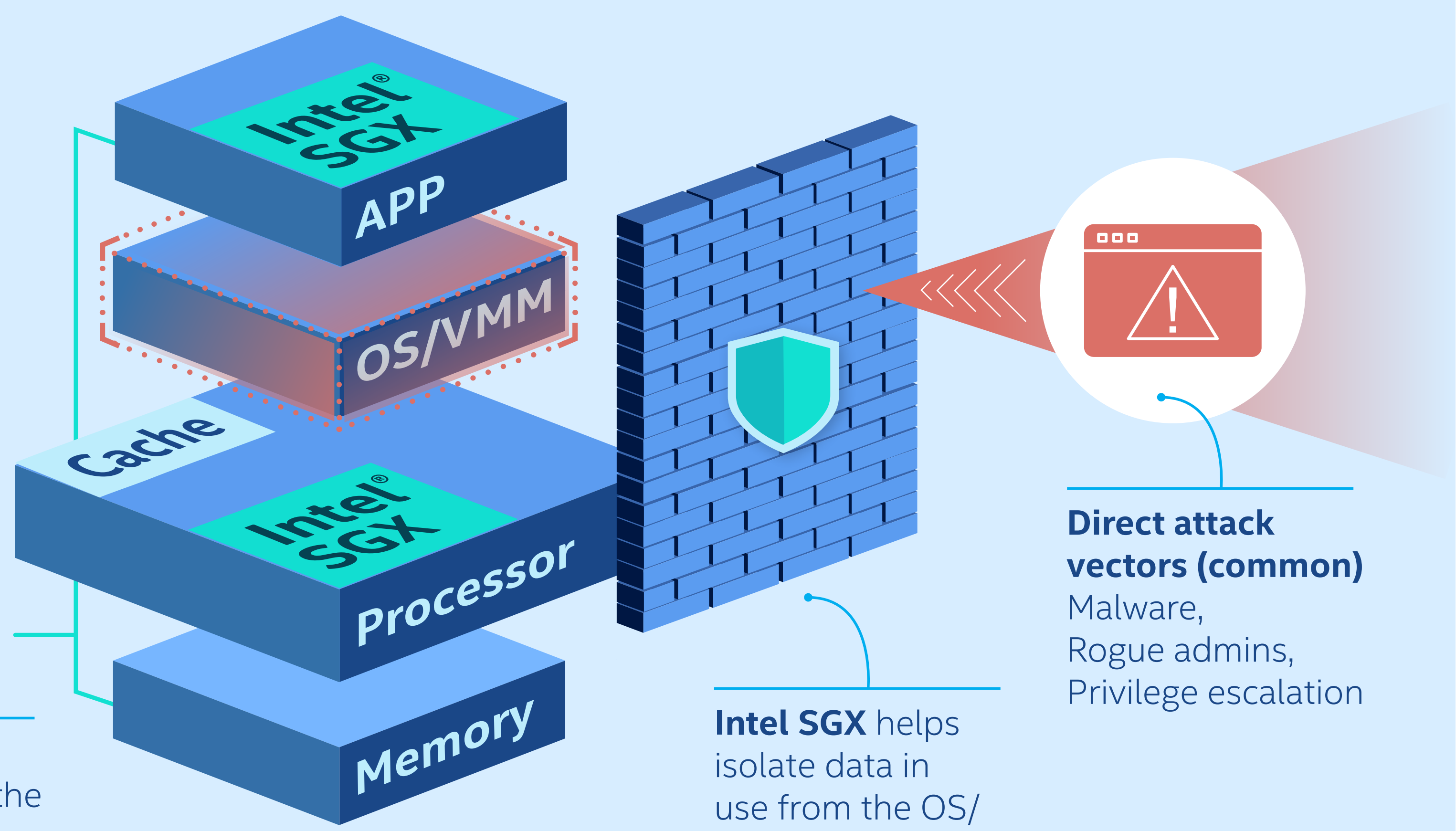
Intel® SGX: Moving beyond encrypted data to encrypted computing

1 How does Intel® Software Guard Extensions (Intel® SGX) help protect me from threats?

Intel SGX adds another layer of defense by helping reduce the attack surface

Intel SGX helps protect code and data from attack by malicious software and privileged escalations while that data is being processed.

Developers can create trusted execution environments (TEEs) directly within the processor/memory domain.



