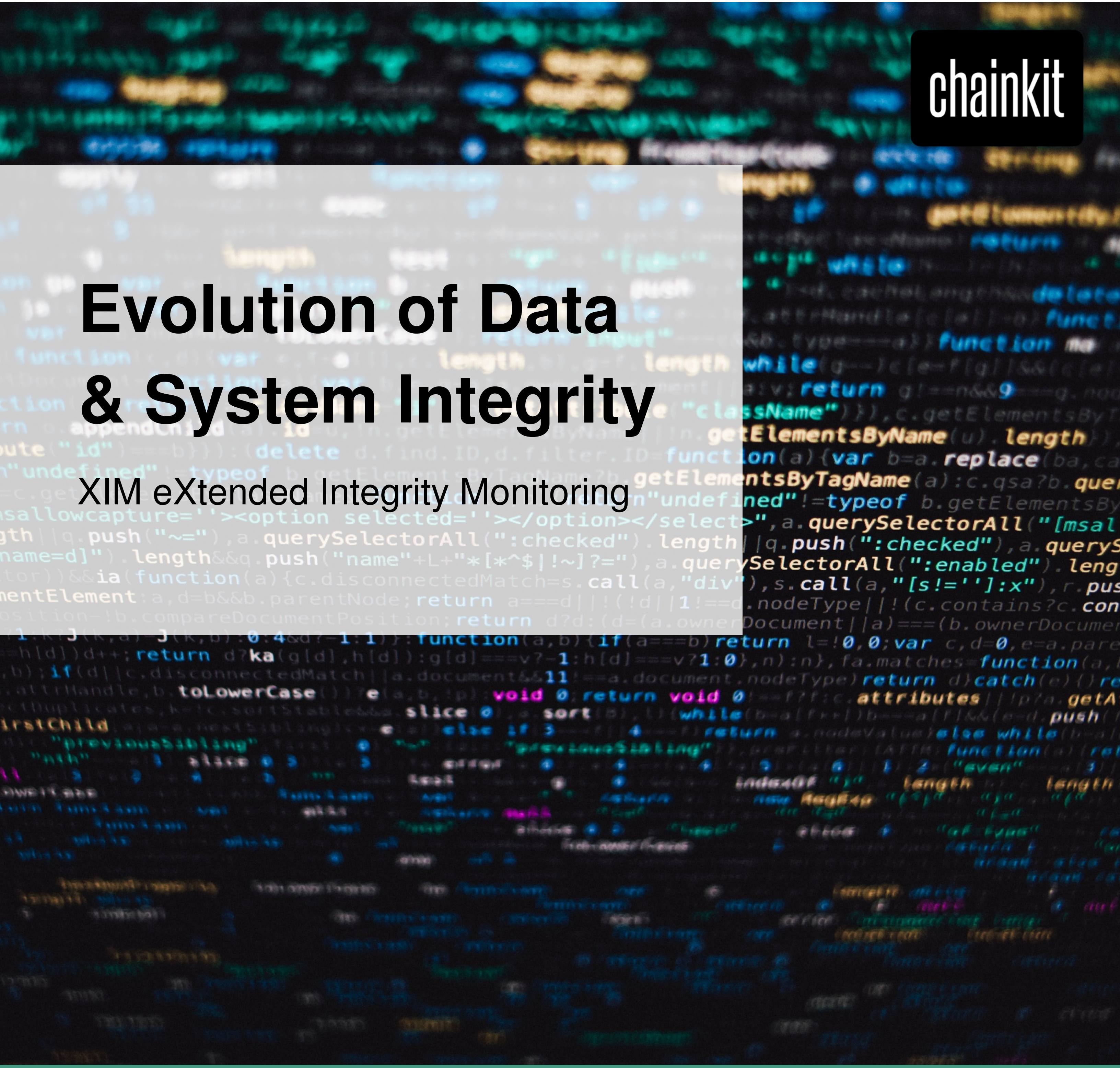


chainkit

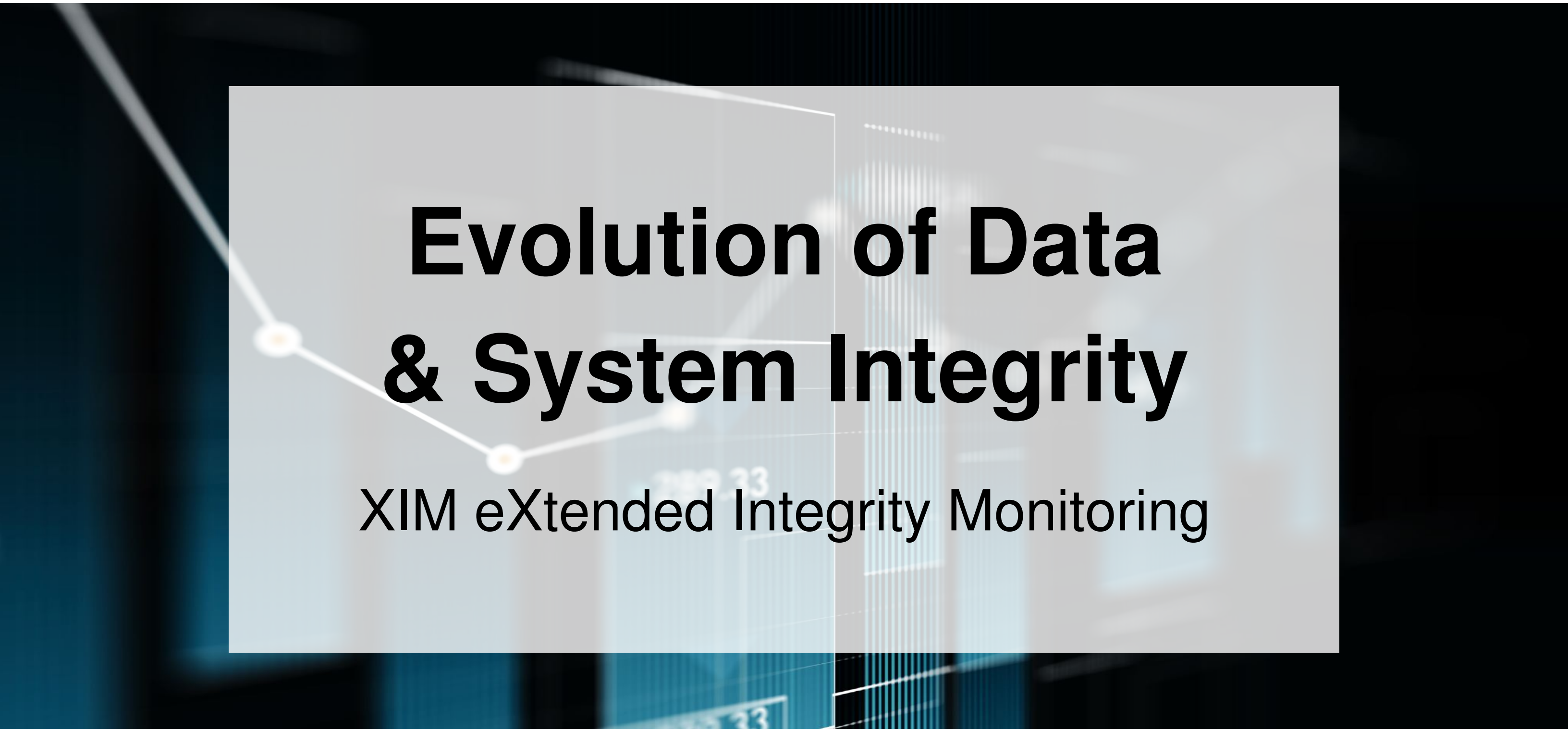
# Evolution of Data & System Integrity

## XIM eXtended Integrity Monitoring

Chainkit pioneers XIM to respond to the demands of social, mobile, big data, IoT and new regulatory compliance requirements that the current standard – FIM (file integrity monitoring) – simply cannot keep up with. This is the critical gap in most security programs that unnecessarily heightens cyber risk.

# Contents

This whitepaper is the first in a series, examining the evolution of Data and System Integrity of computing systems. In this paper, we will examine the importance of **Agile Integrity**, while related papers will also focus on Depth of Integrity, Seamlessness, Legal Weight and modern applications of eXtended Integrity Monitoring in Threat Detection, Attack Visibility, Digital Forensics, Incident Response, Audits and Regulatory Compliance.



