guardtime

Primer on Guardtime

Why work with us

www.guardtime.com

Guardtime solves one of the biggest problem areas in cyberspace today: trust, integrity and accountablility

We solve a multi-trillion dollar problem

With an estimated 95% of all enterprise networks having been compromised it is no surprise that every day the news headlines inform us of a new data breach, a new loss of intellectual property, more damaged reputations and increased legal liability.

The loss of intellectual property from Fortune 500 firms has been described as the biggest transfer of wealth in history. A study published jointly by the World Economic Forum and McKinsey in Jan '14 estimates the cost of ineffective cybersecurity to rise to three trillion dollars by 2020.

Our solution is called KSI and it is completely unique

The challenge with all modern security solutions is that there is no verification mechanism. Whether firewalls, anti-virus, sandboxing, IDS or multi-vector virtual execution you are given no choice but to trust that the security measures are working and hope for the best. Yet it only takes one successful breach or malicious insider to suffer a loss of your most critical intellectual property. Trust without verification is a failed strategy.

Guardtime's Keyless Signature Infrastructure (KSI) is the only solution that can provide exabyte-scale instrumentation for the digital assets on your network, whether binaries, configuration parameters, routing tables, data stores or events logs, giving you mathematical certainty that your infrastructure is in the correct state and alerting you when it is not. It is still impossible to prevent unauthorized acts but it is possible to have 100% detection and real-time mitigation.

KSI technology restores trust by providing accountability

Prior to the Internet the solution to the problem of lack of trust was verification. "*Doveryai no Proveryai*" is a Russian saying that was translated for Ronald Reagan and became his signature phrase "*Trust, but Verify*". This worked in the physical world because it was possible to have extensive verification procedures that enabled both sides to monitor compliance.

KSI enables the equivalent for digital society and is the basis for "attributable networks". You can choose to enter into an attributable network; you can still maintain your privacy; however, any unauthorized acts will be detected in real-time and you will be held accountable for your actions.

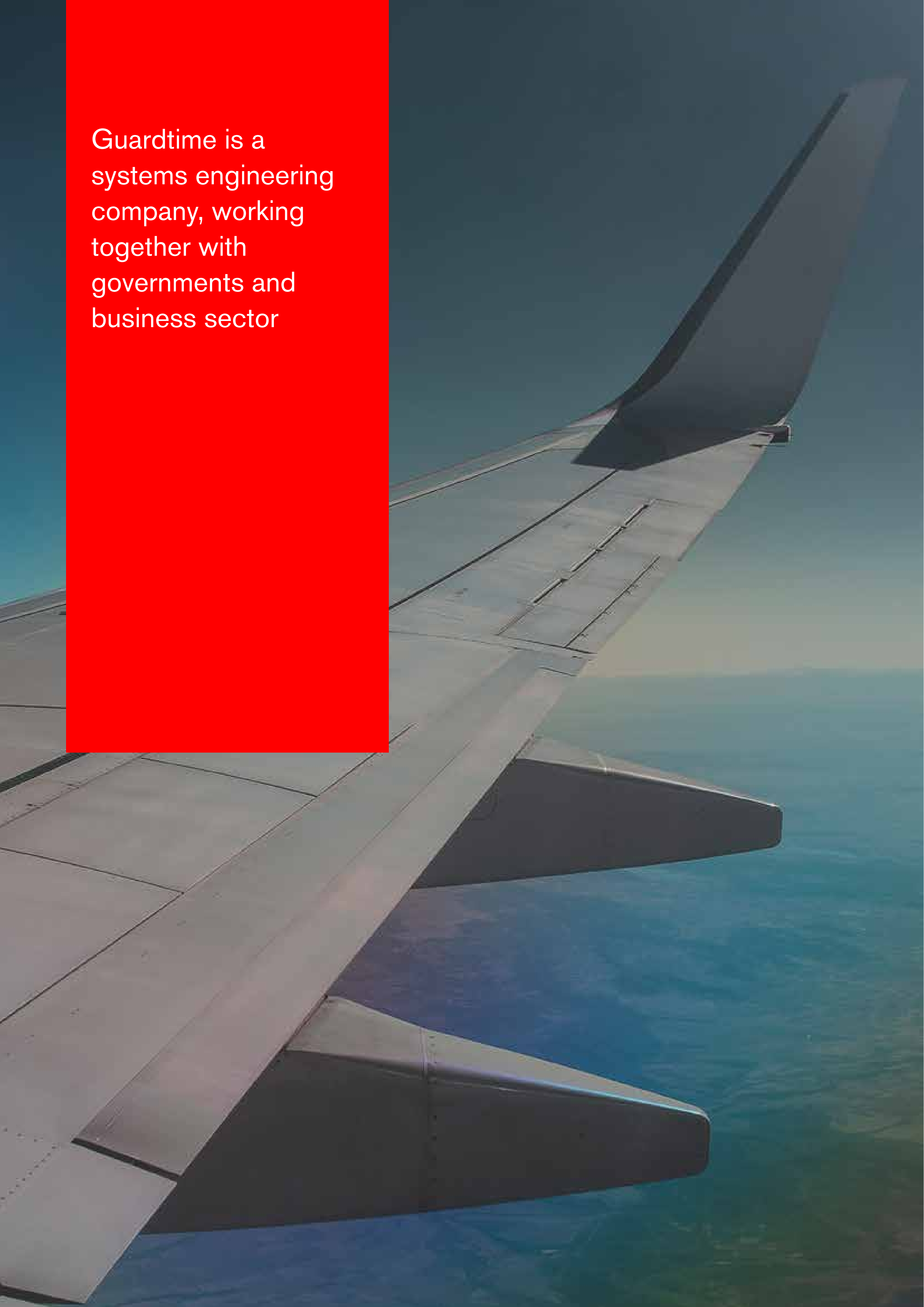
KSI technology was invented in the world's leading digital society