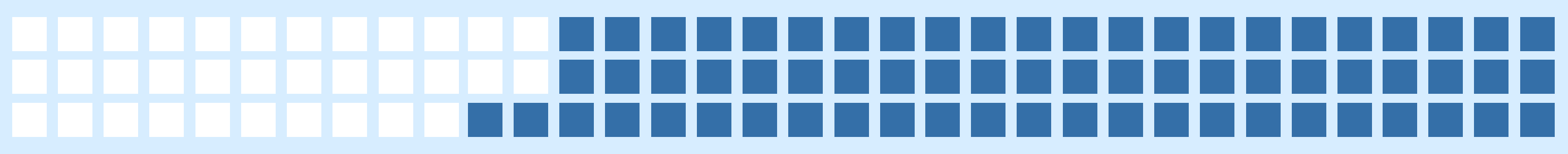
With Intel SGX, the app talks directly to the encrypted enclave on the processor, providing additional protection from potential threats targeting the OS/VMMs

Intel SGX helps isolate data in use from the OS/VMMs that are targeted by direct attacks

Direct attack vectors (common)
Malware,
Rogue admins,
Privilege escalation

The Common Vulnerabilities and Exposures (CVE) database lists more than **11,000** exploitable vulnerabilities in commonly used systems and software[1]

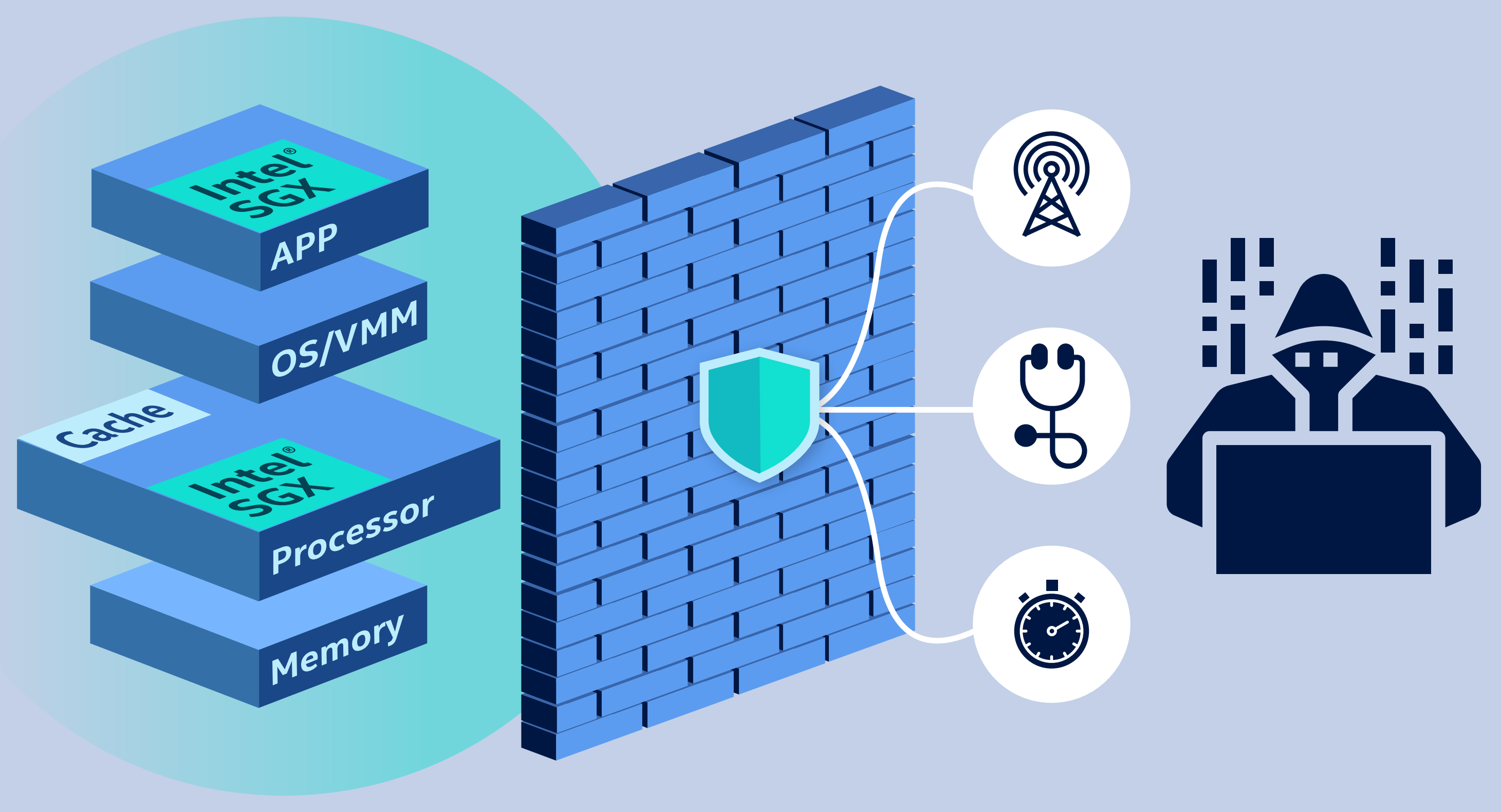
of these, **34%** don't yet have patches[2]



2 What about side-channel attacks?

Side-channel attacks are designed to gather external information from the processor such as power states, emissions and wait times in the attempt to infer data activity and values.[3]

Hackers typically follow the path of least resistance. Today, that usually means attacking software. While Intel SGX is not specifically designed to protect against side channel attacks, it provides a form of isolation for code and data that raises the bar for attackers.



