

guardtime 

# Cyber Risk and Blockchain Technology as a Mitigation Tool for Insurance

David Piesse  
Industry Adviser



guardtime 

# Introduction







# The MEGA Issue of Cyber Risk

Businesses and the economy need a predictable and deterministic environment to grow, where risk can be quantified and managed alongside investment and return.

The World Economic Forum believes the lack of functioning cyber security threatens as much as USD 3 trillion of non-realized potential growth during this decade.

If we are investing more but performing worse, something is fundamentally wrong with the approach we are taking as a society to cyber security.

# Why We are here?

Cybersecurity is an equal opportunity risk that does not respect borders.

Current security models are not sufficient.

Current insurance products are inadequate.



With increased connectivity there are no means to prove exactly what happened when.

To defeat the myth of a \$1000 lock for a \$100 bicycle

**There is a need to provides mathematical certainty, an independent audit trail for all human and machine activity in digital society in order to mitigate the risk and create opportunity from threat.**

# Chain of Truth over Trust – A Key Shift for the Future

TRUTH IN  
NETWORKED  
SOCIETY



Internet-of-Things  
Security

TRUTH IN YOUR  
BUSINESS



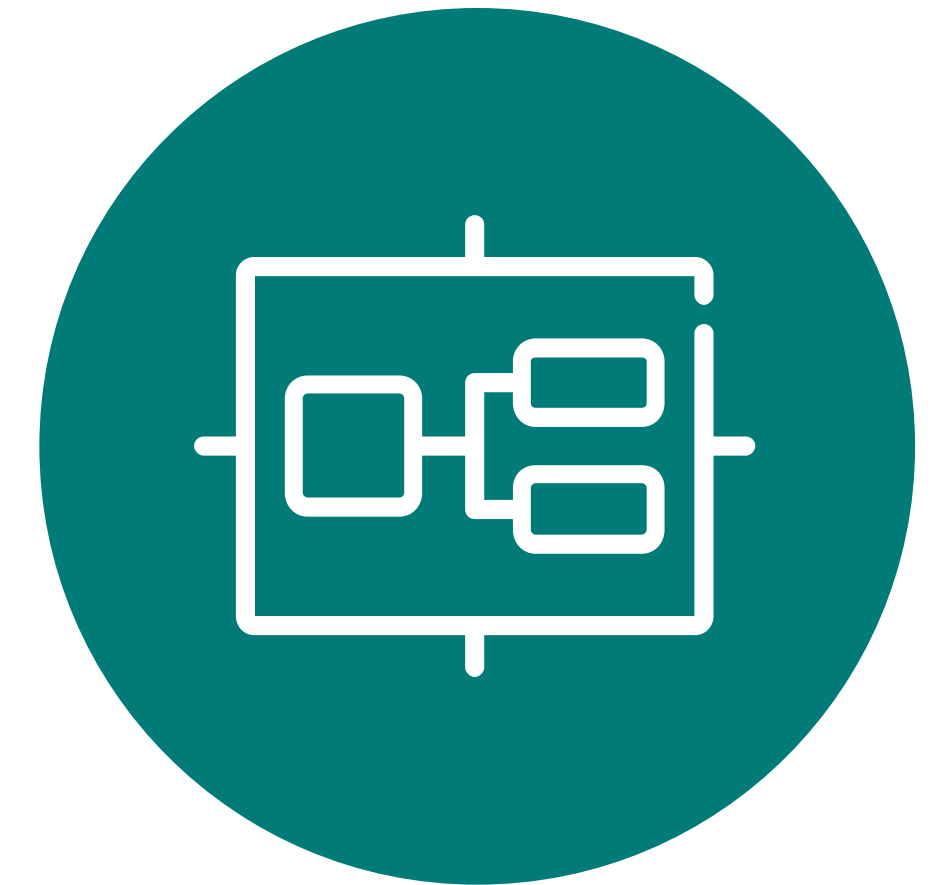
Cybersecurity

TRUTH IN  
YOUR DATA



Big Data Regulatory  
Compliance

TRUTH IN YOUR  
INFRASTRUCTURE



Industrial Infrastructure  
Assurance



## Why Do We Trust

**Trust is as, “firm belief in the reliability or ability of someone or something”. Trusting a network or the data stored in an enterprise or cloud service provider is nonsense without the basic instrumentation and metrics to develop a formal situational awareness into how reliable these assets really are and what they are doing with the data, services, and applications they are hosting.**





# The Quest for Digital Truth

**Truth on the other hand can be measured – it means undeniable independent proof, which can be proven forensically in a court of law. Truth, not trust is essential for any network, enterprise, or data storage asset.**

# Constraints to Cyber Risk Management



**The historical data does not reflect the current environment as in other risks.**

**Data is intangible making it difficult to quantify economic loss through data integrity breach.**

**Accumulation of cyber into one event is complex as IT companies outsource to each other with limited liability and recovery from third parties is difficult.**

**Current regulations are increasing the cost of handling the data breach including fines.**

**Solutions are currently after the breach and not pre-breach mitigation.**







# Estonia



**ESTONIA**



**RUSSIAN FEDERATION**

- Regained independence from Soviet Union in 1991
- 100% Electronic Banking
- 100% Electronic Health Care
- Over 1000+ Online Government Services
- i-Voting

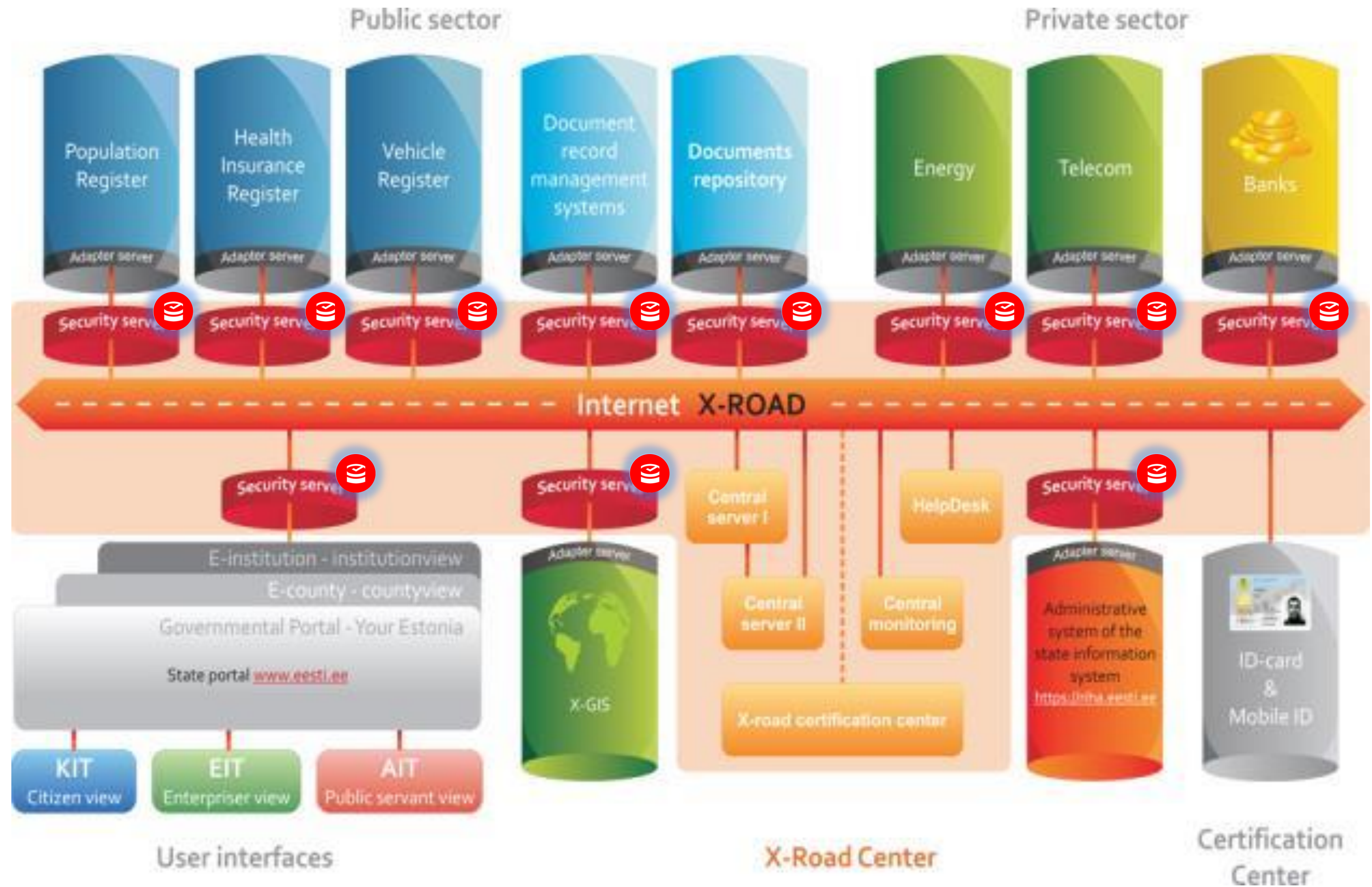
- 
- Victim of a worlds first State Sponsored Cyber attack in 2007
  - Headquarters of NATO Cooperative Cyber Defense since 2008



# Why Estonia succeeded in Digital Transformation

*Guardtime secures over a million Estonian healthcare records on the blockchain*

<http://ibt.uk/A6UXX>  
<http://coinde.sk/1LXm5F7>





# Data Embassy

OTTAWA  
NEW YORK

LONDON  
BERLIN

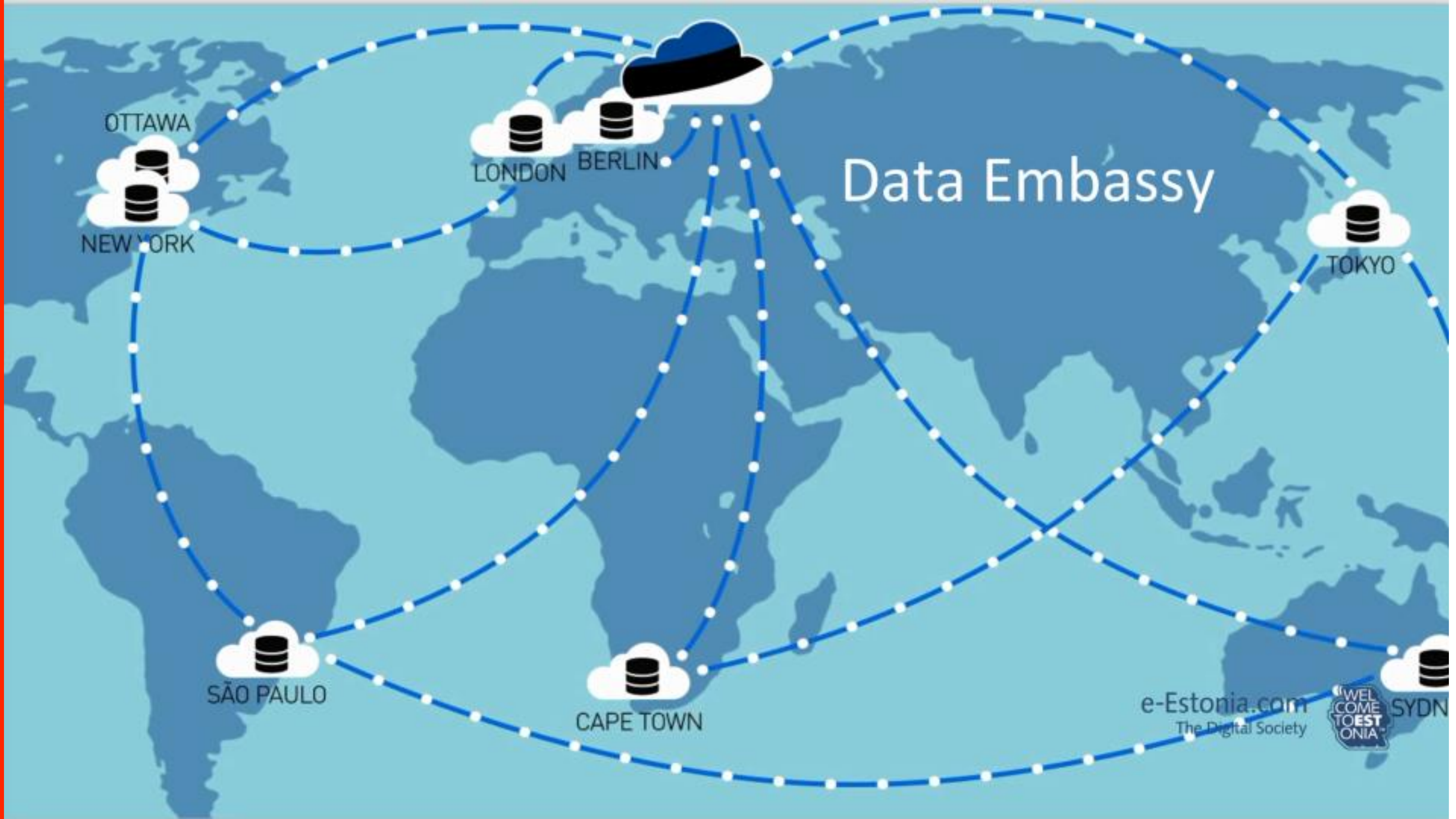
TOKYO

SÃO PAULO

CAPE TOWN

SYDN

e-Estonia.com  
The Digital Society







**What Estonia has implemented at the digital level is TRUST BUT VERIFY – independent verification of everything that happens in cyberspace.**

