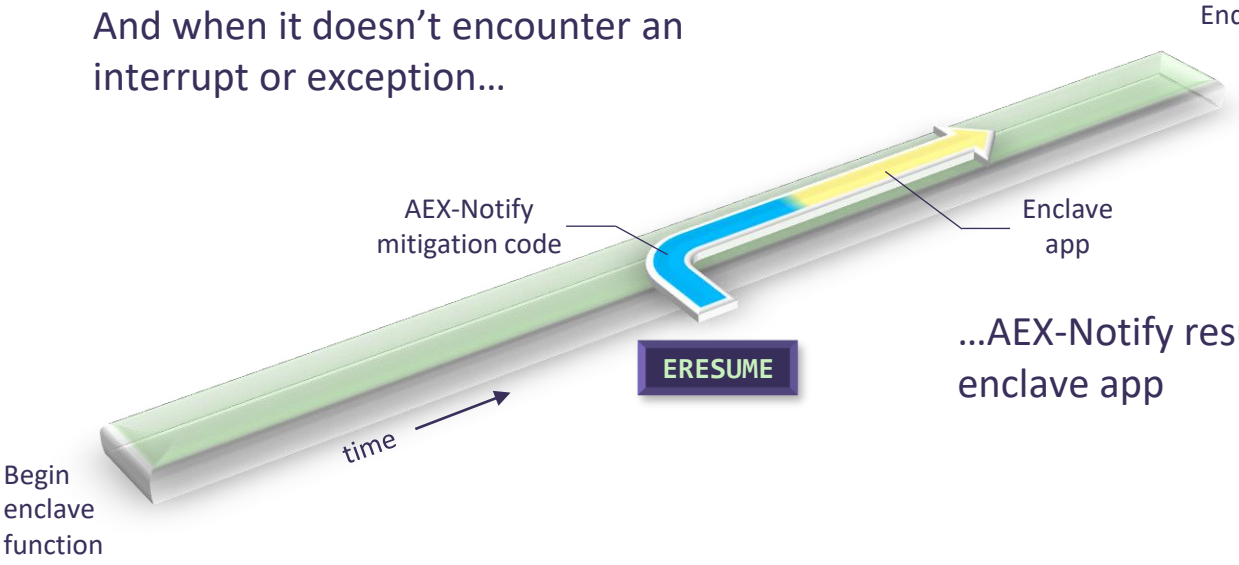
How can AEX-Notify Help?



AEX-Notify will only resume the enclave app when it does not encounter an interrupt or exception

How can AEX-Notify Help?

And when it doesn't encounter an interrupt or exception…



…AEX-Notify resumes the enclave app

What products support AEX-Notify?

AEX-Notify Availability

Currently available hardware:

- 5th Gen Xeon Scalable Processors (codenamed Emerald Rapids)
- These receive AEX-Notify via microcode update:
  - 3rd and 4th Gen Xeon Scalable Processors
  - All Xeon-E processors that support Intel SGX

Software support introduced in:

- Linux kernel, version 6.2+
- Intel SGX SDK for Linux, version 2.20+
- Gramine support coming soon

Summary and Additional Information

- AEX-Notify is a new Intel SGX feature that is used by the Intel SGX SDK to mitigate malicious single-/zero-stepping
- The single-/zero-stepping mitigation is implemented in software, and can be customized for other application-specific use cases
- AEX-Notify is available on all server processors that support Intel SGX
- AEX-Notify is an attestable enclave feature
- The single-/zero-stepping mitigation does not require additional enabling in software
    - For example, this mitigation can be enabled in the enclave manifest file

Notices & Disclaimers

- Intel technologies may require enabled hardware, software or service activation.
- Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.
- No product or component can be absolutely secure.
- Your costs and results may vary.
-