

Guardtime solves a multi-trillion dollar problem with a unique technology

Guardtime solves 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.

Indeed, 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 January 2014 estimates the cost of ineffective cybersecurity to rise to three trillion dollars by 2020.

Guardtime has a completely unique solution

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 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.



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

Guardtime's KSI restores trust in business 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 "attributed networks". You can choose to enter into an attributed 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.

Guardtime's 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 immediate alert and he would have been held accountable for his actions.



World governments are adopting Guardtime's KSI technology

Guardtime has strong government sponsorship and adoption

Our technology is being adopted by world governments, including China, Europe 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).

Further Reading: <http://www.guardtime.com/governments/>

Guardtime's business model is to support our partner ecosystem

We do 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.



A litigation quality global IP portfolio built by leading cyber security experts

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

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.


Our CTO, Matthew Johnson, is a graduate of the United States Air Force Academy and a distinguished veteran of the United States Air Force Office of Special Investigations, where he served as a Special Agent focusing on cyber security, cloud, weapons development, intelligence, and related-security operations.

Guardtime has 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 highly profitable modern virtual machine technology and successfully defended those patents in litigation against Microsoft.

Further Reading:

<http://www.zdnet.com/the-estonian-cryptography-startup-that-wants-to-be-the-qualcomm-of-data-security/>



Exabyte Scale, Carrier Grade Availability

Exabyte scalability and carrier-grade availability

Guardtime's KSI 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 in practical terms, the KSI 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.

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.



KSI 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.

Guardtime's KSI: Summary

Guardtime's Keyless Signature Infrastructure (KSI) realizes the previously unobtainable dream of truly attributable networks. The KSI technology is today used across a variety of EU / US government agencies and commercial companies to tag, track, and locate (TTL) important organizational digital assets in real-time - subsequently proving their authenticity, time, provenance and associated identities.

The implications for any organization creating an attributable network is that they can prevent data loss of their digital assets, assure the integrity of their network, and verify enterprise behaviors even across service providers without having to put their trust in cryptographic secrets or administrators that may also be compromised (also known as the 'insider threat').

Strategically, Guardtime's KSI enables a new era in trusted networking and digital asset and content protection. Every component, configuration, and digital asset can be tagged, tracked, and located with real-time integrity information no matter where that asset is transmitted, stored, or received.