**Estonian scientists have built technology that allows the entire planet to verify EVERY event in cyberspace in such a way that the PRIVACY of each event is maintained but the integrity of events cannot be denied. These integrity technologies hold the promise to provide complete transparency – impossible for governments, corporations, or users to lie – everyone can verify the integrity of events independently from those presenting them.**



guardtime 

# The Problem



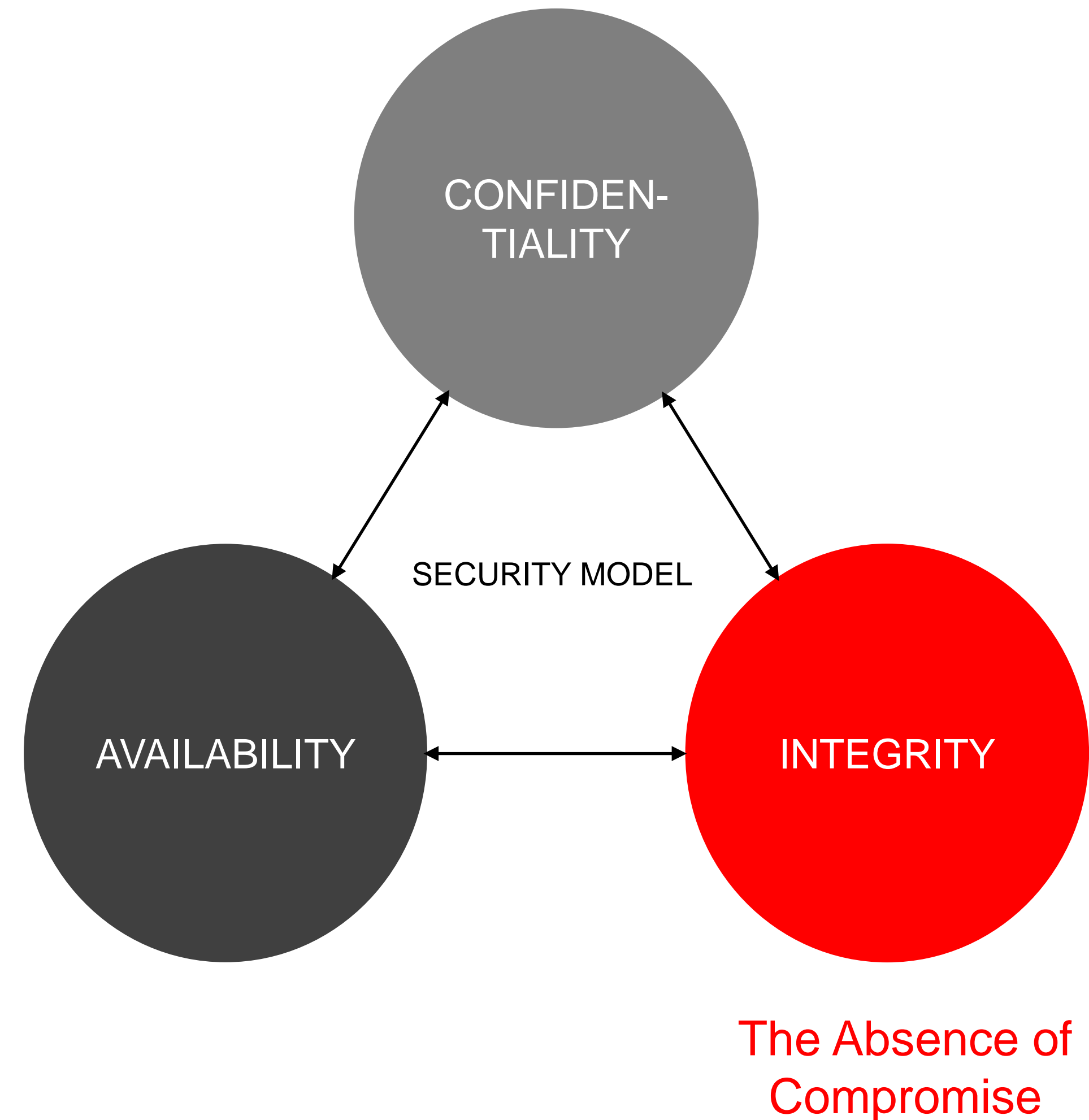


# Data Security: The Blockchain Killer App

The cost of ineffective cybersecurity is estimated at 3 trillion USD by 2020.

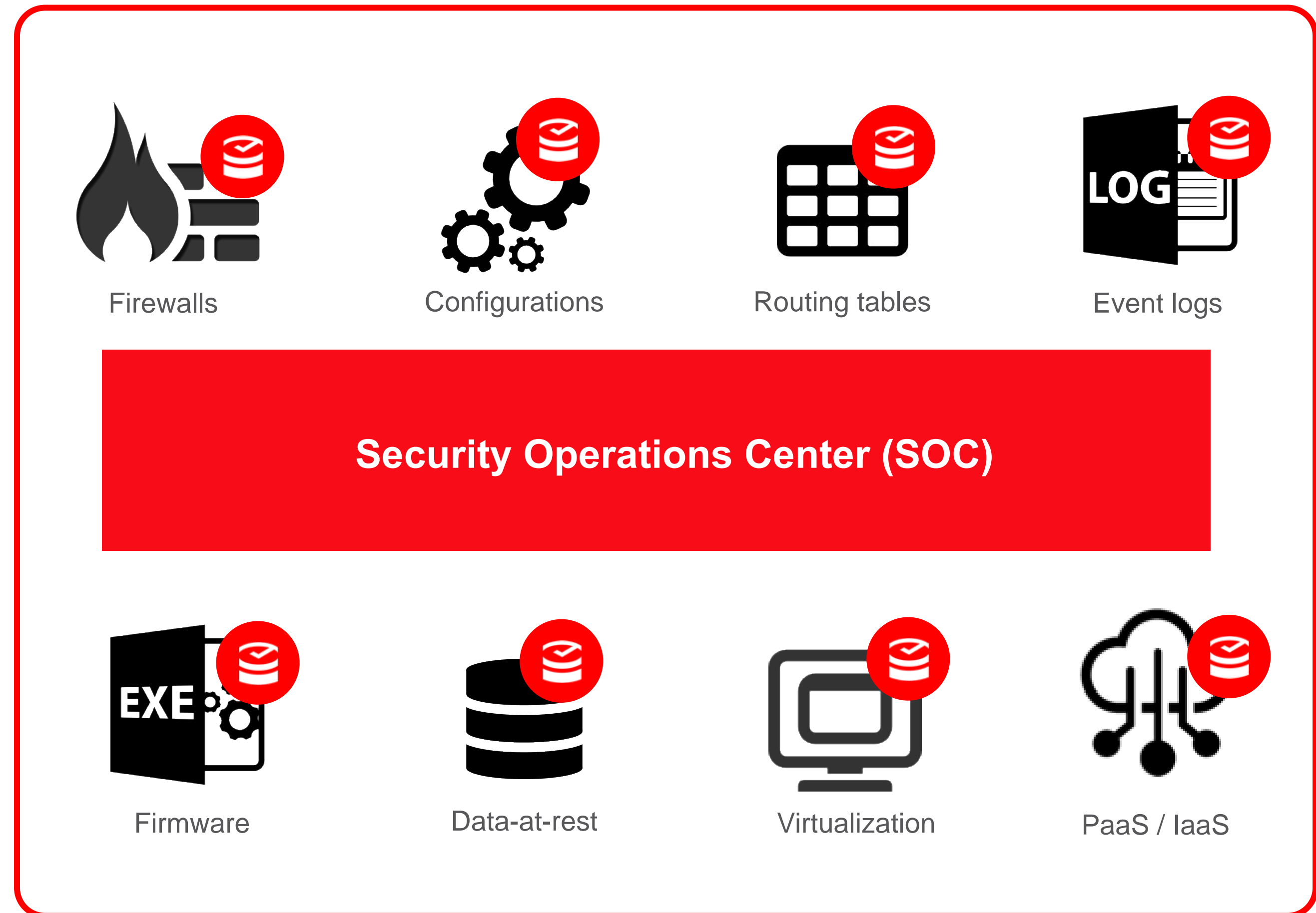
Our thesis and contrarian view is that the root cause for ineffective cybersecurity is the **lack of integrity** of systems, networks, processes and data.

Confidentiality is what you get when your systems have integrity.



# Attributable Internet : Enterprise Security

- Cybersecurity solution is based on continuous verification of the integrity state of Enterprise network, digital assets and data.
- By collecting, analyzing, correlating and reporting this evidence one can build an integrity snapshot of the network and important digital repositories and archives.
- Any unauthorized change in the integrity state represents an attack, whether internal or external, and can be detected with 100% certainty and accuracy.





## The Problem: Governance and Trust

***End-to-end systems have no representation of veracity at the digital asset level.***

1. How do I prove that vital data is authentic (original), reliable (tamper free) and from a credible source (known origin)?
2. How do I eliminate manual processes and establish automated mechanisms to ensure long-term integrity in my digital supply chain.
3. How can I prove chain-of-custody and provenance for vital data moving through my systems?

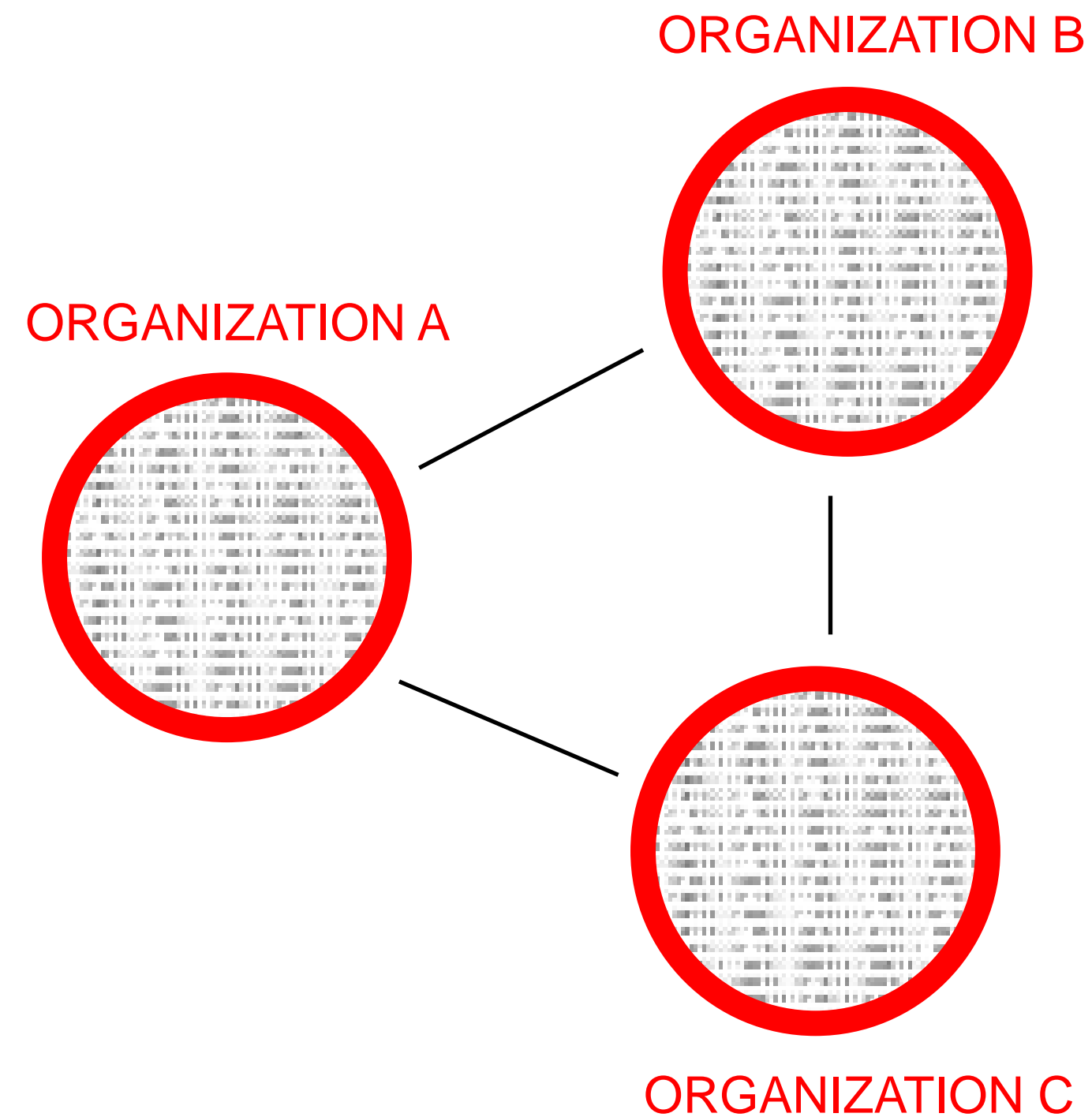
***Generally, “How do I trust my data, and how can I prove it?”***

# The Challenge



Based on the lessons learned from the 2007 state sponsored cyber-attacks Estonian scientists were set a challenge: **re-think information governance** by designing and building a massive scale signature system for electronic data which could prove the time, integrity and identity (human or machine) without reliance on centralized trust authorities.

# Historical Reasons Why Integrity Was Not a Focus



## PKI



PUBLIC KEY



PRIVATE KEY

Throughout the 1990s what mattered was confidentiality of data in motion – not the integrity of systems. With IOT, Cloud, mobile devices the **integrity** of systems and supply chains has come to the fore. PKI works for its original use case not for large scale system integrity.



# Why Does Integrity Matter ?

	<b>Integrity Breach</b>	<b>Confidentiality Breach</b>
<b>Your car</b>	Your braking system stops working	Your braking patterns are exposed
<b>Your flight</b>	Your plane's instruments report that you are 1,000 feet lower than you actually are	Your flight plan is posted on Internet (note: it already is)
<b>Your local power station</b>	Critical systems compromised leading to shutdown and catastrophic failure	Your electricity bill is published online
<b>Your pacemaker</b>	Shutdown and death	Your heartbeat becomes public knowledge
<b>Your home</b>	Your security system is remotely disabled	The contents of your fridge are 'leaked'. You drink how much beer?