# Evolution of Data & System Integrity

## XIM eXtended Integrity Monitoring

## Introduction

Over the past 70 years, computing has evolved from creaky Vacuum Tubes to nanometer-thin Silicon technologies, enabling globally connected pocket Supercomputers for most people on the planet. As we're now on the verge of Quantum computing, it's high time to examine whether one of the three pillars of Cyber Security has kept up?

## History of Integrity Monitoring

**Integrity** is a cornerstone of business, governance and law enforcement, as well as a dedicated principle of their underlying computing systems. Those systems initially evolved from the days of host-based mainframes, to Client/Server computing. Transaction Processing, associated Reports and Static Files were the dominant systems and data types of both eras. Malicious hacking in support of academic security research and digital fraud followed soon after, ushered into the mainstream by the Morris Worm virus of 1988. Four years later, innovative research from undergrad Gene Kim @ Purdue University released the popular tripwire tool and pioneered the category of File Integrity Monitoring (**FIM**). It became an early foundation for computer security (intrusion detection), audits, forensics, and mainstream regulatory compliance requirements such as SOX-404 and PCI-DSS, to name a few.

## Big Veracity – Future of Integrity Monitoring

By 2007, Client/Server computing had reached its zenith and the disruptive iPhone release catalyzed existing Web Computing demand for a wider **Variety**, greater **Volume** and **Velocity** (3 Vs) of data types, with associated new databases and processing systems. The terms Big Data and NoSQL were coined to cover the cambrian explosion of new software for this demand, and the introduction of Cloud computing proved to be the dominant operational model to deliver solutions satisfying this demand. But one critical 'V' was left behind in this revolution - **Veracity**.

These new Agile data types use critical abstraction layers of parallel processing and data granularity which are not represented by their underlying files on a 30-year-old POSIX file system architecture. Streaming Data, multiple Transformations via Data Pipelines, Publish-Subscribe distribution models, Eventual Consistency, Document, Graph and In-Memory databases are just a few of the radical advances behind mainstream e-commerce, search and social media services we rely on more than ever.

> "Chainkit takes everything we love about Tripwire 28 years ago and modernizes it for real-time dynamic datasets in the cloud with big data workloads."
>
> *Val Bercovici, CEO & Cofounder, Chainkit*

## XIM – Integrity Monitoring for Agile Systems

Agile data is active, constantly capturing, transforming and moving information. Static file integrity monitoring (FIM) was never designed to represent the proper state of dynamic data flowing through an agile big data system in the cloud, or at the edge. Yet regulatory requirements in the Public Sector, Financial Services, Healthcare, Retail, Communications, Transportation and other industry verticals have only grown since the

invention of FIM, almost 30 years ago. We need a new Integrity Monitoring Architecture which works across old and new data types and systems. In response to these modern

requirements, Chainkit introduces e**X**tended **I**ntegrity **M**onitoring or **XIM** for all data and associated systems.

