Data Content Monitoring for Security, Integrity, and Availability: A Mission-Critical Line of Defense

An IPLocks White Paper, by Frank W. Sudia
September 2002

Threats to Critical Systems

You know you're running a mission-critical system or network if a breach of confidentiality, authenticity, data integrity, or availability would cause serious impact to your organization in terms of direct financial loss, client/user downtime, damage to reputation, and/or legal or regulatory problems.

Protection Objectives
Confidentiality
Integrity
Availability
Authenticity

Threats to Data Systems
External / Hackers and Malware
Insider Misuse / Fraud
Technology / HW & SW Failures
Human Errors / Unintentional

Loss Consequences
Financial Loss (Direct)
User / Client Downtime
Damage to Reputation
Legal / Regulatory

External hackers and malware (trojan horses or viruses) contribute about 30% of the threat, with the remaining 70% originating from malicious insiders (fraud or misuse), technology failures (hardware and software), and human error (input errors, operator errors, etc.)

Negative outcomes could include loss or alteration of data, violations of security policy, illegal transaction input, disadvantageous transactions, denial of service, or information theft.

Current Protection Methods

If your systems are networked, you're already practicing defense-in-depth, deploying firewalls, anti-virus, SSL, virtual private network, 2-factor authentication, network intrusion detection (IDS), host IDS (file checksums), vulnerability scanning, and honey pots.

To guard against data loss, you're running on high availability platforms, with fault tolerant RAID storage and possibly database replication (shadowing).

In addition you enforce many other security policies and best practices in your production databases and applications, including role-based access control (RBAC), password standards, change management, application data edits, transaction rollback, referential integrity, and user-defined data types.

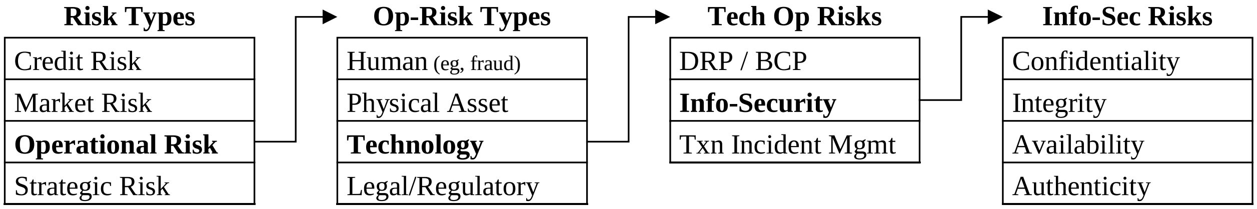
Mandates for Systems Assurance

If you operate in a regulated industry, such as financial services or health care, the problem increases, because your systems are subject to various laws and regulations requiring strict security controls, including Gramm-Leach-Bliley (GLB), HIPPA, E-SIGN, regulations of the Federal Reserve, SEC, OCC, and FDA, and the Basel II capital accord.

Furthermore to enforce your contracts in court you must prove that your computer-generated evidence is “reliable.” Opposing parties can point to past control or integrity problems to suggest that your data is not reliable.

Operational Risk Management

In larger organizations you’re moving beyond info-sec policies and procedures towards a “risk management” framework. Authentication and confidentiality form a part of the picture, but integrity and availability make equally important contributions to your total risk exposure.



Risk Types	Op-Risk Types	Tech Op Risks	Info-Sec Risks
Credit Risk	Human (eg, fraud)	DRP / BCP	Confidentiality
Market Risk	Physical Asset	**Info-Security**	Integrity
Operational Risk	**Technology**	Txn Incident Mgmt	Availability
Strategic Risk	Legal/Regulatory		Authenticity

Many technology solutions can address your authentication and confidentiality requirements, but far fewer solutions are targeting system integrity and availability issues.

The Problem: Survivability and Operational Resilience

However, despite all your efforts, no matter what shields, policies, or processes you put in place, or how much vulnerability and penetration testing you perform, there will still be significant gaps or threats that you won’t know about, or can’t adequately defend against.