## An Awakening to Integrity as a National Security Threat Vector

***“The most serious national security threat looming in cyberspace may be the potential for vital data to be altered by cybermarauders”***

– James Clapper, Director of National Intelligence (ODNI)

***“The newest cyberthreat will be data manipulation.”***

– Mike Rogers, Director NSA

**“Once integrity attacks start doing real damage -- once someone dies from a hacked car or medical device - there will be a real outcry to do something.... Again and again, we've tried to retrofit security in after the fact.”**

- Bruce Schneier, Researcher

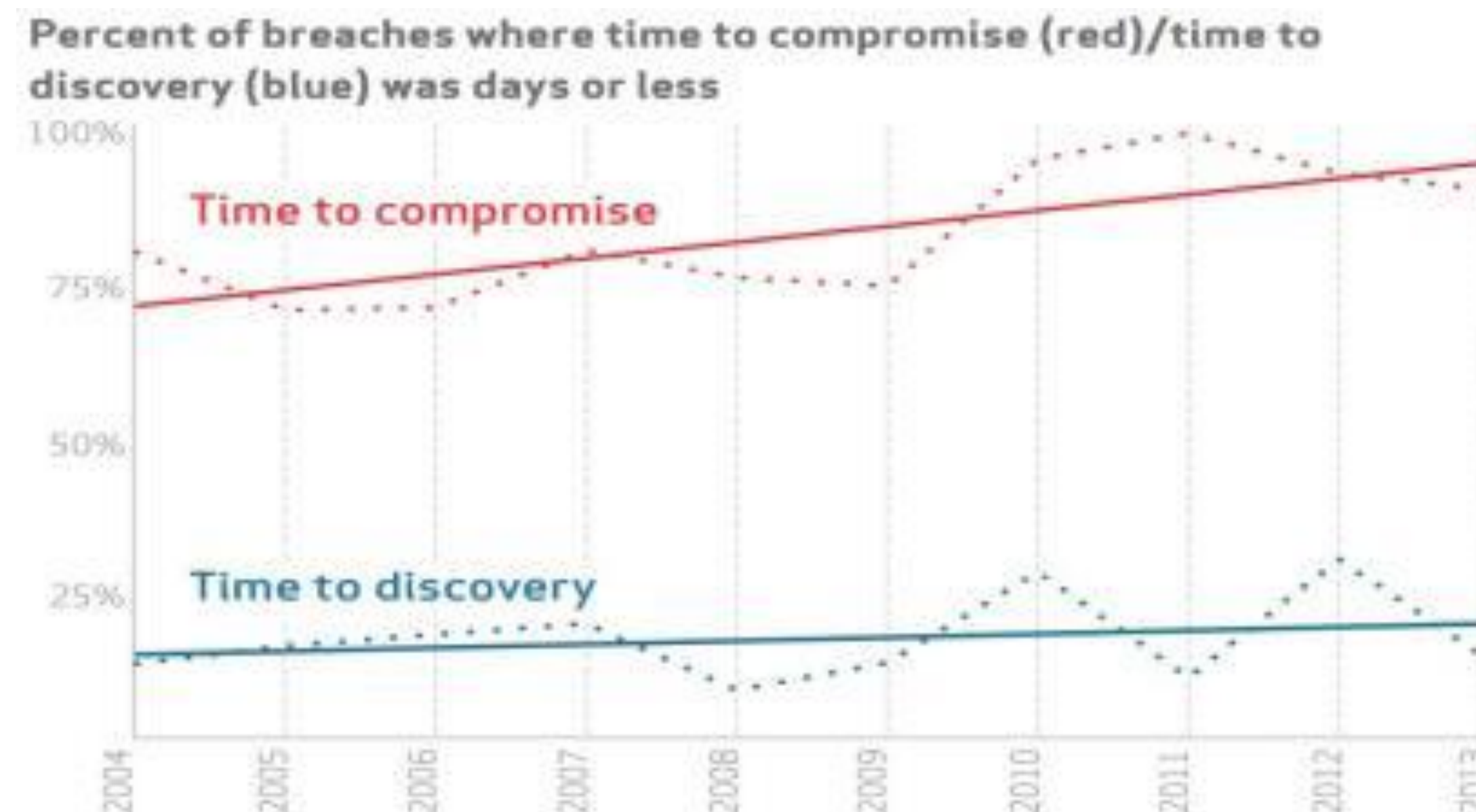


# Time to compromise vs. time to discovery

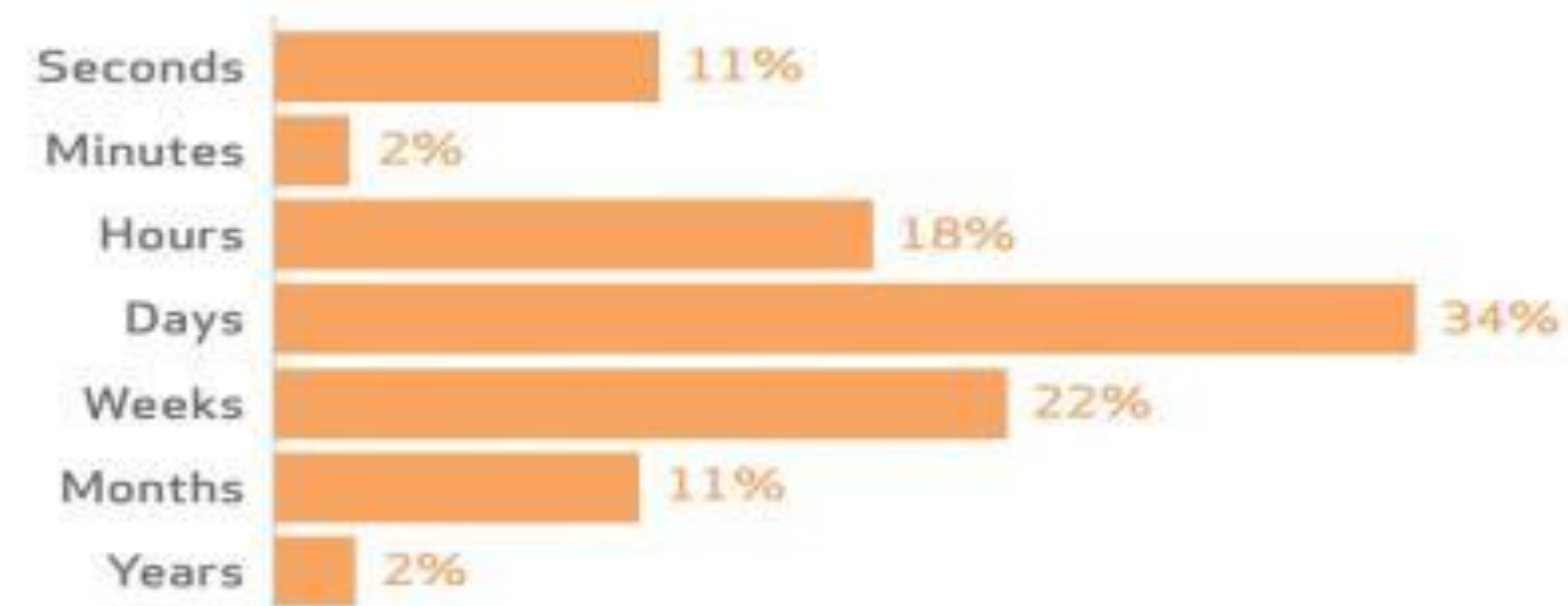
Over the last decade:

- Time to compromise has decreased, 90% less than a day
- Time to discovery has remained flat, only 15% found in less than a day
- For insider threat, 69% of compromise detections take more than a day; 35% take weeks or more

Source: 2014 Verizon Data Breach Report



Discovery timeline within Insider Misuse (n=1,017)



# Encryption is Not Good Enough – 6 Reasons

You cannot encrypt systems



You cannot audit encryption

Encryption gives a false sense of security

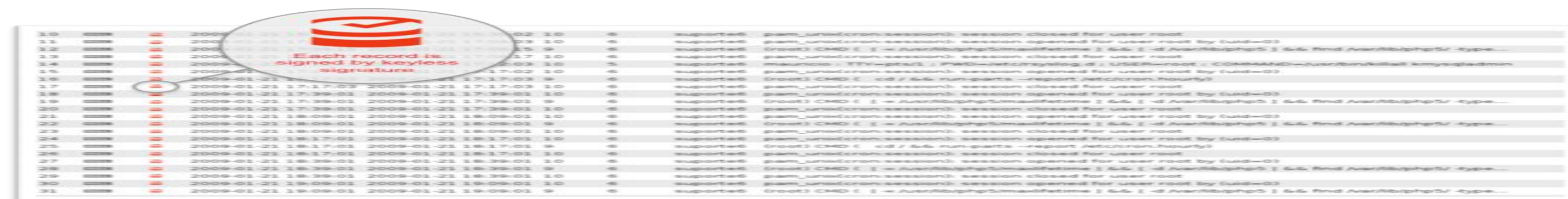


Encryption does not work against insider threat



Data Integrity is big threat in Cyberspace

You can't prove encryption works – “blood type”



**SILICON VALLEY MANTRA IS TO ENCRYPT EVERYTHING – INTEGRITY SHOULD PREVAIL**



**DIGITAL EVIDENCE IS LIKE LOOKING FOR A  
NEEDLE IN A HAYSTACK – Data in Motion Moves to Data  
At Rest.**



**ANSWER IS TO HAVE REAL TIME SITUATIONAL AWARENESS FOR EACH  
STALK OF HAY – CURRENT UNDERWRITING IS DONE ON PRIVACY**



guardtime 

# Solution





# Register Vital Digital Assets in the Blockchain

Keyless signatures (hash functions), linked to the blockchain, enable the properties of data to be verified without the need for trusted third parties, keys or credentials that can be compromised.



Upon verification, KSI Signature allows to assert:

- Registration Time
- Registration Entity
- Data Integrity



# Keyless Signature Infrastructure (KSI) – INDUSTRIAL BLOCKCHAIN

“Blockchain Consensus Model is the most important invention since the Internet itself and a much deeper concept than currency..”

**Marc Andreessen – Silicon Valley  
Entrepreneur and World Wide Web Hall of  
Fame**





# Separation of Blockchain and Bitcoin - the coin is not the chain

## Unbundling of a Bank



InsureTech



# What is Blockchain

- **Blockchain is a distributed ledger of all digital events in one place. It is distributed and shared by different parties.**
- **Only updated by a mutual consensus of the participants in the system.**
- **It is immutable and once entered the data cannot be erased.**
- **It was used as the technology behind Bitcoin but was around before BITCOIN – the COIN is not the Chain.**
- **There is no need to trust a central party.**
- **It will have impact on the back office and the mitigation of systemic risk for front office innovations.**



*bitcoin*



ethereum



**NXT**  
Cryptocurrency



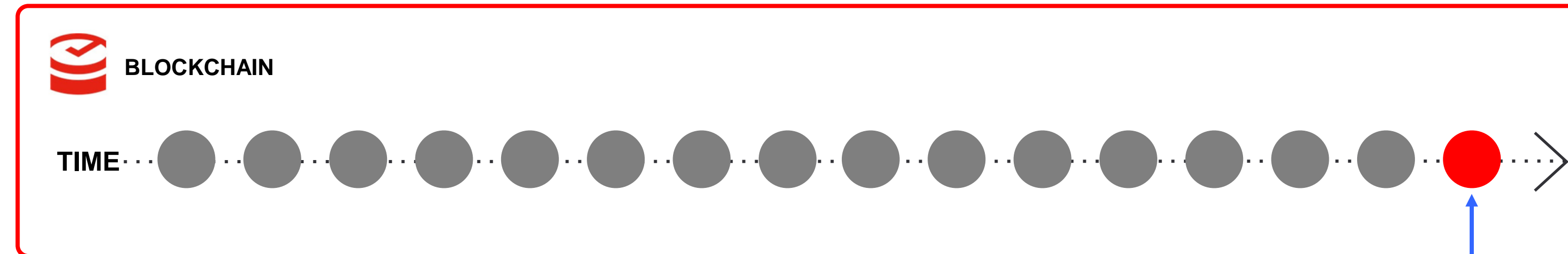


# MUTUALLY DISTRIBUTED LEDGER TECHNOLOGY (MDL)

- **LEDGER** is a place to record data.
- **DISTRIBUTED** means ledger is in different locations.
- **MUTUAL** means shared by consensus.
- **TECHNOLOGY** means a technical platform to execute a **MUTUAL DISTRIBUTED LEDGER**.
- That protocol is **BLOCKCHAIN**.



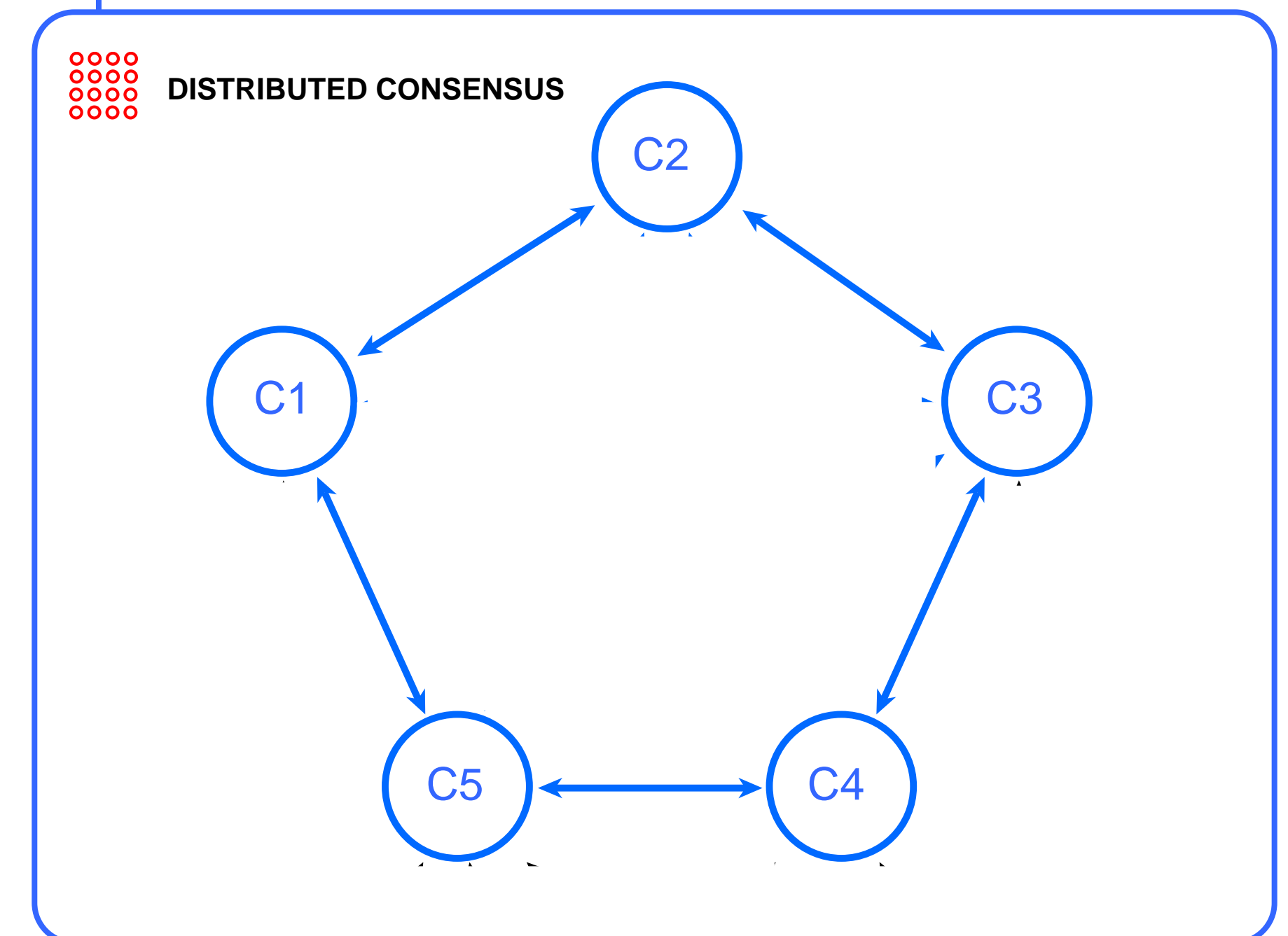
# Blockchain Principle



**“Blockchain” is a distributed database that maintains a continuously growing list of data records, chained together against revision and tampering.**

**“Distributed consensus” is an agreement between different compute-nodes over what is a true or false record**

**As every client has a copy of the blockchain it is impossible to manipulate information and cover up your tracks. The integrity and provenance of information systems can be mathematically proven.**