## Evolution of Data & System Integrity

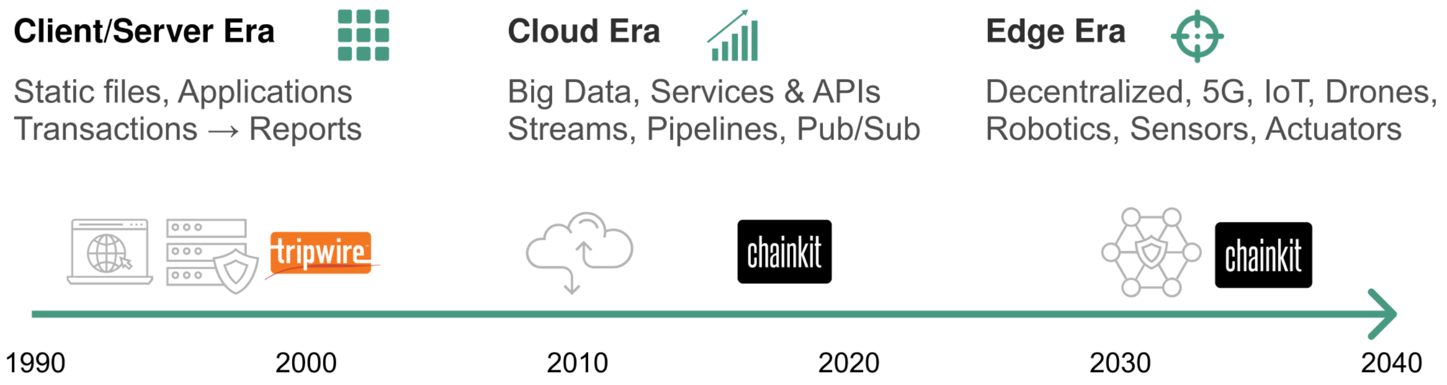

Client/Server Era
Static files, Applications
Transactions → Reports
Cloud Era
Big Data, Services & APIs
Streams, Pipelines, Pub/Sub
Edge Era
Decentralized, 5G, IoT, Drones,
Robotics, Sensors, Actuators
tripwire
chainkit
chainkit
1990
2000
2010
2020
2030
2040

*Fig. 1: Evolution of Date & System Integrity Timeline*

# Key Differentiators

**XIM** is a 21st century design for integrity monitoring, built upon the original 20th century FIM requirements, updated for modern social, business, security and regulatory needs. The key features and benefits of a XIM solution include:

## Performance

XIM systems must scale performance to match the speed of processing today. That means streaming data feeds from billions of sources at 100 gigabit network speeds to multi-step data processing pipelines delivering results from data centers, sensors telco towers and robots - to mobile devices, vehicles, actuators, TVs and laptops, required within millisecond and microsecond latencies on-demand.

## Granularity

In-memory arrays, stacks and linked lists matter. Network frames matter, rows and columns matter in a database, logs matter, transactions matter, frames in a video matter, events and attributes in telemetry matter. Today’s apps are richer in data types than ever before. Every byte matters, not just those in a file.

## Domain separation

Integrity monitoring is an essential service. Operating it within the same domain as the data and systems being monitored introduces risks of data and system poisoning. Good cyber security hygiene and auditing best practices recommend separation of duties for identities and domains between the monitored and the monitor.

### Operational efficiency

XIM is best offered as a managed service using the popular SaaS subscription model. Dedicating precious internal human resources to the care and feeding of a monitoring system carries a significant opportunity cost for all regulated industries, which can assign more valuable business responsibilities onto their IT/OT cyber security, DFIR, compliance and internal audit staff.

### Architecture

Cloud-native architectures, based on API-driven services, enable the modularity, composability and horizontal scale needed to keep up with the relentless pace of modern data systems operating at the performance levels described above. XIMs should be service-oriented and container-based, allowing for efficient orchestration in a public, private, multi or hybrid-cloud environment.

## XIM Priority – Log Integrity Monitoring

Security event logs are the lifeblood of cyber security, DFIR and compliance in a 21st century organization. Security Incident and Event Management (SIEM) solutions are popular with Enterprises and Managed Security Service Providers (MSSPs) which operate Security Operations Centers (SOCs). Mission-

> "Why implicitly trust that your logs are correct when they're so easy to tamper with?
>
> Don't trust your logs, *verify them explicitly.* Think forensically 24/7."
>
> *Val Bercovici, CEO & Cofounder, Chainkit*

critical SIEM solutions comprise of the 4 Big Data ‘V’s:

**Volume** - processing up to multiple terabytes of log data every day

**Variety** - capturing events from dozens of different sources (endpoints, firewalls, Email, IAM/PAM, IDS/IPS, DNS, Proxies, hosts, network, apps)

**Velocity** - log forwarding, collection, indexing, querying and presentation at wire speed

**Veracity** - log tampering jeopardizes value of the entire SIEM solution, reducing SOC efficiency and productivity, exposing related organizations to increased cyber risk.