After suffering a crippling, prolonged national-scale cyberattack, Estonia recognized that a new approach was needed to restore and guarantee trust in digital systems.

Under the auspices of the Estonian Government and the small country's private sector, in 2007 a team of Estonian cryptographers, network architects, software developers and security specialists designed a digital signature system that could provide exabyte-scale real-time authentication for all the world's networked digital assets.

In Estonia Edward Snowden could not have committed his unauthorized act. With real-time monitoring of the integrity of digital events, his attempt to cover his tracks would have raised an alert and he would have been held accountable for his actions.

Guardtime is a systems engineering company, working together with governments and business sector



The world's leading researchers and cyber experts are on our team

Dr Ahto Buldas, our Chief Scientist, holds the chair of Information Security at the Tallinn University of Technology and is the lead inventor of KSI technology. He has published over 30 papers in the field and has spent over 10 years researching the theory behind the technology.

Matthew Johnson, our CTO, is a graduate of the United States Air Force Academy and a distinguished veteran of the United States Air Force with a focus on cyber security solutions for defense and cloud supporting national protection objectives for mission and information assurance.

We have strong government sponsorship and adoption

Our technology is being adopted by world governments, including in China, EU and the United States of America. We are actively working with accrediting authorities in all regions to ensure standardization of our technology across federal networks where deployment provides real-time authentication and monitoring for all digital assets, including firmware, software, configurations, data stores and event logs in compliance with regulatory risk management framework guidance (NIST SP 800-53, CNSSI 1253, and ICD 503).

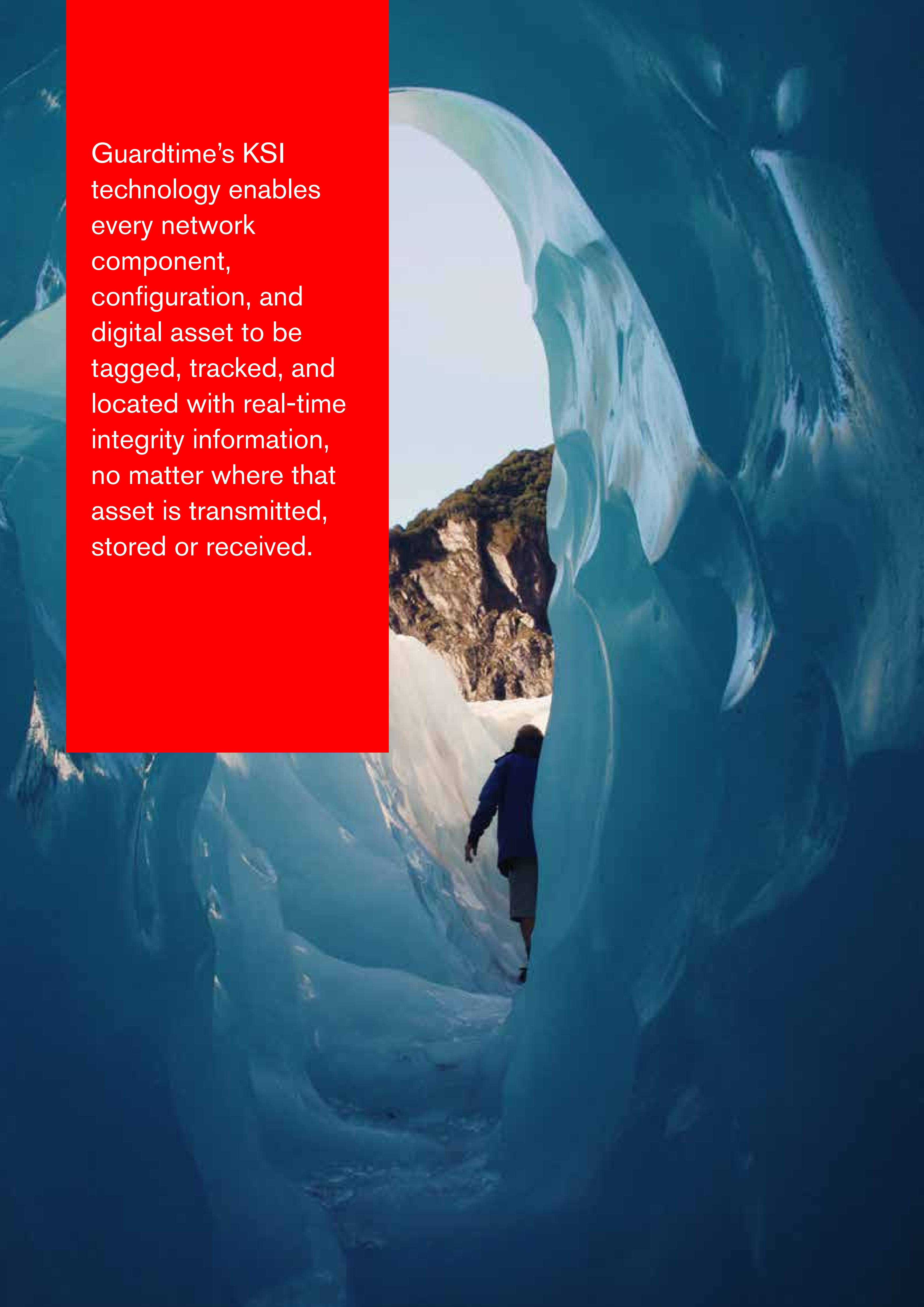
Our business model is to support the partner ecosystem