# Enabling Technology

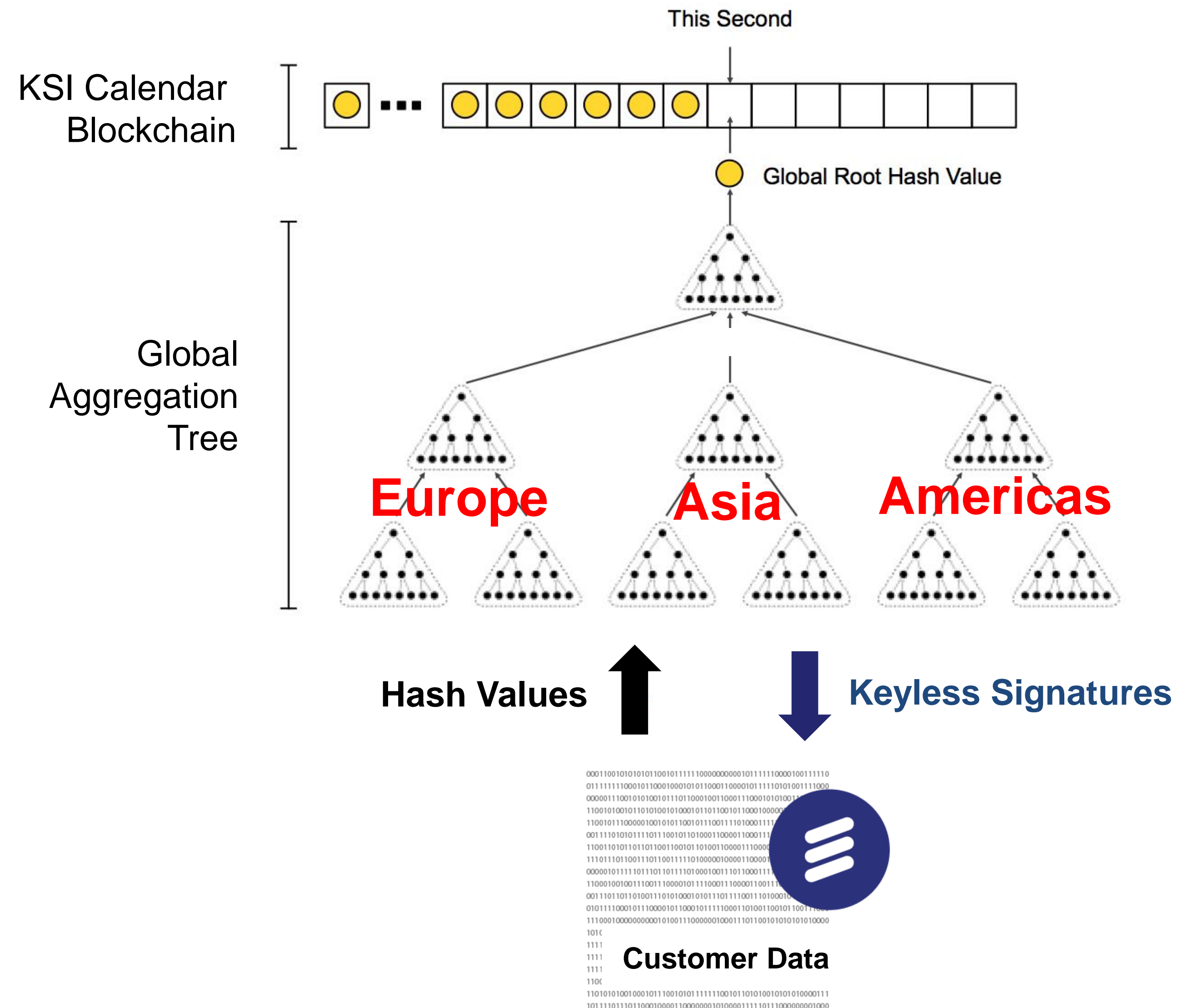
## keyless signature infrastructure (KSI®)

KSI® is a **blockchain technology** invented in Estonia

KSI is an emerging **global standard** respected and supported by governments, industries and moving into cyber-risk requirements for **data integrity**

KSI blockchain is a public ledger that provides proof of **time, integrity** and **identity** of electronic data.

Used by governments **since 2007**, KSI will be made available for global enterprises by Ericsson in 2015.







# Widely Witnessed Evidence

guardtime





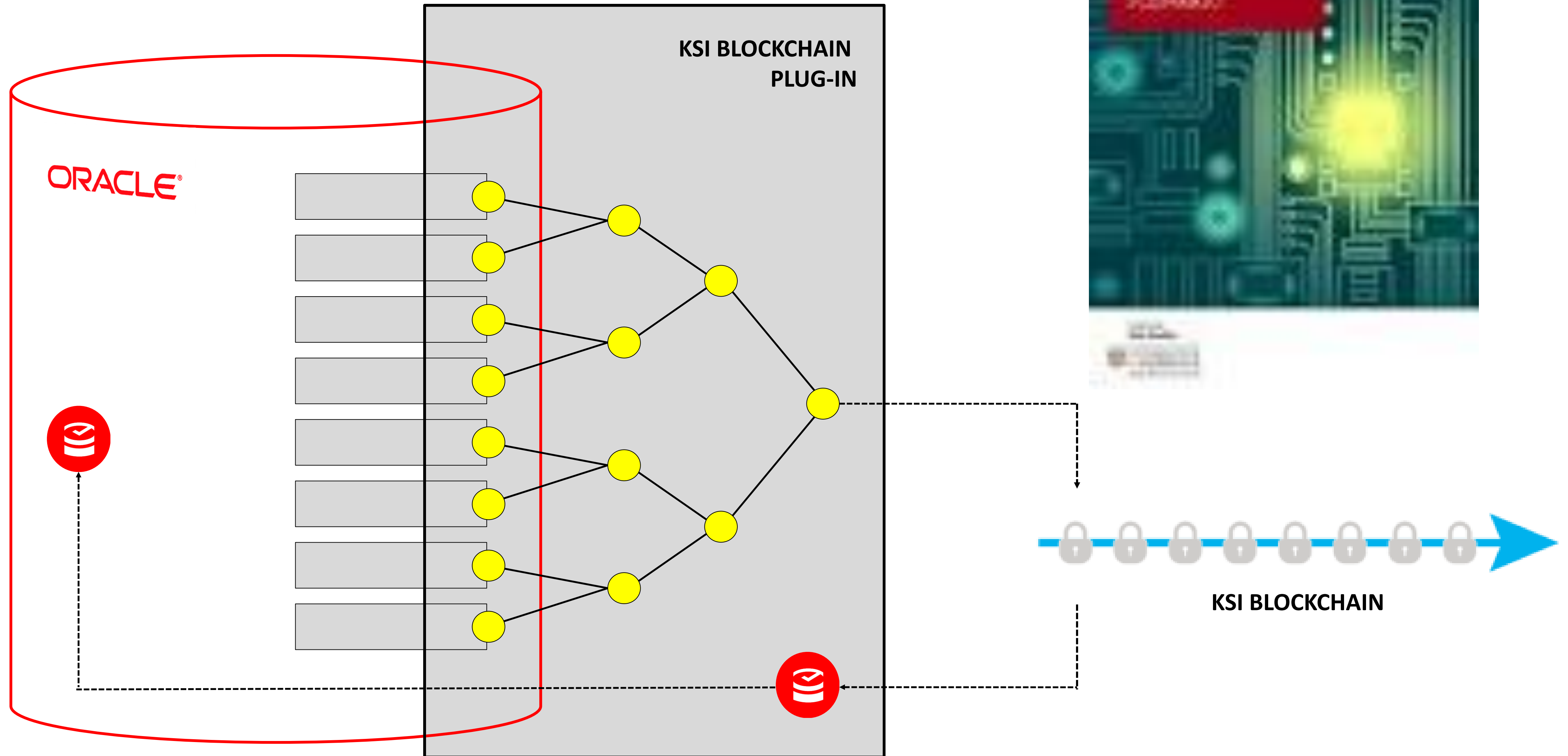
guardtime 

# IOT/BIG DATA





# KSI Blockchain Plug-in for Oracle Database



# Big Data Regulatory Compliance: Solution Benefits

**1.**

## **Know the 4W's of Big Data**

Know the who, what, where  
and when for your big data  
assets.

**Proof of Access**

**2.**

## **Blockchain Backed**

Built on industrial-scale  
blockchain technology for  
leading edge security.

**Proof of Ownership**

**3.**

## **Immutable Audit Trail**



Powered by a bullet-proof  
cryptographic audit trail  
designed for legal  
compliance.

**Proof of Lineage**

KSI Big Data Solution offers *veracity at scale* for  
Big Data assets based on industrial-scale blockchain technology



# Big Data Legal Hold

guardtime  +  Hortonworks

Enabling Big Data Regulatory Compliance

Legal Hold

Chain of Custody

Long Term Archival

E-Discovery

Data Assurance

Forensic Readiness

**Veracity at Scale for Data at Scale**

## Big Data Blockchain Concepts:

### 100% Accountability

Data events are captured and record time, integrity of asset, and signer origin.

### Immutable Ledger

Impossible for anyone to tamper with ledger and any data tampering can be easily detected.

### Universal Time Source

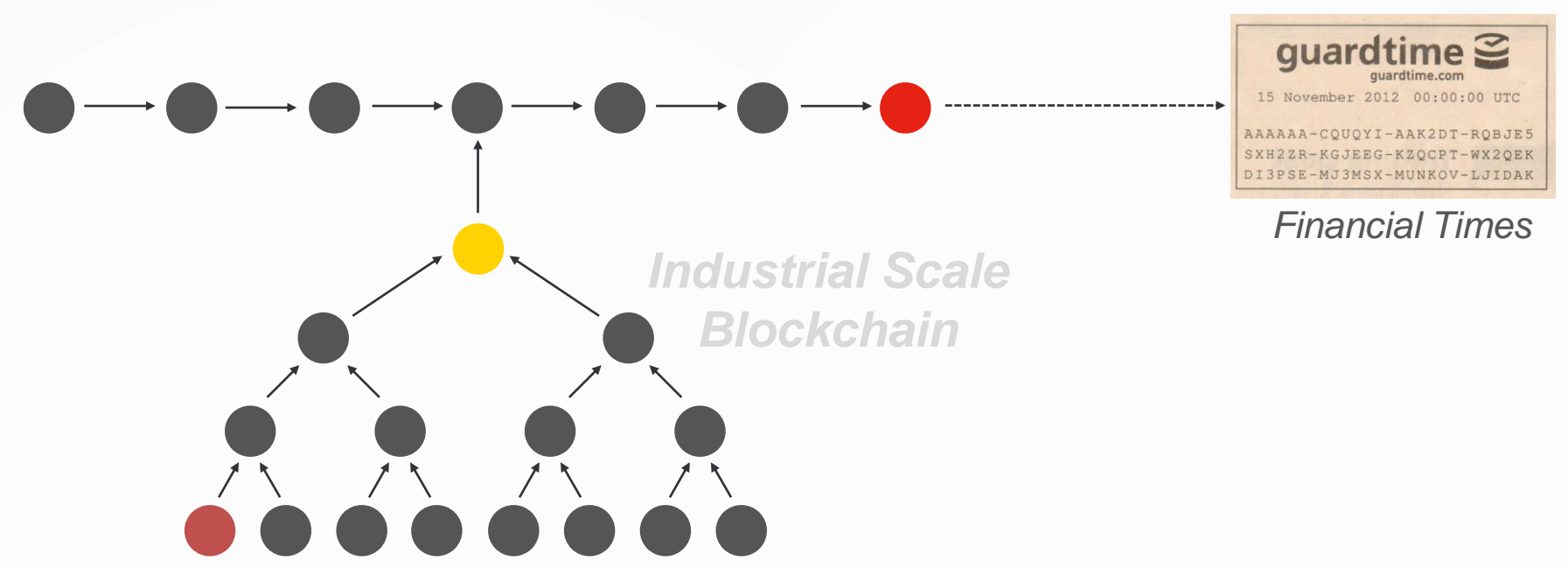
Time is an inherent property of the system so events can be unified across distributed systems

### Decentralized Consensus

Ability for auditors, law enforcement, or third parties to independently verify asset veracity.

# IoT Data Supply Chain Provenance


**Internet of Anything**



In-field Signing  
**SIGN DATA** 




HTTP

**guardtime**   
Central Blockchain Service

Digital Fingerprint + Metadata

HTTP

Enterprise Integration

Sign at Ingest  
**REGISTER DATA** 

**REGISTER DATA** 

Continuous Verification

**VERIFY DATA** 



**GOVERNANCE**

- Legal Hold & Archive
- e-Discovery / Forensics
- Chain-of-Custody

Data Provenance at Scale for Data Lakes and Surrounding Data Ecosystem

**Apache Hadoop**




Defensible End-to-End Lineage

## Capabilities

- Native Hadoop Integration
- Register at Ingestion
- Continuous Verification
- Indefinite Term Proofs
- Evidence Export
- Provenance Graph

CLOUD ENTERPRISE

**SOC**

Verify Externally  
**VERIFY DATA** 



Analysis & Insights

INTEGRITY  
AUTHENTICITY  
NON-REPUDIATION



guardtime 

# Case Studies





# CYBERLIABILITY MANAGEMENT

## use case: connected car

### Benefits:

› Real-time monitoring of the software and data uploaded to and / or executed on the connected vehicle.

› Forensic traceability of data in case of disputes – the ability to pinpoint liability, independent proof of what happened when.

### NETWORK ATTACK VECTORS:

ENTERPRISE

OEM

GRID

WEB

ROADSIDE

HOME

- ✓ Application and SW tamper events are detected in real-time.
- ✓ ECU reporting of compromise.
- ✓ Roll-back of SW & configuration to known trusted state.
- ✓ Real-time SW verification.
- ✓ Real-time tamper detection.
- ✓ Real-time mitigation and integrity monitoring of functions.



### SERVICES:

AV CONTENT

TELEMATICS

DIAGNOSTICS

ADAS

DSRC



# Critical Infrastructure Protection

- KSI used to ensure the management and control platform and networks for nuclear power sub-systems have integrity.
- <http://www.ibtimes.co.uk/u-k-nuclear-power-plants-protected-cyberattack-by-guardtime-blockchain-technology-1533752>





# Estonian National Health Care



**BUSINESS INSIDER UK** FINANCE

## Estonia is using the technology behind bitcoin to secure 1 million health records

Oscar Williams-Grut    
Mar. 3, 2016, 3:14 PM  1,485  1

[FACEBOOK](#) [LINKEDIN](#) [TWITTER](#) [EMAIL](#) [PRINT](#)

Guardtime, a startup that uses technology similar to that underpinning bitcoin to secure public and private data, has signed a deal with the Estonian government to secure all the country's 1 million health records with its technology.