A common (Splunk) event log pipeline appears as follows:

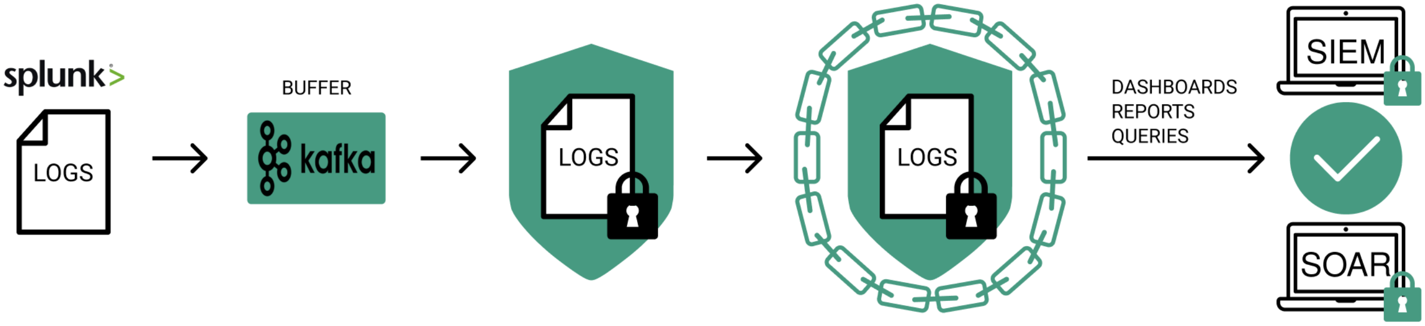


*Fig 2: Splunk event log pipeline*

Where we see logs being forwarded from an endpoint, to a collector where they are aggregated, indexed and ultimately queried, processed by rules and then displayed as dashboards, or reports.

The tamper risk for these pipelines is at every log transformation point, represented as black arrows pointing left to right above and below. Due to the prevalence of anti-forensic and other stealth tampering techniques such as timestomping, up to 39% of malicious tampering remains undetected (page 7 in report) which is represented by the faint gray 'Man in the Middle' (MitM) attacks below:

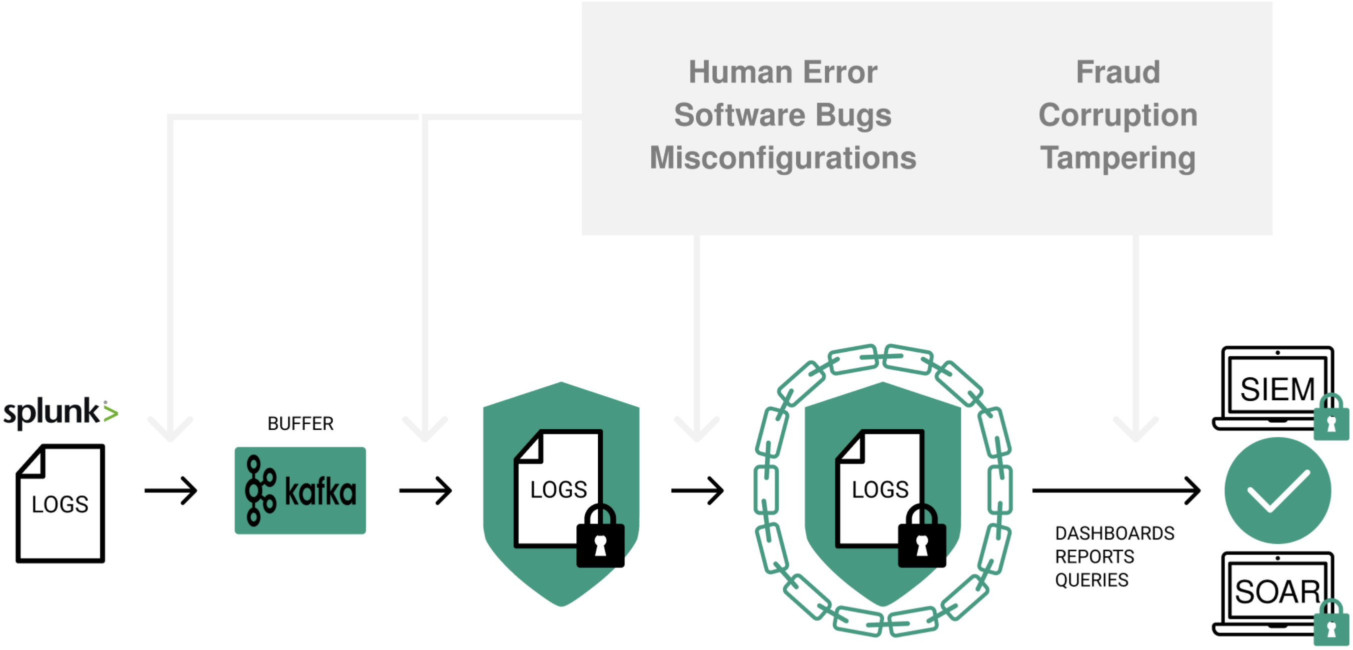


*Fig 3: Undetected tampering in Splunk event log pipeline*

The startling conclusion of this undetected digital tampering reality is that modern data pipelines are forced to imply or assume integrity because FIM can't keep up, and XIM is a new emerging standard, not yet broadly implemented. That means our global supply chains, patient health telemetry, financial market info, consumer marketing and

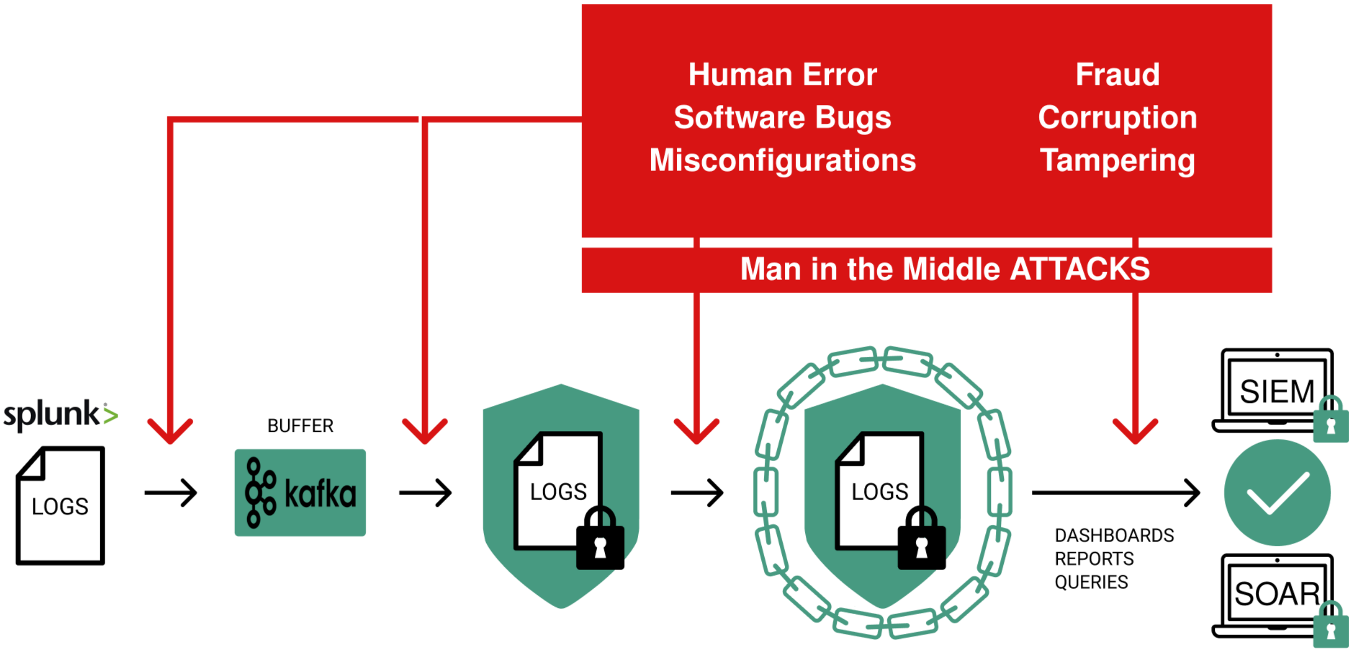


*Fig 4: Explicit verification of integrity at every step*

sales data, news feeds on social media and so forth, cannot be trusted at face value.

But XIM provides a solution: XIM solutions can convert faint grey matter above into deterministic green (good) and red (bad) data pipeline veracity, with explicit verification of integrity at every step! The performance, granularity, domain separation, robustness and architecture of XIM solutions enable complete agile integrity monitoring (veracity) of data pipelines like these, regardless of volume, variety or velocity.

