Bull

Unlock the value of your sensitive data while minimising risk

BullSequana SH, powered
by Intel® Xeon® 6

Security and sovereignty in the age of strategic computing

As organisations navigate the demands of mission-critical workloads, artificial intelligence, and real-time analytics, the need for secure, high-performance infrastructure has never been greater. Yet many enterprises face modernisation challenges - burdened by legacy systems, integration complexity, and rising operational costs.

In regulated sectors, (defense, public sector, finance, healthcare...) these technical hurdles are compounded by growing concerns around data protection and digital sovereignty. Ensuring that sensitive data is processed securely, remains under control, and complies with local regulations has become a strategic imperative.

Bull addresses these challenges with **BullSequana SH powered by Intel® Xeon® 6** - a platform engineered and assembled in Europe, designed to meet the highest standards of cybersecurity and sovereignty. Built on a secure-by-design approach, it combines full supply chain transparency, advanced hardware protection, and trusted execution technologies to deliver a scalable, regulation-compliant solution for Europe's most demanding industries.

Security by design: a holistic approach

At the heart of Bull's infrastructure offering, the BullSequana SH platform is engineered with a security-first philosophy. Its modular and scalable architecture is built to support the most demanding workloads while embedding advanced security mechanisms at every layer from the silicon to the system level. BullSequana SH integrates a comprehensive suite of protections to ensure data integrity, confidentiality, and resilience against evolving cyber threats.

Confidential Computing at the core:

BullSequana SH is built on the latest Intel® Xeon® processors and integrates advanced technologies such as Intel® Software Guard Extensions (SGX), Intel® Trust Domain Extensions (TDX), and cryptographic memory integrity. These features enable to create Trusted Execution Environments (TEEs), where sensitive data is processed in isolated enclaves - shielded from unauthorised access, even during execution. This approach ensures that confidentiality is preserved throughout the data lifecycle, supporting secure workloads in highly regulated environments (defense, public sector, finance, healthcare...).

What is Confidential Computing?

Confidential Computing is a security technology that protects data while it's being processed. Traditionally, data is encrypted when stored (at rest) or transmitted (in transit), but it can become vulnerable when in use (during computation). Confidential Computing fills this gap by using secured and isolated areas within the processor, encrypting data in memory and ensuring it remains protected even during processing, and preventing unauthorised access from the operating system or hypervisor.

End-to-end Chain of Trust

Security in BullSequana SH begins at the silicon level. The platform incorporates a secure boot process, firmware validation, and a hardware root of trust anchored in silicon. Public cryptographic Root-of-Trust keys establish a verifiable chain from hardware through firmware to the operating system, ensuring that only authenticated and trusted code is executed. This layered trust model prevents tampering and unauthorised modifications at every stage of the boot process.

Resilience through Trusted Execution Architecture

Bull's Trusted Execution Architecture (TEA) reinforces platform integrity by supporting secure detection, upgrade, and recovery mechanisms, as recommended by NIST SP 800-193 Platform Firmware Resilience guidelines. It is underpinned by a derivative of ProvenRun's ProvenCore, a micro-kernel formally proven and that has successfully gone through certification at the highest security level on Common Criteria (EAL7). It minimises the Trusted Computing Base (TCB), reduces the attack surface, and securely executes the above-mentioned services . Anchoring the Root-of-Trust within the Baseboard Management Controller (BMC), the system ensures secure recovery even in the event of firmware compromise.

Proactive threat mitigation

Security is not static. BullSequana SH benefits from continuous monitoring by Bull's dedicated Product Security Incident Response Team (PSIRT). This team actively identifies, analyses, and mitigates emerging threats, ensuring that the platform remains resilient against evolving cyber risks. This proactive approach complements the platform's secure-by-design philosophy, which embeds protection mechanisms from the earliest stages of development.

Choose European expertise, manufacturing and supply chain

BullSequana SH is designed and manufactured in Europe, embodying Bull's commitment to digital sovereignty and strategic autonomy. In an era where control over data and infrastructure is critical, this platform offers organisations full transparency and traceability across the entire supply chain - from component sourcing to system integration.

Control on the supply chain

By centralising production at Bull's industrial facilities in France, BullSequana SH ensures strict compliance with European regulations and export controls. This manufacturing approach not only reduces exposure to geopolitical risks and supply chain disruptions but also guarantees the authenticity and integrity of every hardware element, reinforcing the chain of trust from production to deployment.

Stringent quality control

Every component undergoes rigorous quality checks to meet high European standards, minimising risks associated with overseas supply chains, such as counterfeit parts or inconsistent manufacturing quality.

Comprehensive hardening processes

Security begins at the factory level, where each system undergoes rigorous hardening processes. These include network segmentation, default-deny firewall configurations, and strict access controls - measures particularly suited to industrial and regulated environments where any breach can have serious operational consequences.

Ensure compliance with European regulations

By aligning with both cybersecurity and environmental regulations, BullSequana SH enables organisations to meet their digital transformation goals while fulfilling their corporate social responsibility commitments. It is a future-ready infrastructure that supports not only operational excellence but also ethical and sustainable growth.

Ensuring data sovereignty

The platform is built to meet the highest standards of data sovereignty, ensuring that sensitive information remains under control and is processed in accordance with data protection laws. This is particularly vital for organisations operating in regulated sectors such as healthcare, finance, defense, energy, automotive and critical infrastructure.

Compliance with cybersecurity frameworks

The platform adheres to key international and European cybersecurity frameworks, including ISO 27001 for information security management and IEC 62443 for industrial cybersecurity. These certifications ensure that BullSequana SH provides a robust foundation for risk mitigation, operational continuity, and legal compliance.

Environmental & safety standards

In addition to its sovereign design, BullSequana SH aligns with European environmental and safety directives. It incorporates eco-design principles to reduce energy consumption and carbon footprint, supporting customers in their sustainability goals while maintaining operational excellence.

This includes the use of energy-efficient components, optimised cooling systems, and a reduced carbon footprint in line with EU environmental directives.

Intel® Xeon® 6 processors also deliver better performance per watt compared to the prior generation. As a result, this improved efficiency can help organisations meet their sustainability goals.

BullSequana SH: a trusted infrastructure for Europe's strategic needs

BullSequana SH powered by Intel® Xeon® 6 offers a secure, sovereign, and high-performance platform tailored to the most demanding operational environments. Its secure-by-design architecture, rooted in European manufacturing and compliance, ensures that organisations can confidently manage sensitive data while meeting strict regulatory and cybersecurity standards.

By combining advanced hardware-based protections, confidential computing capabilities, and proactive threat monitoring, BullSequana SH delivers robust resilience against evolving cyber threats. Bull alignment with international certifications such as ISO 27001 and IEC 62443 reinforces its suitability for sectors where trust and reliability are paramount.

From healthcare and finance to manufacturing, defense, and public sector, BullSequana SH adapts to a wide range of mission-critical use cases. Whether supporting secure patient data processing, real-time financial analytics, or industrial control systems, the platform empowers organisations to innovate without compromising on security or sovereignty.

Notices & Disclaimers

- Performance varies by use, configuration and other factors. Learn more on the Performance Index site.
- Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details.
- No product or component can be absolutely secure.
- Your costs and results may vary.
- Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.
- Intel technologies may require enabled hardware, software or service activation.
- ©Intel Corporation. Intel, the Intel logo, Xeon and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Connect with us

bull.com

Bull is a registered trademark © Copyright 2026, Bull SAS – All rights reserved.