The deal with the Estonian e-Health Authority comes alongside





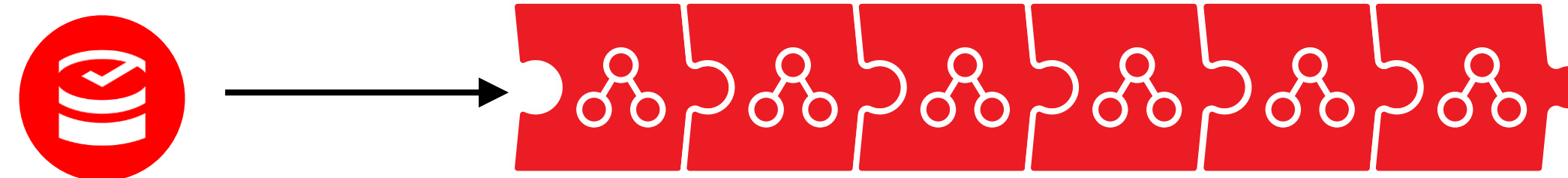




# Use Case: E-Healthcare in Estonia

**Goal is to solve several key problems for back-end healthcare record storage:**

- 1** To discover unauthorized changes, also those made by the insiders, and report them in a timely fashion.
- 2** To produce independent and legally sound proof of record for internal, external and regulatory compliance purposes.
- 3** Achieve the above capabilities across extremely large systems with terabytes of data and millions of records



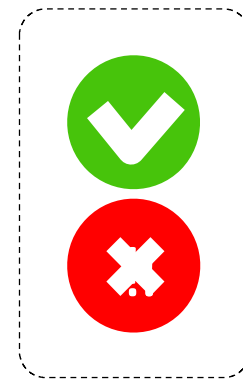
**KSI BLOCKCHAIN**



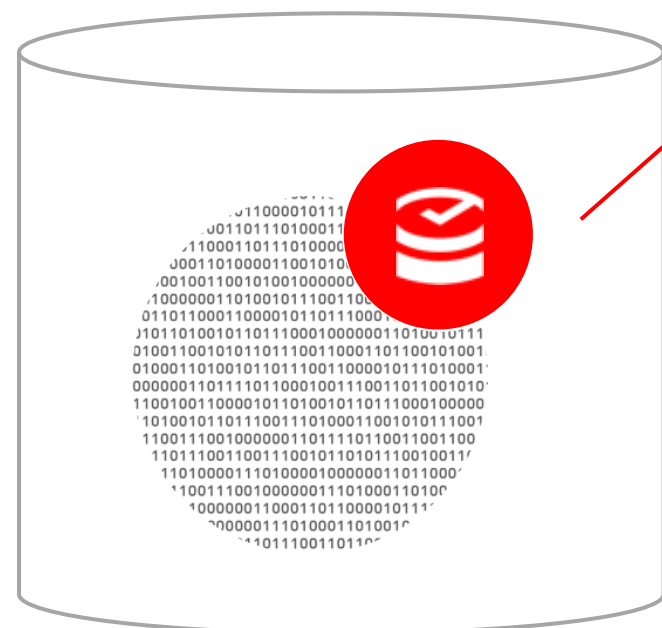


# IOT Provenance, Integrity and Assurance

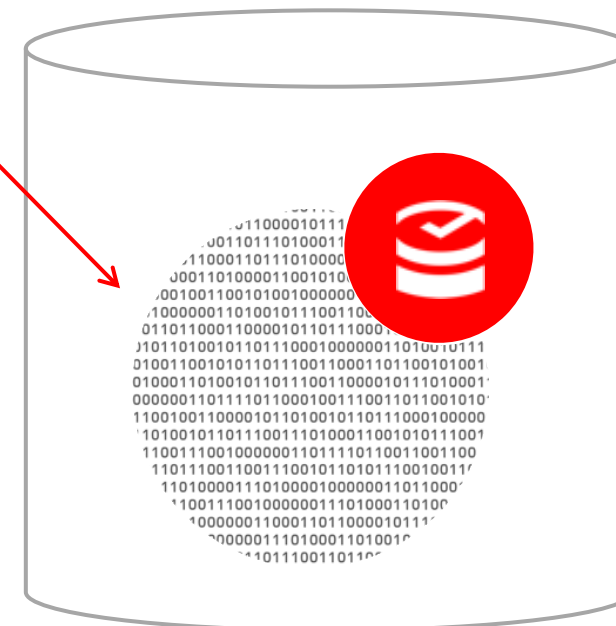
Uploaded executable code is verified on-board, in real-time and only valid code is executed.



Collected sensor data is signed in real-time during the mission and transmitted along with the integrity proof.



**Authorized executable code repository**



**Collected sensor data storage and archive**

## Benefits

- On-board, real-time verification of uploaded executable code makes it impossible to inject malware or otherwise tamper with authorized set of instructions.
- On-board, real-time signing of the collected sensor data provides complete tamper evident chain of custody from data capture to storage to long-term archiving.



# Critical Infrastructure: Telecom Core Networks

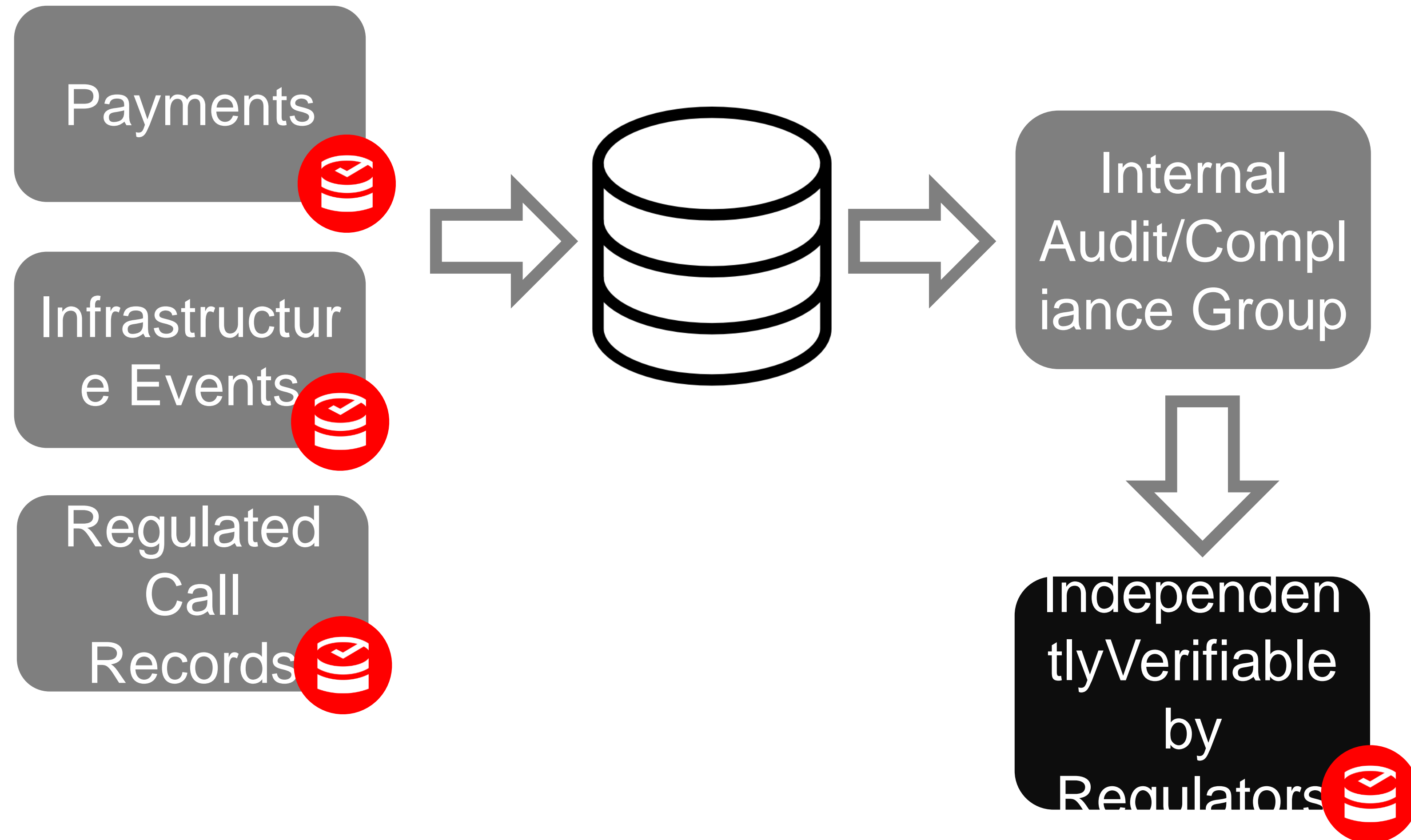
Real-time situational awareness and end-to-end provenance for critical infrastructure components

- Firmware
- Configuration
- Software
- Audit Compliance Logs



# SEB Bank payments

SEB Bank in Estonia use KSI to sign all payments, Infrastructure events, and regulated phone call data.

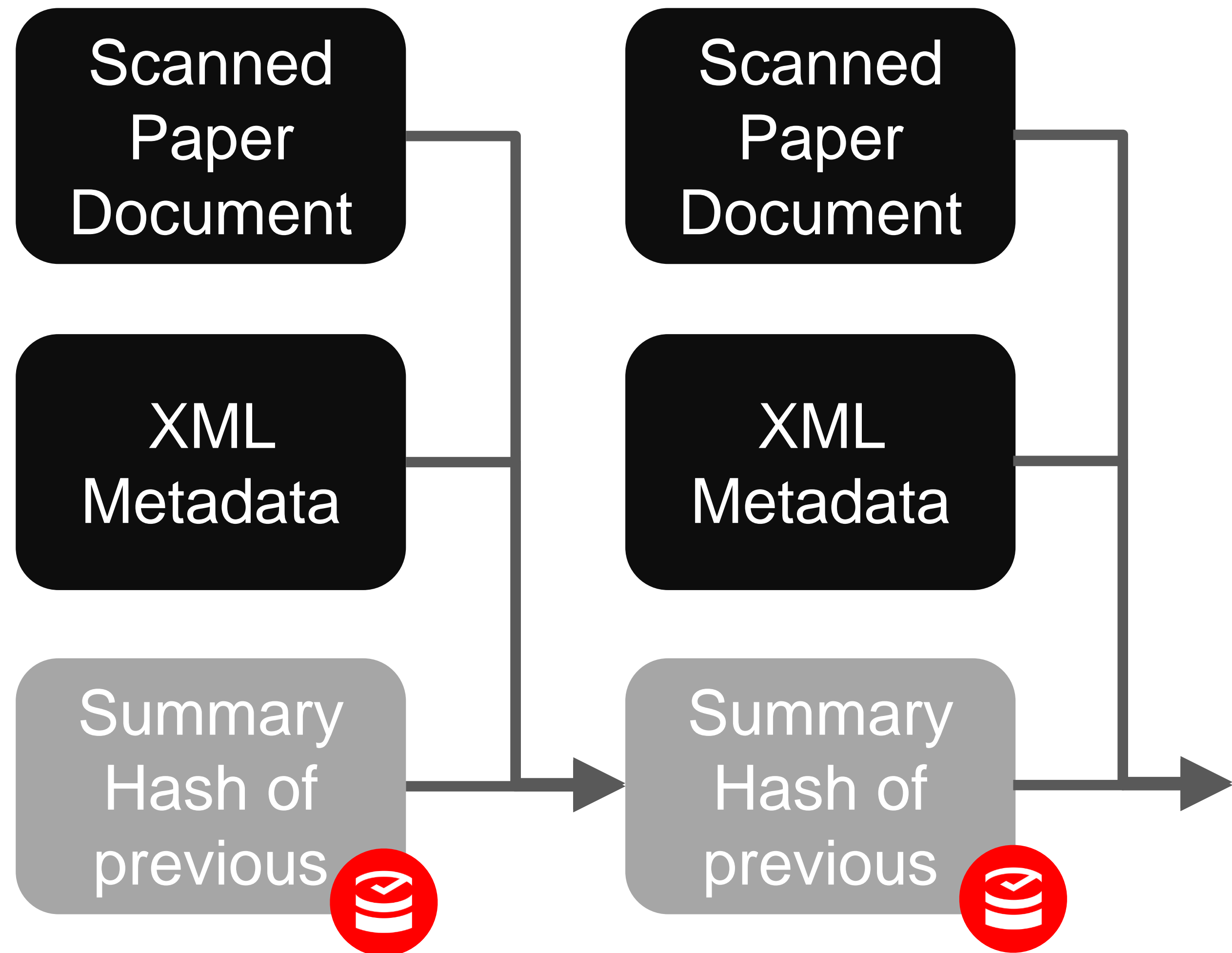




# Estonian Government

Electronic records and associated metadata are chained to the previous record, signed and stored in a database.

- Provable ordering
- Impossible to delete a record undetectably
- Metadata provides attribution and government transparency
- Monitored and verified in real-time



REPUBLIC OF ESTONIA  
GOVERNMENT



# Cloud



“how do I comply with the law and trust my mission critical processes to an outsourced vendor who has little if any accountability?”



## What do Enterprise CIOs need for Cloud Migration ?

Q: What do CIOs need to move their mission critical processes to the cloud

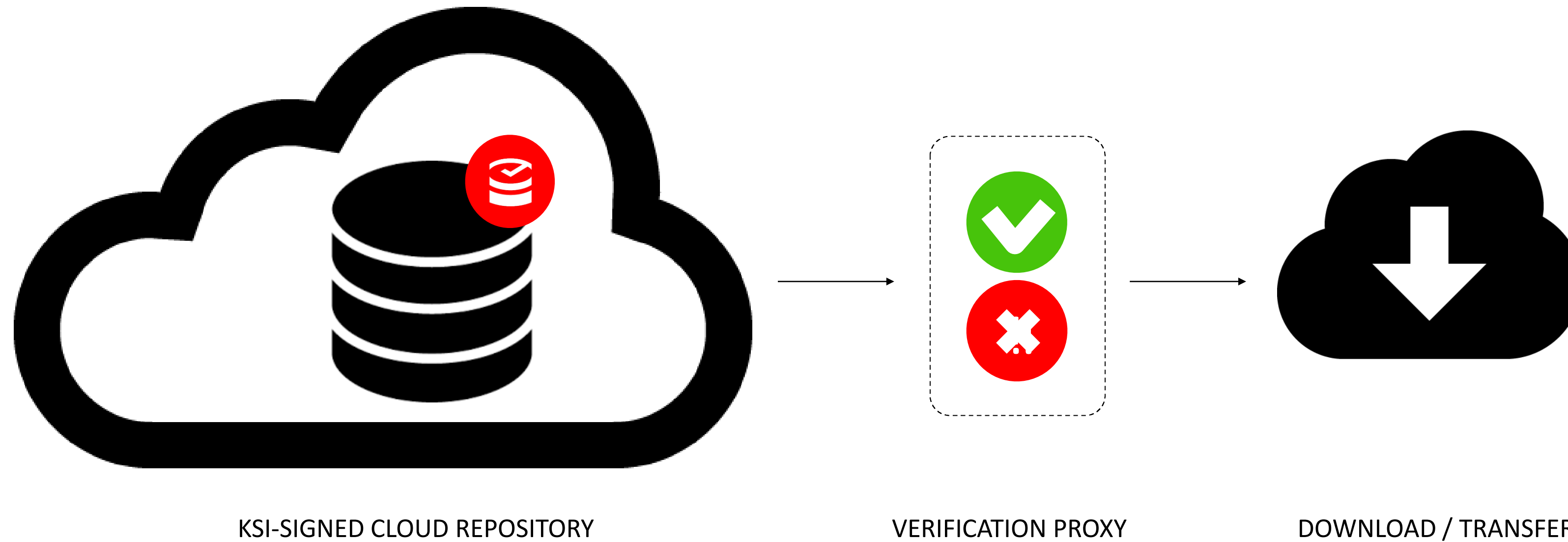
A: “accountability, reliability, compliance, security, verifiability, auditability, acceptance of liability” etc.