3 Why should I trust Intel SGX?

How Intel SGX addresses security vulnerabilities

Collaboration
Ongoing collaboration with researchers and partners, including our founder role in the Confidential Computing Consortium, helps us identify and mitigate vulnerabilities quickly

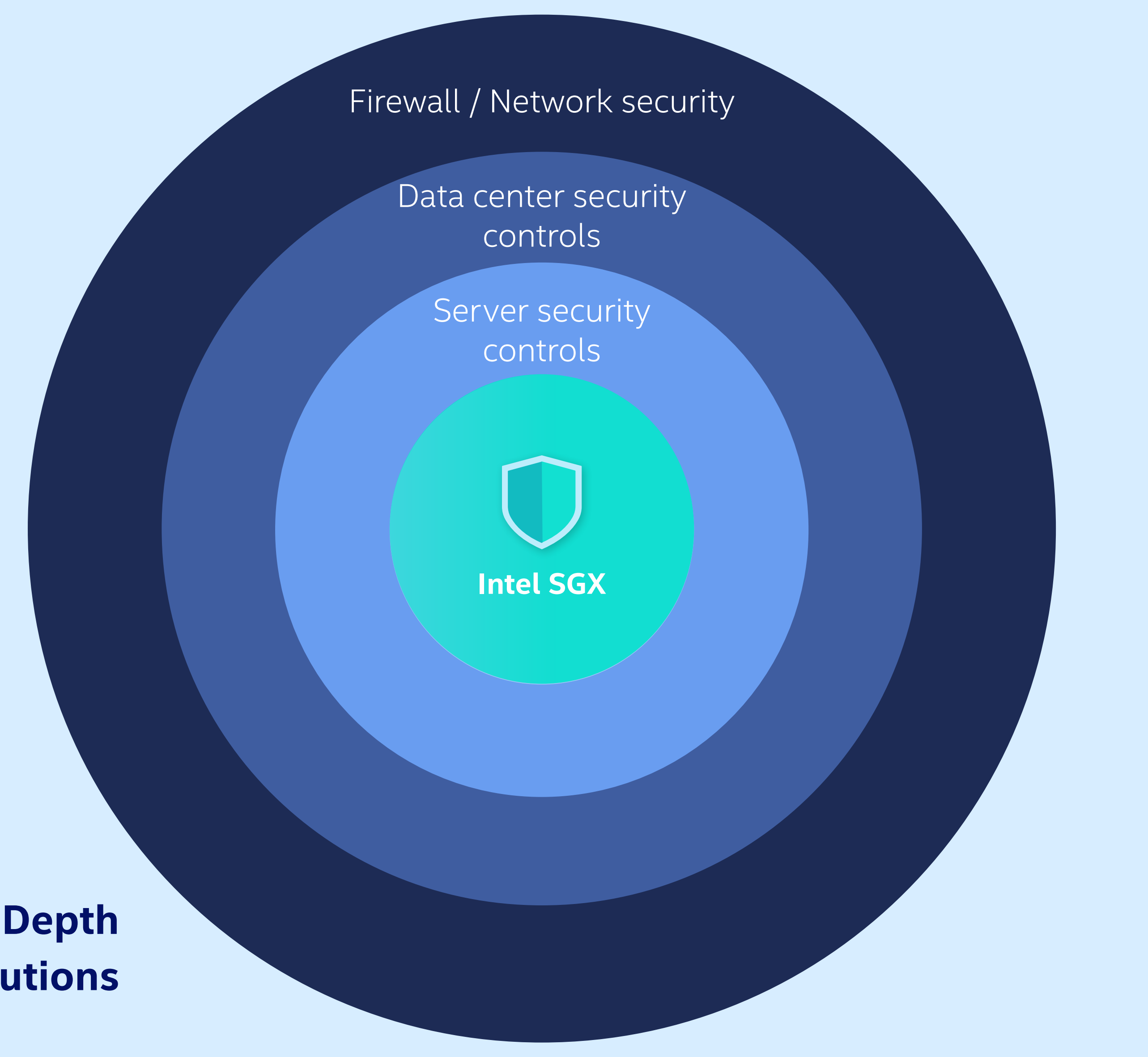
Hardened security
Intel SGX is designed to be regularly updated to be continuously hardened against attacks

Verification
Intel SGX enables applications to request verification that they are running on patched and uncompromised systems

Intel SGX protects against **thousands**[4] of known and unknown threats, many of which still do not otherwise have mitigations.

Intel SGX is the most tested, researched and deployed hardware-based data center TEE, with the smallest available attack surface within the system.

Intel SGX is already relied upon by security leaders in industries such as healthcare, financial services, government, and cloud services.



Defense-in-Depth Security Solutions

Although side channels will continue to be a vector of attack that Intel works diligently to mitigate, **your code and data remain significantly more protected with Intel SGX than without it.**

[1] https://cve.mitre.org
[2] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
[3] As of August 2020, hundreds of research papers have referenced Intel SGX.
[4] Intel SGX is not vulnerable to most OS layer threats, and there are over 140,000 threats in the database today. https://cve.mitre.org

0920/JS/CAT/PDF 344105-001EN