- Unknown vulnerability or unpatched system
- Trojan horse program gets root privileges
- Undiscovered virus deletes or corrupts records

- Bad data feeds or file imports from other systems
- Bugs or glitches at any level of your hardware or software
- Spidering corruption (cascading updates or deletes) in a distributed database
- Inconsistent data written to database by different application modules
- Trading partner files claim on corrupt data

- Disgruntled employee deletes critical data
- Malicious insider steals money or proprietary data
- Violations of security policies or other business rules
- Mal-administration (e.g., rogue DBA problem)
- Input of fraudulent or fictitious transactions

- Mistyped prices: product giveaways (if too low) or lost sales (if too high)
- Administrative and operational errors

The IPLocks DAS Solution: Data Content Monitoring

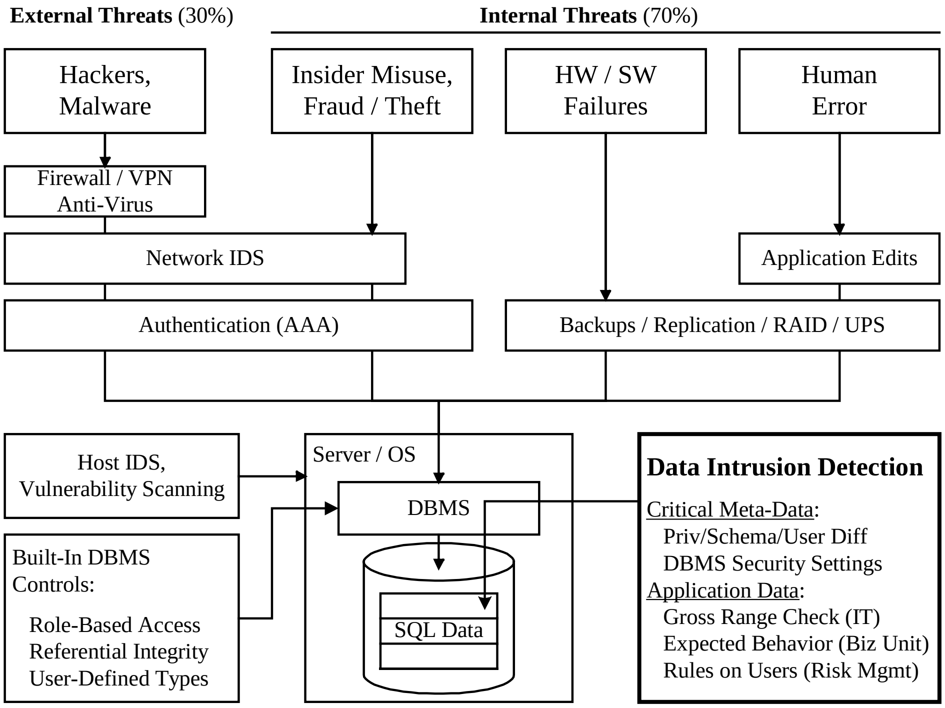
Even if your security shields and policies have failed, there's another way to tell if your system has been compromised or corrupted – Look at your data! IPLocks' Data Audit Server (DAS) implements a suite of lightweight, near-real time data inspection paradigms that can:

1. Serve as a vitally needed "smoke alarm" for potential corruption or other problems arising from all threat sources, both intentional and unintentional,
2. Monitor security settings and security-relevant actions looking for anomalies or event signatures, or
3. Permit you to create and continuously enforce a wide range of business and auditing rules, both anomaly and signature based, beyond what application developers could reasonably provide.

Indeed there is no viable alternative – critical enterprise data is dynamic and therefore does not exist anywhere but inside a relational database. Our application data content monitoring procedures are safe and effective, with low system performance impact and low false positives.

DAS "Data Intrusion Detection System" Positioning

The chart below shows the positioning of DAS in the info-sec landscape. Across the top are the four main data system threat categories (consistent with the technology risk definitions of the Basel II accord), followed by the standard countermeasures applicable to each.