They demand that there is a secure supply chain and that every step in that supply chain can be verified in real-time and when things go wrong it is possible to figure out what went wrong and that there is someone who can be held accountable.”

Today not a single cloud vendor can say this.



# US Intelligence Community : Deterministic Cloud DLP



- Only **signed assets** allowed to leave
- Policy is fail-close (no signature = no ability to move content).
- Underpins existing access controls (which may be compromised through privilege escalation).

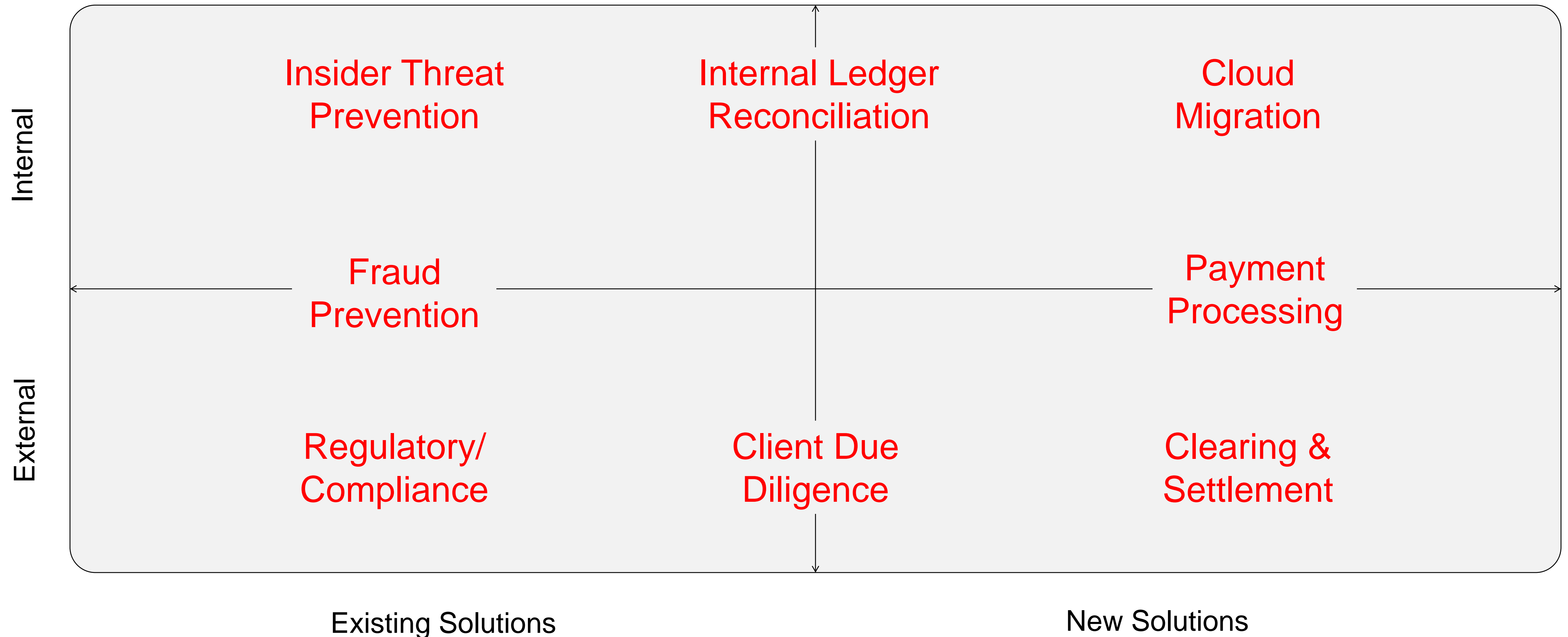


guardtime 

# Insurance Blockchain



# Where do Blockchains Fit In?





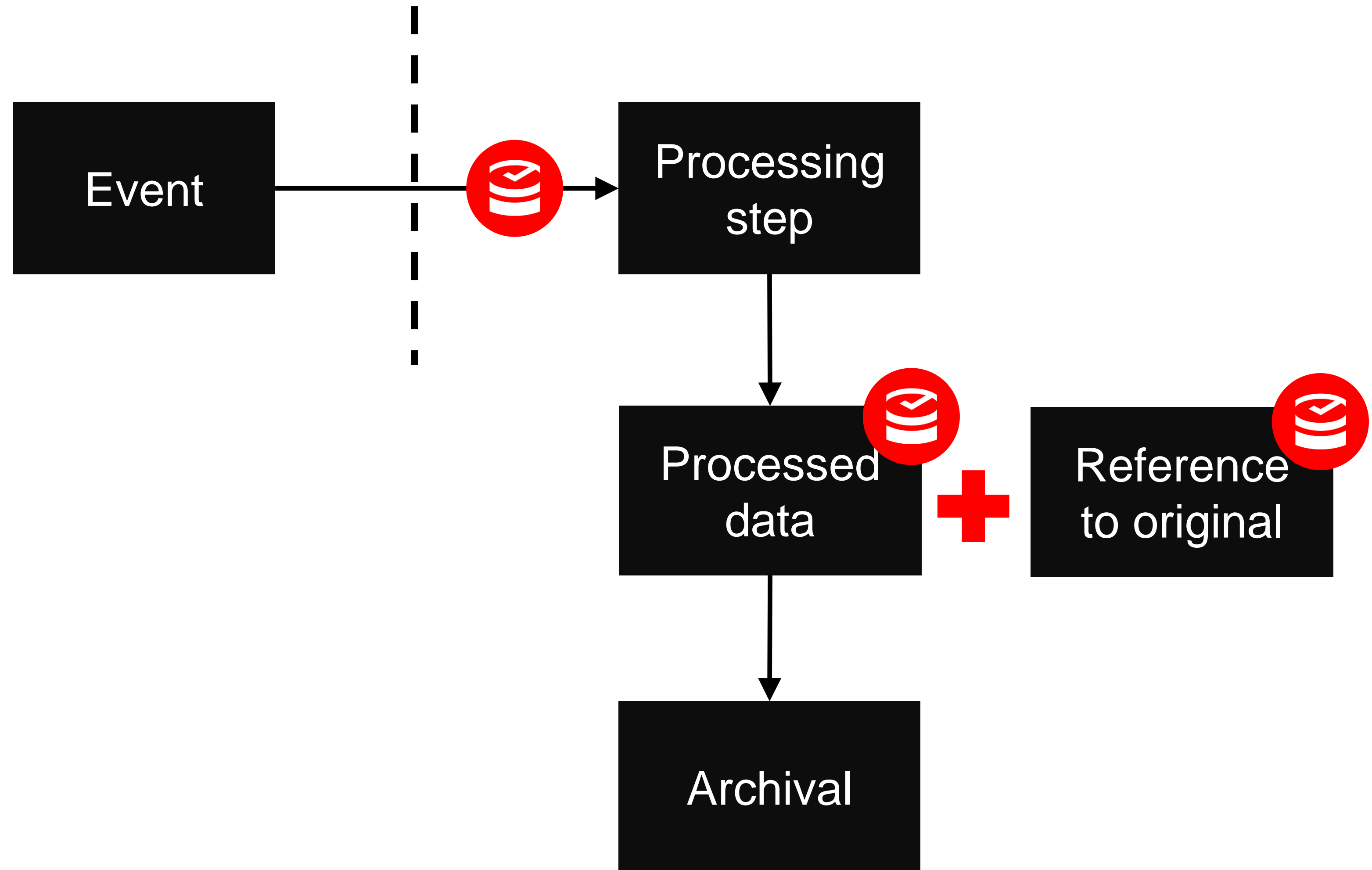




# Cryptographic Chain of Custody: Payment Processing

KSI can be used to create a chain of custody, establishing when, and who touched or modified data during each step in processing a transaction

When payment processing data is saved to disk, KSI verification proves that the data has not been changed while it was vulnerable.





## What can KSI Address for Insurance Industry – for example ?

Cryptographically verifiable long running transactions and payment systems that are globally distributed for resiliency and compliant with various reporting requirements.

- New Claims Settlement and Payments
- Healthcare Record Protection
- Cyber Liability Solutions
- Reinsurance/Retro

*But Insurers are also businesses with vulnerabilities, and **production requirements** for compliance and regulatory reporting and security.*

- Fraud detection and prevention
- Insider threat
- Regulatory archival – e-discovery
- Cloud
- Digital Identity / KYC / AML
- Safe Electronic Trading of Records
- Dispute Resolution – less legal reserving
- Telematics, Smart Cities, Teleradiology

# E-Discovery : Proving Long Term Validity of Records

**Tryg**  
Certificate of Insurance  
Public and Product Liability Insurance  
Travel Insurance

This is to certify that the below mentioned insureds have been issued by TrygVesta and are effective subject to the terms and conditions of the policies as at 1 January 2009.

**Policyholder:** The Danish Gymnastics and Sports Association (DGI) and The National Olympic Committee and Sports Confederation of Denmark (DIF) and all athletic associations, clubs etc. under DGI and DIF.

**Period of insurance:** 1 January 2009 – 31 December 2009

**Geographical area covered:** Worldwide including the USA/Canada

**Public and Product Liability Insurance**  
**Policy number:** 670-8.000.308  
**Policy limits:** USD 1,000,000 in total for bodily injury and/or property damage per insurance year.  
**Scope of cover:** The insurance covers the Insured's legal liability to pay damages.

**Travel Insurance**  
**Policy number:** 654-1448-000008  
**Scope of cover:**

Transport of patients/respiration	unlimited
Escort	unlimited
Travel accident	Death DKK 614,156
	Personal injury DKK 1,028,305
Delayed luggage	DKK 5,714
Damaged luggage	DKK 99,562
Assault	DKK 813,722
Personal liability	Property damage DKK 5,000,000
	Bodily injury DKK 10,000,000
Legal expenses	DKK 125,000

This certificate of insurance has solely been issued for the purpose of information and does not provide the bearer with any special rights. Further, the certificate of insurance does not enhance, extend or change the cover of the above-mentioned insurance policies.

**Date of issue:** 18 December 2008  
**Issued by:** TrygVesta  
Klaudestrøvej 801  
2750 Ballerup

Carl Hallander  
Senior Vice President

**TrygVesta**  
Tryg is the Danish division of Tryg, a group of assets of two billion dollars in the world.  
Our core business is with marine, aviation and health insurance products for both companies and business.

**Tryg**  
Trygvestvej 100, 2750 Ballerup  
Tlf: +45 44 44 44 44, Fax: +45 44 44 44 44

Verify with Link2Cloud App from  
Apple App Store or Google Play

**guardtime**  
guardtime.com  
15 September 2008 00:00:00 UTC

AAAAAA-CI2WSY-AAK5KY-QHRS3L  
GGQYLI-U02JYT-IMJ3O2-LA340F  
5HP5EU-70U6CG-RTKJ3K-OAAOLG

**MARKET**  
Thursday September 18 2008

**S&P 500 index**  
1350  
1300  
1250  
1200  
1150  
Aug 2008 Sep  
Change on day +3.73%

**FTSE 100 index**  
5600  
5400  
5200  
5000  
4800  
Aug 2008 Sep  
Change on day -2.25%

**FTSE Eurofirst 300 index**  
1250  
1200  
1150  
1100  
1050  
Aug 2008 Sep  
Change on day -1.99%

**US equities**  
Financial stocks came under further pressure as the Federal Reserve's rescue plan for AIG offered only partial relief to the markets. Morgan Stanley and Goldman Sachs suffered particularly heavy losses in early trade.

**UK equities**  
The FTSE 100 index closed below 5,000 for the first time since May 2005. HBOS ended 19 per cent lower after a very volatile session that saw the stock trade in a 126p range as some 430m of its shares changed hands.

**AIG rescue deal fails to calm**

**GLOBAL OVERVIEW**  
Search for cash and low-risk investments

gan Stanley and Goldman Sachs came under heavy pressure while recently battered UK bank HBOS tumbled a further 19 per cent.

**TED Spread**  
Three-month \$ Libor rates over three-month treasury bills (% points)

**Chinese equities**  
Shanghai Composite

◀ The gap between the three-month Libor and the

E-Discovery requires the ability to produce as evidence all potential data and requires meetings to discuss the status of the data from whence it came, has it been tampered with and when was it created. This means that all electronically stored insurance information needs to be stored for long periods – registers to SOLVENCY II. Trust Anchor.



# Industrial Infrastructure Assurance

Critical infrastructure is becoming increasingly connected and exposed to advanced persistent attacks and nation-state adversaries, where **data tampering** and **corruption** that can lead to significant economic consequences and have a catastrophic impact on human life.

Adversaries, typically sponsored by nation-states, have become sophisticated enough to develop attacks on Industrial Control Systems such as SCADA and PLC, resulting in catastrophic attacks such as the Stuxnet **zero-day attack** in Iran which reportedly ruined almost one-fifth of Iran's nuclear centrifuges.



# Microfinance and Microinsurance Sectors



- **Trusted Feeds for Farmers for Claims**





guardtime 

# Impact and Implications







Innovation in FINTECH can cause systemic risk and must be allowed to continue but risk must be mitigated to avoid emerging cyber risk.



# Cyber Resilience with KSI Blockchain

## TIMELINE

### INVENTORY

Record digital assets in the Blockchain by keyless signatures.

Insurance inventory for digital assets

Cyber Risk Assessment Service to determine which assets are signed

### DETECT

Continuously verify that the network is still free of compromise

Blockchain based real-time alert upon compromise

Pre- and Post Observational Support

### RESPOND

Notify insurance provider that there has been a compromise

Make real-time decisions from the Blockchain real-time integrity information identifying assets compromised with a response service.