Guardtime does not have a sales force. We do not have a marketing department. We are a systems engineering firm that continues to develop the KSI technology stack, enabling the partners in our ecosystem to provide solutions built around our stack for their enterprise and government customers

We have a global, litigation-quality IP Portfolio

We have a robust and ever-expanding portfolio of issued patents and pending patent applications covering not only the KSI technology stack itself but also application-specific solutions.

Our lead IP counsel has more than 25 years of experience on three continents handling all aspects of intellectual property. Having started and while managing the IP program at VMware, he wrote the key, fundamental patents for the company's modern virtual machine technology and successfully defended those patents in litigation against Microsoft.



Guardtime's KSI technology enables every network component, configuration, and digital asset to be tagged, tracked, and located with real-time integrity information, no matter where that asset is transmitted, stored or received.

Attributable Networks

Attributable Networks mean that organizations can prevent data loss of important digital assets, assure the integrity of their network, and verify enterprise behaviors even across the service providers without having to put their trust in cryptographic secrets or systems administrators.

Every network component, configuration, and digital asset can be tagged, tracked, and located with real-time integrity, time and provenance information no matter where that asset is transmitted, stored, or received, at exabyte scale.

Exabyte scale integrity

Integrity is often defined as the absence of corruption, in systems, networks, processes and data. The base assumption for modern security is that it is impossible to prove the absence of corruption and therefore it is necessary to search for vulnerabilities.

The introduction of KSI however brings the scientific method back to the integrity of digital systems by giving a mathematical proof that systems and processes that make up a digital environment are free of compromise.

The implication is that if you can guarantee the state of your network, then any unauthorized change in the state of that network represents an attack, whether internal or external, which can be detected with 100% certainty. It is the difference between searching for needles in a haystack and having real-time situational awareness of every stalk of hay.

Scalability and carrier-grade availability

Our technology in a nutshell: It enables the state of networked digital assets to be independently authenticated and monitored at exabyte scale in real-time. To put this is practical terms, the infrastructure allows the validation of all the world's networked digital assets within a single second. That's every individual event in every log file, every data item in every data store and every configuration parameter on every switch and router on the planet.

Forensic auditability and portability of evidence

With electronic assets in large enterprise and government networks spanning hundreds of thousands, millions, or even billions of items, there is an urgent and growing need to keep track of the state and status of those assets and to constrain their activities. Until now, there has been no way to instrument the network at the scale required.

With KSI signatures attached to every digital asset, real-time instrumentation becomes possible providing proof of time, identity, and authenticity.

This proof affords the consumer, service provider, or data broker to finally trust the provenance and integrity of any network interactions and the forensic evidence of the signatures makes legal indemnification issues easy to resolve; highlighting who, what, where, and when a digital asset was touched, modified, created, or transmitted.

The evidence generated is portable across networks and the service providers who operate them.

Independent verification

Independent verification is probably the most important innovation in KSI. It means that the verification of an event in cyberspace can be verified without reliance on implementation of procedure, security of keys or any trusted human.

As a practical example consider the implications of a connected car involved in a collision. Who is liable: the driver, the vehicle manufacturer, the software vendor, the network hardware manufacturer, or the telco?

With independent verification there is no dispute as to exactly what happened when it can be verified without the need to trust any of the parties involved