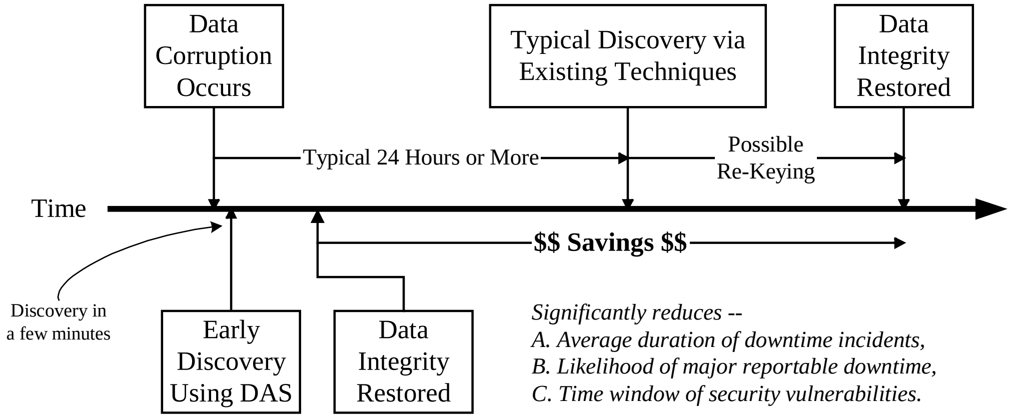


By monitoring application data, IPLocks DAS can provide alerts of attacks, misuse, system failures, or operator errors that other shields or policies have failed to prevent.

And by focusing on realized rather than hypothetical risks, and identifying the affected business application and severity, IPLocks DAS gives your response team the most relevant information.

Integrity-Availability Causal Linkage

If an attack, system failure, or operational error has occurred, you want to be warned as quickly as possible, to minimize your time and cost to recover from it. Modern data storage systems can restore your data back to a selected point in time. If the errors arose from a point event, such as a power failure, you can restore back to that specific time.


Data Corruption Occurs
Typical Discovery via Existing Techniques
Data Integrity Restored
Typical 24 Hours or More
Possible Re-Keying
Time
$$ Savings $$
Discovery in a few minutes
Early Discovery Using DAS
Data Integrity Restored
Significantly reduces --
A. Average duration of downtime incidents,
B. Likelihood of major reportable downtime,
C. Time window of security vulnerabilities.

However corruption can sometimes remain undetected for days or weeks. In that case substantial manual effort may be required, including reviewing the entire database for consistency and re-entering recent transactions, a process that could easily take a day or more.

In Pursuit of "Killer" Downtime

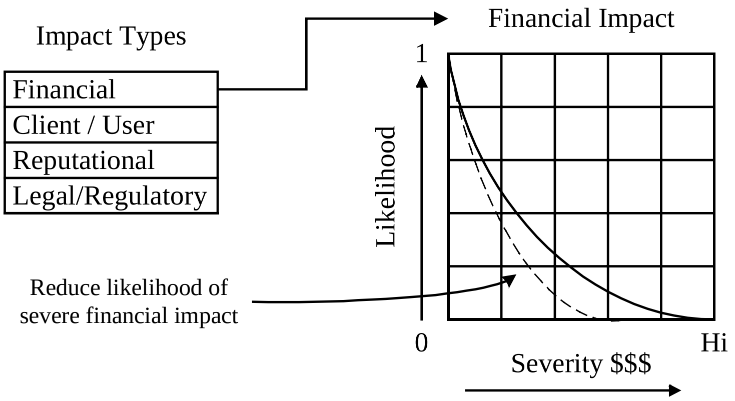
If you haven't experienced a "day of downtime" you know another IT professional who has. Whether resulting from a bad data feed, system crash, application input glitches, or corrupt backup files, such an event can put acute stress on your enterprise, with major financial and reputational impacts.

Type of Business	Loss / Hour
Retail Brokerage	$6,450,000
Credit Card Sales Auth	$2,600,000
Infomercial / 800# Promotion	$199,500
Pay Per View Services	$150,250
Catalog Sales Centers	$90,000
Airline Reservations	$89,500
ATM Service Fees	$14,500

Average Financial Impact of Interrupted Computer Operations (1996)
Source: Contingency Planning Research, West Orange, NJ

A major objective of IPLocks DAS is to reduce the incidence of severe downtime by giving warning to permit early initiation of system recovery. Likewise if there is a violation of security policy, DAS can shorten the window of vulnerability.

As shown on the chart below, small downtime incidents (upper left) occur frequently. For severe downtime (lower right) the likelihood is lower, but not low enough! IPLocks DAS can further reduce the likelihood of severe downtime, moving the curve to the left, thereby making a real improvement ("moving the needle") on your total operational exposure.



When you seek to quantify or financialize your risk exposure (a premium option for banks under the Basel II accord) reduction of downtime and integrity impacts are major areas to pursue your goals of risk reduction and loss prevention. The area of curve displacement is a measurable and substantial return on investment (ROI).