### RECOVER

Fix the problem and then restore the network to the original state by resigning the detected assets.

Automated processes for eDiscovery and Subrogation





# INSURANCE IDEAS and discussion



Launching the Insurance Blockchain starting to happen in London Market ?

KSI as NACOSS equivalent for cyberliability?

Responding to emerging regulations in cyber?

Partnerships with automotive manufacturers / OEMs?

Enterprise risk assessments and enterprise-wide cover for cyberliability?

Change policy wordings in new cyber products to KSI-based warranties in exchange for higher limits, discounts and guarantee of claims payments?

# Re-Invention of Security

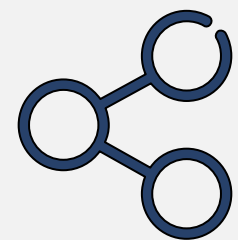
## Data-Centric World Requires a New Focus

### FROM: PROTECT ONLY

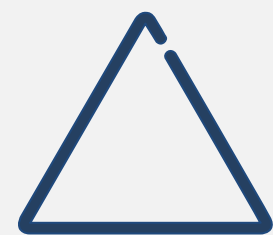
*100% protection is possible*



Perimeter-centric: access control, encryption



Hardened end points, users not devices



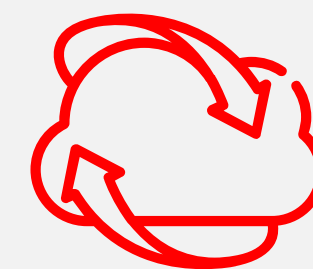
Data is locked down



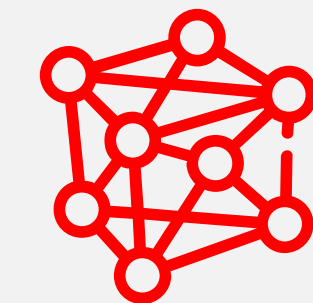
Illusion of liability protection: third party audits, certifications

### TO: VERIFY EVERYTHING

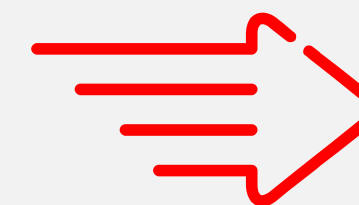
*compromise is inevitable, location matters*



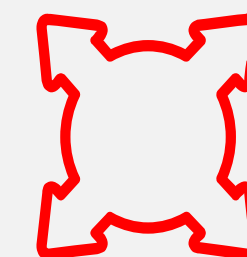
Data-centric: every data asset is tagged, tracked, located, verified



Immutable validation of end points: every user AND all devices



Data is portable without breaking the law



Onus for proof: independently verifiable, mathematical forensics

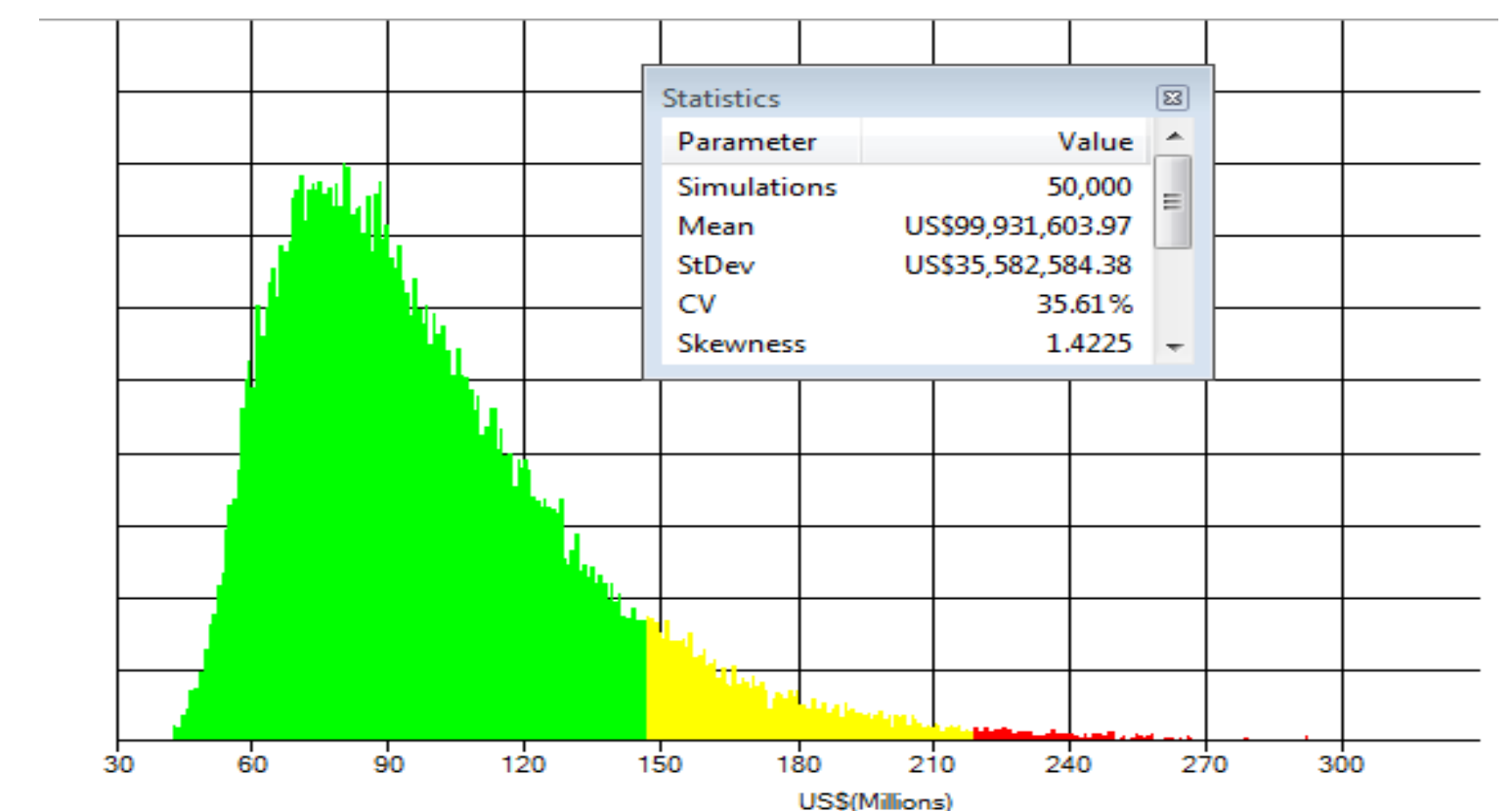
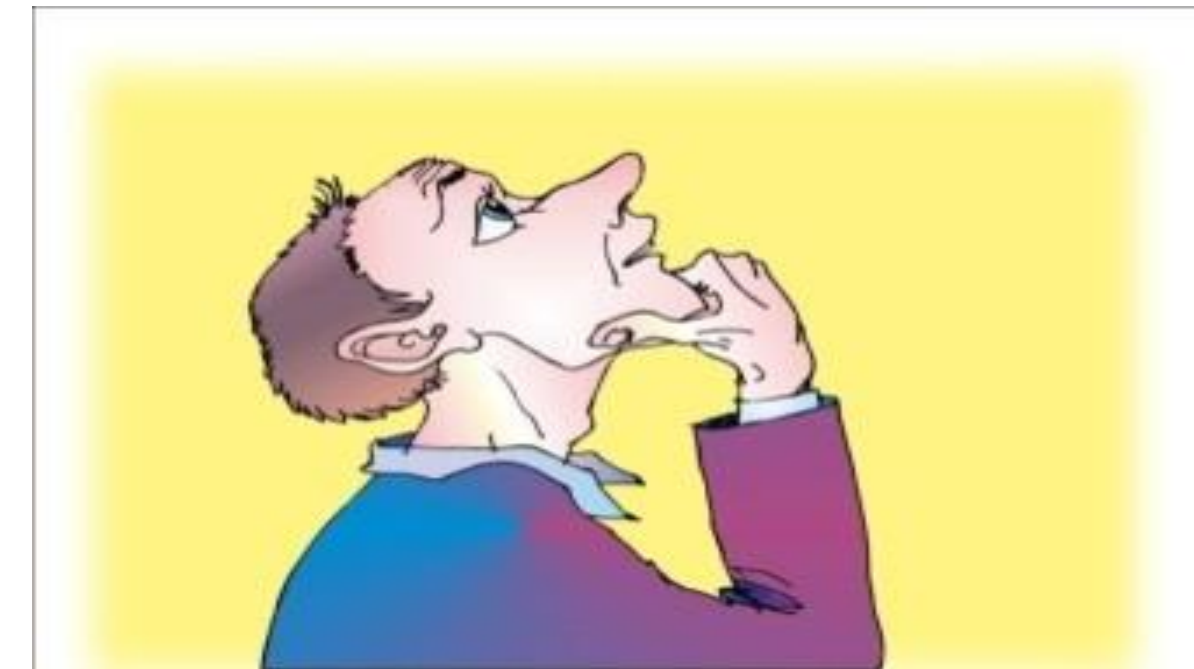


# Quantifying Cyber Risk Internally

There are two primary techniques in use to analyze financial effects of different strategies :

*Scenario testing (FA)* - projects business results under selected deterministic scenarios into the future. Results based on such scenario are valid only for this specific scenario

*Stochastic simulation (DFA)* - thousands of different scenarios are generated stochastically allowing for the full probability distribution of important output variables, like economic capital, risk transfer, investment strategies and profit maximization



# Correlation of Cyber Risk to Corporation

Cyber is a large emerging risk.

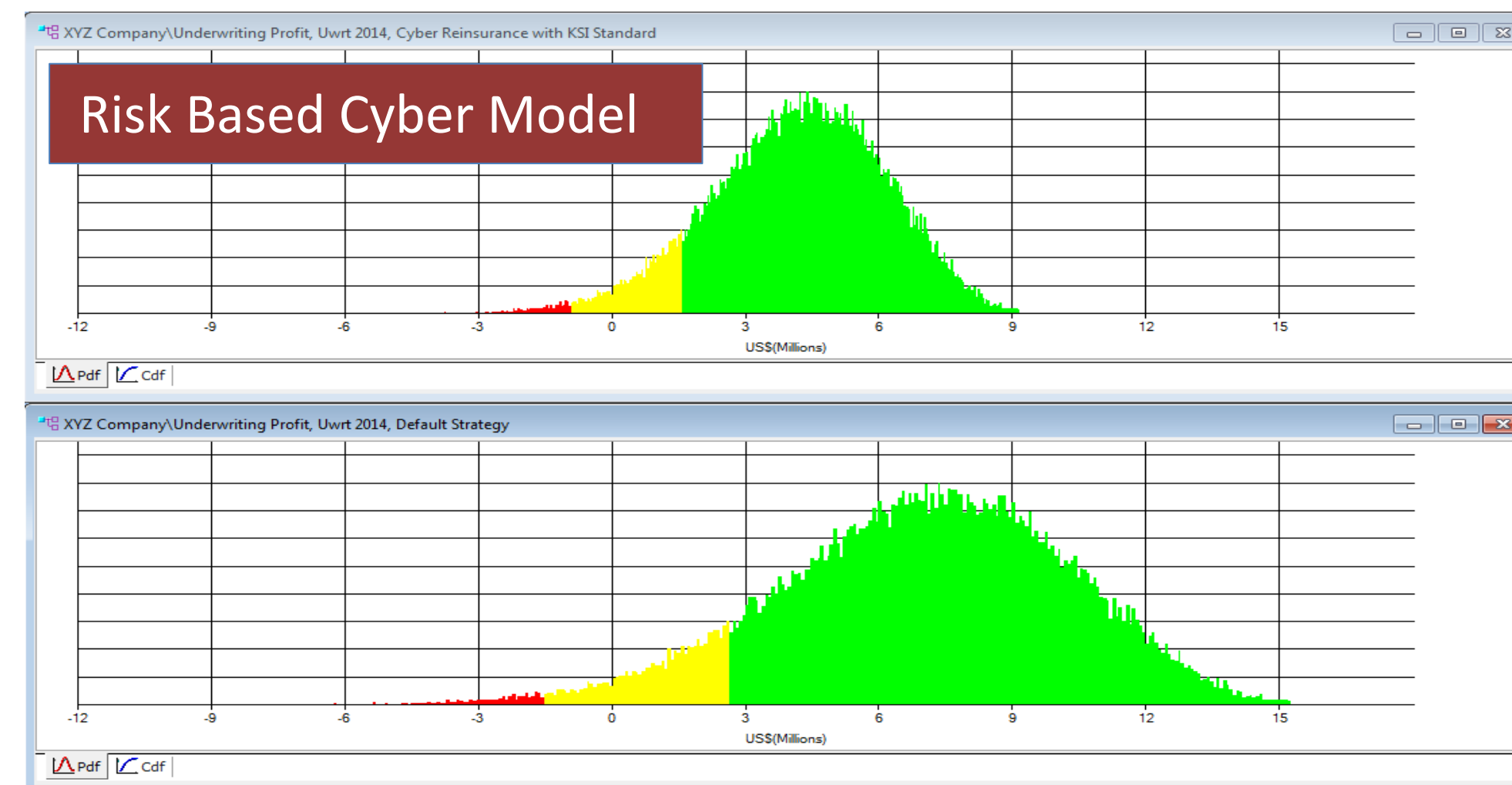
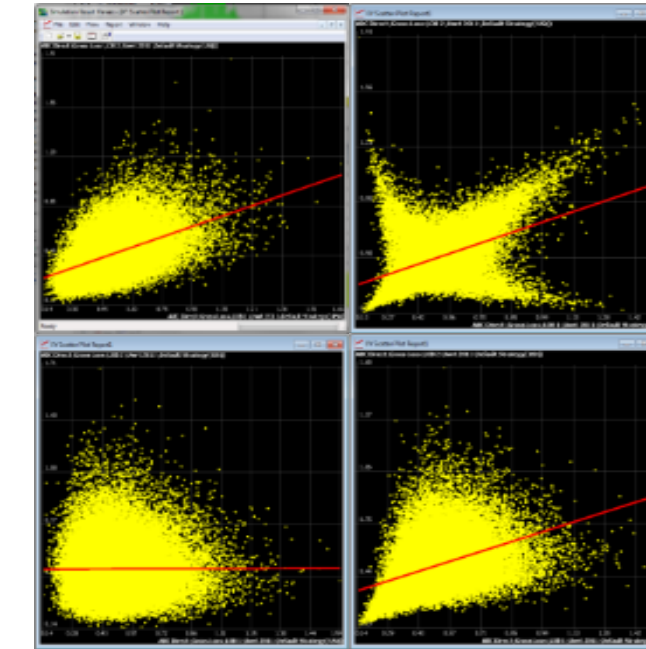
It is a risk deep rooted in data integrity.