## Chains of Custody

**XIM** delivers powerful integrity solutions which offer benefits beyond mere cyber security intrusion detection or compliance. XIM integrity is strong enough for international courts of law. For example, criminal investigators and prosecutors have long employed paper chains of custody for preservation of physical evidence integrity for a case, from the collection, transportation, and storage of it, all the way to presentation in a court of law.

XIM enables digital chains of custody using accepted cryptographic math to ‘bookend’ their physical counterparts in 3 fundamentally important ways:

1. XIM allows deputized sysadmins to collect forensic artifacts immediately after a cyber security incident is identified, before a law enforcement agent arrives on the scene. Time is money and preservation of vital evidence during that time delta could mean the difference between life and death - or billions of dollars in the mix.

2. XIM allows law enforcement agencies to exchange data sets across jurisdictional boundaries while maintaining independent 3rd party attribution of associated integrity.

3. XIM enables prosecutors to attest to the integrity of all included evidence in court, without needing accredited law enforcement agents to travel and testify to its integrity.

Pre-built connectors for Splunk, ElasticSearch and other log management systems automatically enable Chains of Custody on all configured logs, while system administrators or app developers can extend this capability directly to the systems they manage and/or develop by invoking the simple Register() and Verify() API verbs published by the globally Chainkit cloud service.