How We Do It: Practical Data Guarding Paradigms

Data intrusion monitoring is the "art of the possible." IPLocks' procedures are designed with the goals of targeting real problems while generating low false positives and minimal performance impacts. Unlike other intrusion detection products that focus on network traffic, file checksums, or registry settings, DAS examines row/column level SQL data, logging in as a client via JDBC.

Given the division of labor in larger enterprises, it is useful to separate "gross" data corruption and security issues which are of interest to IT security (since anyone could agree they represent technology failures), from "fine" errors and problems that are mainly of interest to the business unit (since detailed business knowledge is required to identify and act upon them).

Gross Corruption / IT Security Interest

Critical Metadata Changes Role / Privilege Model Changes Schema / Object Changes User / Group Changes Security Settings
Gross Range (Sanity) Checking Date Ranges Numeric Ranges Non-Text in Text Field (by code page)

Gross events, such as garbage data, are easier to find with low false positives. These are more suitable for an infrastructure monitoring service, which can be handled by IT with minimal setup time for each system to be guarded. In mature applications, all system or administrative changes are likely to be of interest, and security personnel will appreciate receiving positive notification of such events, even if they are authorized.

DAS detects attack signatures by logging primary events and then monitoring for completed attacks. Large tables are scanned "gently" over time using I/O controlled procedures – never using general selects. Total I/O utilization is controlled and budgeted.

Fine Errors / Business Unit Responsibility

Complex Business Rules Users / consultants must "instrument" the app Reference data comparisons (cross-server)
Statistical Distributions (sudden, significant changes) Minimum, Maximum, Average Bar Graphs, Group-By
Fraud Detection Digit Analysis (Benford testing) Financial audit tests of consistency

Fine errors, in or near the valid band, require more effort to detect and generate higher false positives. Designing tests to find such errors typically requires research, as well as in-depth knowledge of business rules, application design, and database schema. If not handled by business unit staff, this project is suitable for outside IT consultants.

Alerts and Reports / Security Issues

Various conditions detected by IPLocks DAS will be of interest to different groups within the organization. Within DAS you can create groups to receive and respond to alerts via e-mail or pager. Alerts are placed into periodic reports, and may be cleared by e-mail replies, or simply by fixing the error condition, whereupon they reset themselves.

To monitor system and application level data, IPLocks DAS requires highly privileged (read) access on the DBMS. However this risk can be mitigated by placing DAS inside the data center, where it communicates with response teams primarily via e-mails and replies.

Freestanding Audit Tool

IPLocks DAS acts as a read-only client, and is not in-line with your transaction path. It does not require any code on your servers and is not a new "layer" in your systems architecture.

Your application programmers should focus on P&L enhancing features. Creating, managing, and fine-tuning audit tests should occur in an external tool, to facilitate dynamic evolution of new controls on existing systems and foster consistent application across multiple systems.

Separating the surveillance tool from the system under observation strengthens controls on insiders. A third-party monitoring server provides clear confirmation and documentation for authorized changes, as well as notice of potentially unauthorized ones, thus providing an additional control on highly privileged users, who can bypass other administrative tools.

Appliance Format / Hardware Assisted

IPLocks DAS is delivered as a rack-mount appliance with browser based administration. Large customers prefer minimal install time and IPLocks assumes responsibility for hardware selection and compatibility. Offloading analytic processing to the DAS appliance minimizes performance degradation of the observed system. DAS can monitor multiple databases from a single unit, across platforms, without delays in porting to multiple operating systems.

Recommended Areas for First Use

IPLocks' Data Audit server is recommended for immediate deployment in high risk, high return areas such as:

- Applications moving to managed services, same team no longer maintaining them
- Applications downsizing from mainframe to Unix, where security needs are greater
- New e-services projects, especially high risk deployments (e.g., DBMS in DMZ)
- Any application requiring high data integrity (payment enabled, or reputation risk)

Summary

The IPLocks Data Audit Server (DAS) provides safe and effective near-real time content inspection for data intrusion monitoring and detection. It belongs in your enterprise security arsenal as an additional mission-critical line of defense.

Contact

IPLocks, Inc.
3393 Octavius Drive
Santa Clara, CA 95054

Tel: 408-748-2229
Fax: 408-748-2234

www.iplocks.com
sales@iplocks.com