The risk must be mitigated to give resilience.

The risk must then be quantified by stochastic modeling.

To integrate cyber risk to the total risks of a company correlation needs to be applied in the DFA model

**Data Centric Security** is the means to achieve this correlation.





# Shift from IT to Board Oversight

Cyber Risk is definitely not an IT issue

It Requires Board Oversight and Governance

This is an operational risk of large scale

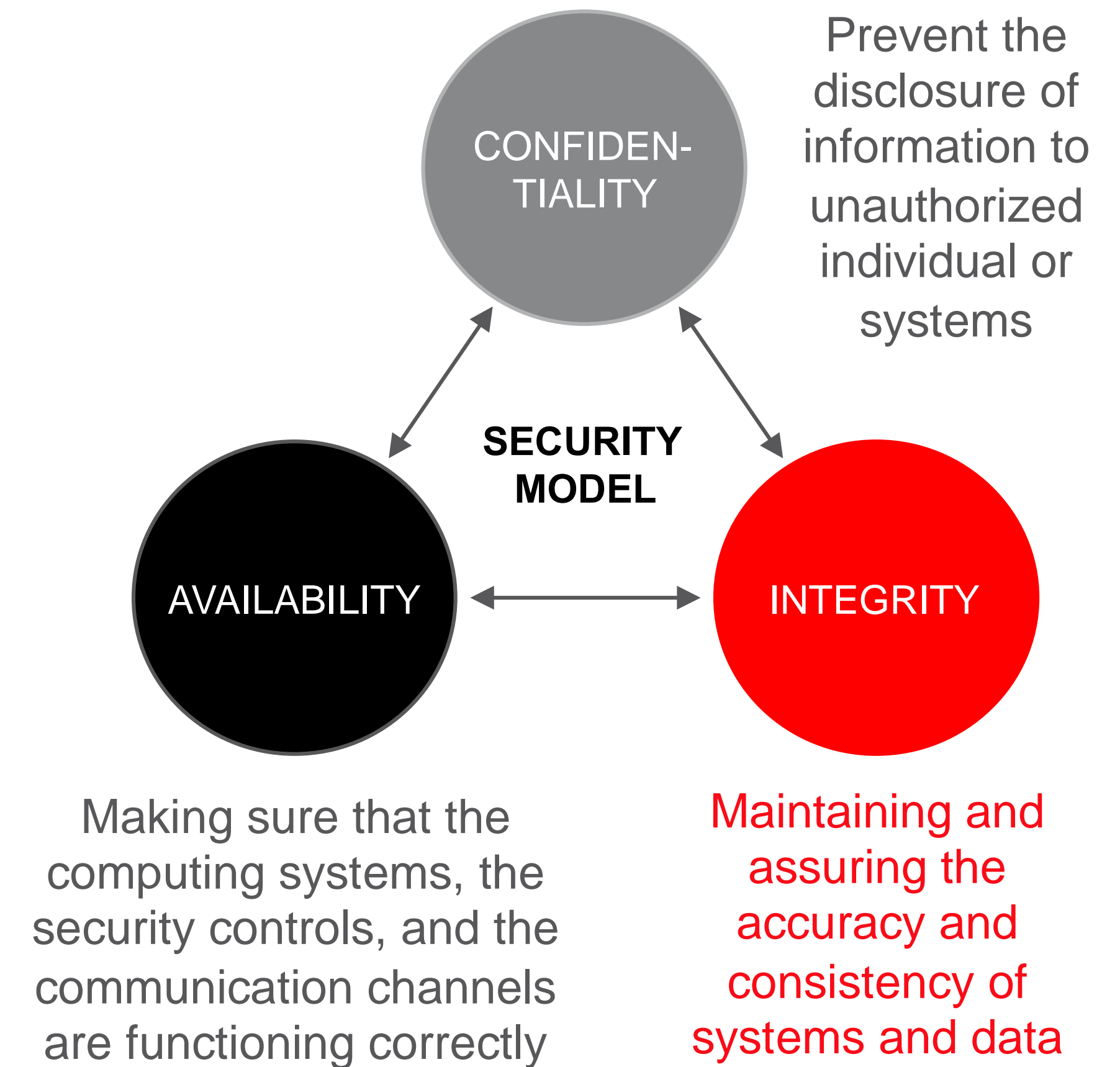
The IT budget should be split to Security Budget

CISO should report to the CEO

The Security budget points to data integrity

Corporation insurance will head towards **data integrity** and not only confidentiality/availability

The Security Model – CIA triad

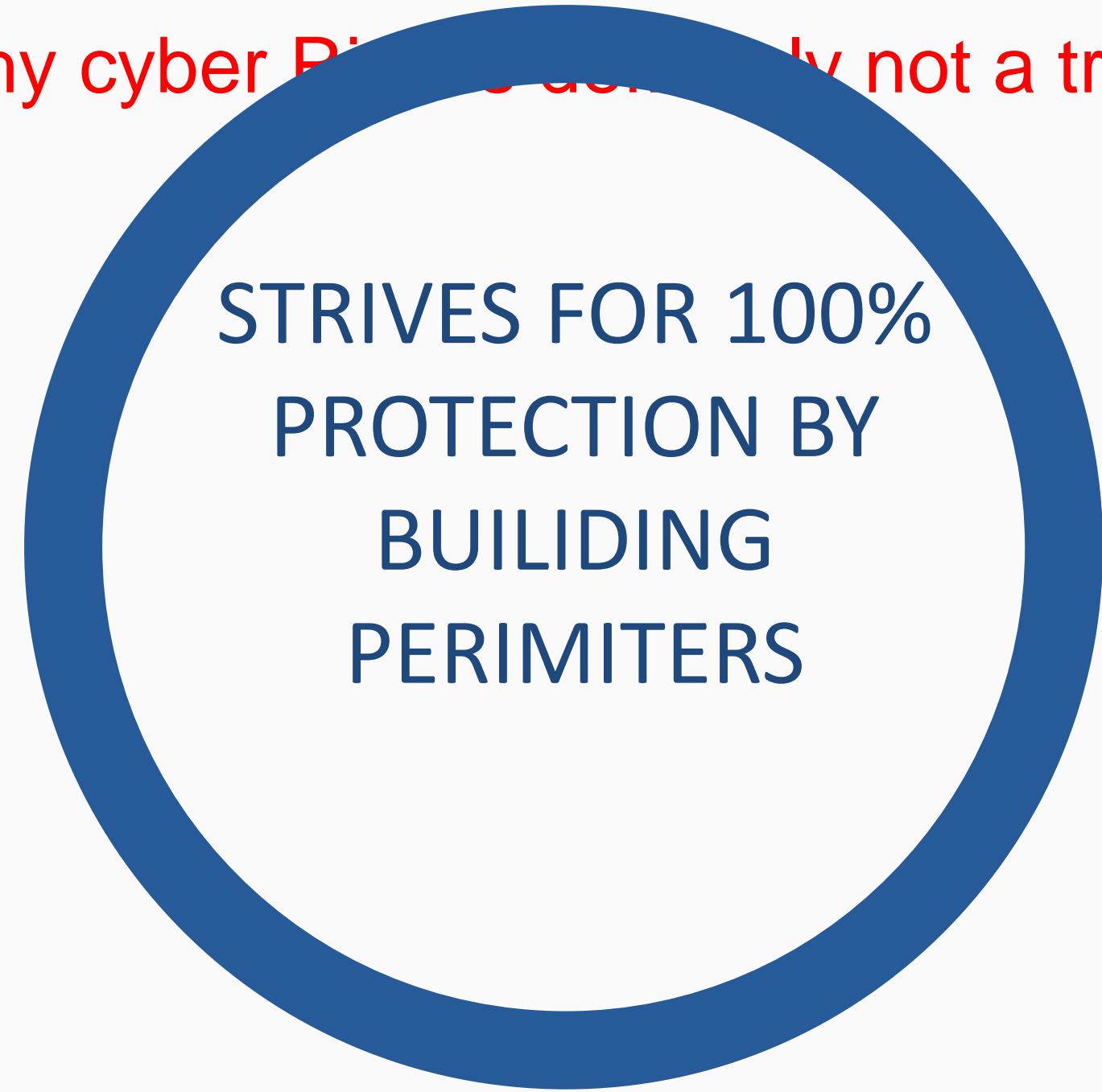




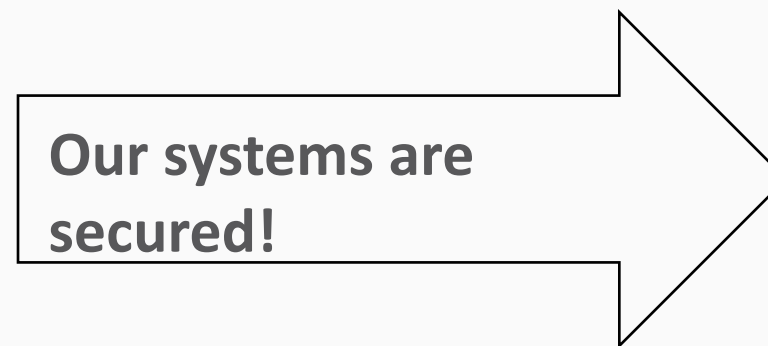
# Changing Business Needs Demands a New

## Security Model

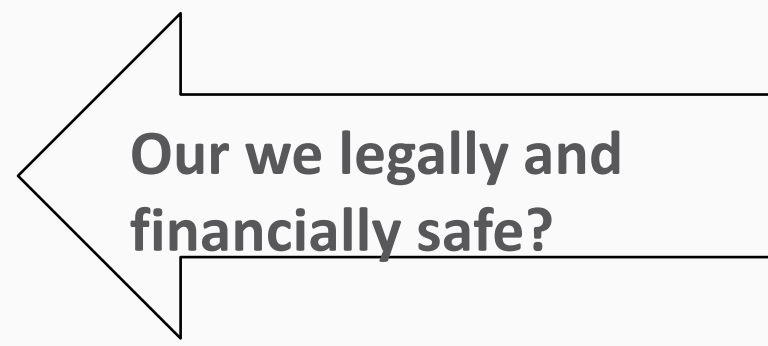
and why cyber risk is not a traditional IT issue



CIO / CSO / CTO



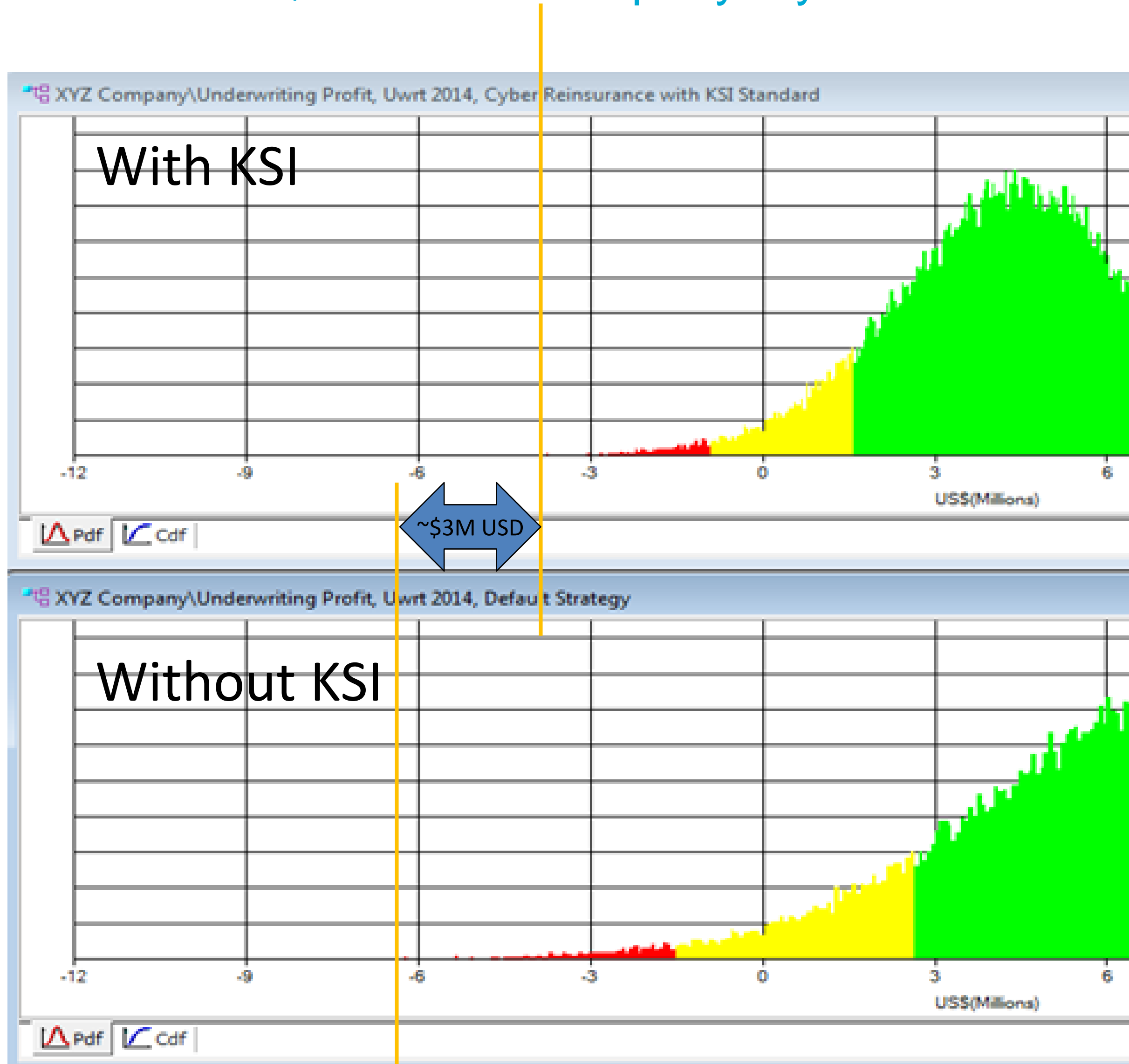
CEO / CFO / CRO





# How ksi will pay for itself

if this was a \$50M USD company a year



In 2012, Cyber Ins was \$5K per \$1M USD coverage – max \$200M limit of coverage

Privacy and perimeter only

No data centric model considered

Mega breaches happened and raised risks

Now, \$50K per \$1M USD – max \$500M USD – with caveats

Need mitigation resilience with KSI

Need data centric integrity to prove a lower risk is tolerated

DCS can be covered by the costs of reducing risk

# The New Google

**Today, we Google for everything, mostly information or products.**

**Tomorrow, we will perform the equivalent of “googling” to verify records, identities, authenticity, rights, work done, titles, contracts, and other valuable asset-related processes. There will be digital ownership certificates for everything.**



# Guardtime

[David.piesse@guardtime.com](mailto:David.piesse@guardtime.com)