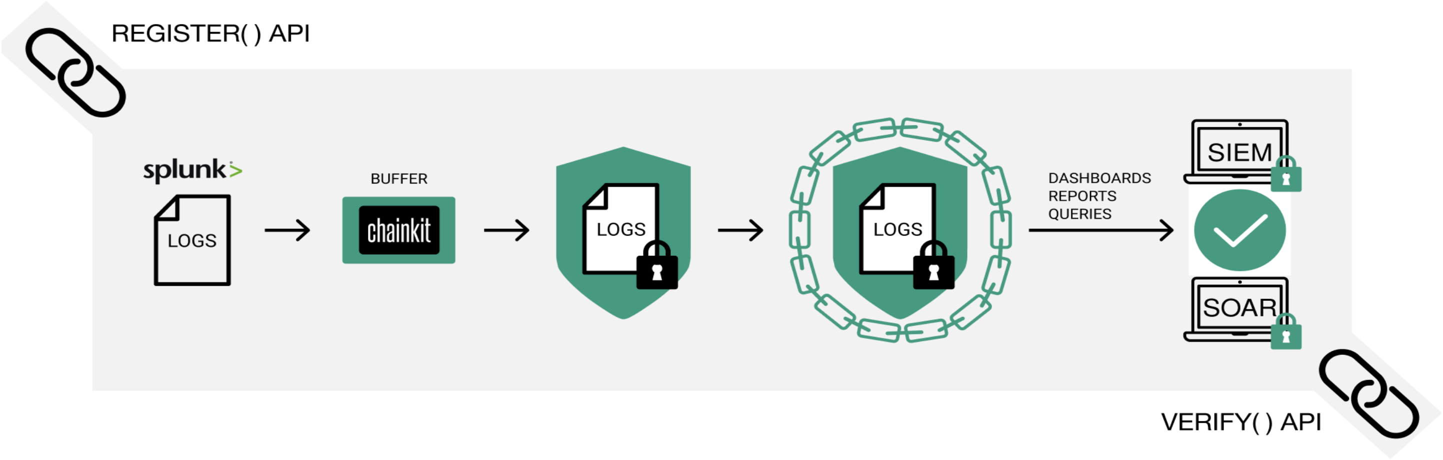


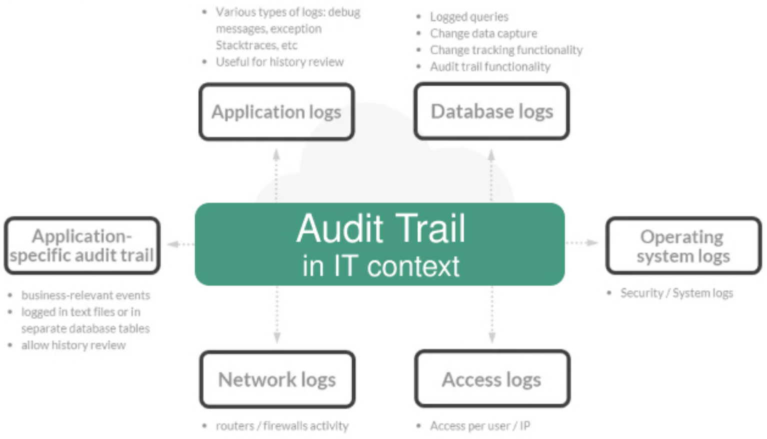
*Fig 5: Chains of Custody*

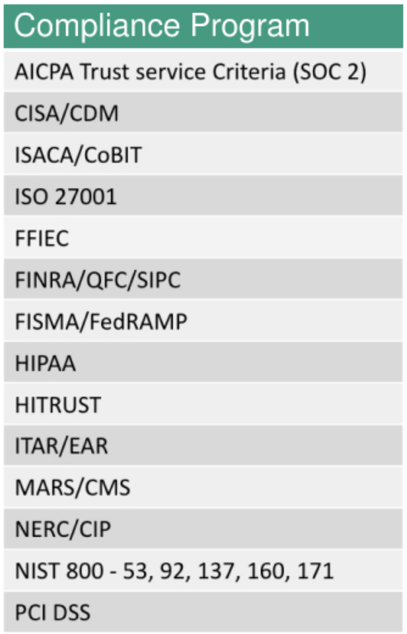
## Integrity Monitoring for the 21$^{st}$ Century

Tripwire FIM was a seminal development for digital systems at the end of the 20th century. It ushered in the ability to systematically detect cyber-attacks intrusions, while also enabling auditing of the systems it was protecting.

### Compliance Foundation for:

- Governments
- Financial Services
- Healthcare
- Retail
- Telco


Various types of logs: debug messages, exception Stacktraces, etc
Useful for history review
Logged queries
Change data capture
Change tracking functionality
Audit trail functionality
Application logs
Database logs
Application-specific audit trail
Audit Trail
in IT context
Operating system logs
business-relevant events
logged in text files or in separate database tables
allow history review
Security / System logs
Network logs
Access logs
routers / firewalls activity
Access per user / IP



| Compliance Program |
|---|
| AICPA Trust service Criteria (SOC 2) |
| CISA/CDM |
| ISACA/CoBIT |
| ISO 27001 |
| FFIEC |
| FINRA/QFC/SIPC |
| FISMA/FedRAMP |
| HIPAA |
| HITRUST |
| ITAR/EAR |
| MARS/CMS |
| NERC/CIP |
| NIST 800 - 53, 92, 137, 160, 171 |
| PCI DSS |

*Fig 6: Compliance*

As we've seen with the advent of 21st century Big Data and Cloud systems powering all government, business and personal apps, first-generation FIM solutions gave way to requirements only met by XIM. Updated for modern social, business, security and regulatory needs, organizations can confidently apply XIM solutions today to address their key cyber security and DFIR integrity gap in the CIA triad, while meeting important new regulatory compliance requirements.

Despite the ever-increasing risks of malicious adversarial tampering in all key data sets and systems, XIM solutions finally let security, DFIR and compliance teams turn any log file into a tamper-evident audit trail they can retain full confidence in!

# About Chainkit

For organizations who require the highest levels of cybersecurity and regulatory compliance, Chainkit - the pioneers of extended integrity monitoring (XIM) - empowers organizations to proactively manage cyber risk, enable new business initiatives and make security a differentiator by safeguarding data integrity with absolute confidence.

Chainkit is revolutionizing integrity monitoring by addressing the demands of cloud, social, mobile, big data, IoT and new regulatory compliance requirements.

For the first time, organizations can detect cyber stealth attacks in real-time, protect the integrity of forensic artefacts with absolute proof, and achieve the highest level of compliance.

The Chainkit service is a low-friction cloud and on-premises solution that enhances existing security platforms including Splunk and Elastic. There's nothing to replace and no new platform to install. Custom solutions are enabled through its RESTful API.

The Chainkit team wakes up every morning on a mission to eliminate data integrity threats including ransomware, malware, malicious insiders, bugs, and even honest user mistakes.

Chainkit is headquartered in Silicon Valley, California with team members in North America, Australasia and Europe.

Learn more at **www.chainkit.com**.

chainkit

www.chainkit.com