# HCL Domino 14.5 Security and Compliance with SecurTrac.

This document covers an overview of the HCL Domino 14.5 Security and Compliance features and then highlights how SecurTrac doesn't just complement Domino 14.5, it elevates it into a truly audit-ready platform. This document also provides "use case" scenarios that demonstrate how SecurTrac can be used to help organizations in various industries meet compliance requirements.

Extracomm Inc.

9 /4 / 2025

# Table of Contents:

Table of Contents: ........ 1

Introduction: ........ 2

Security and Compliance Feature Overview in HCL Domino 14.5 ........ 2

SecurTrac – A Compliment to HCL Domino 14.5 Security and Compliance Features........ 3

How SecurTrac Enhances Compliance in Domino 14.5 ........ 3

SecurTrac Features and Capabilities ........ 4

Scenario Spotlights for SecurTrac on HCL Domino 14.5 ........ 5

Scenario Spotlight #1: Patient Data Access Monitoring in a Regional Hospital Network........ 5

Scenario Spotlight #2: Insider Threat Detection in a Multinational Bank ........ 6

Scenario Spotlight #3: Intellectual Property Safeguarding in a German Pharmaceutical Company ........ 7

Scenario Spotlight #4: NIS2 Compliance in a European Government IT Agency........ 8

Scenario Spotlight #5: Confidential Document Access Monitoring in a Corporate Law Firm ........ 9

Conclusion:........ 11

## Introduction:

HCL Domino 14.5 introduces a powerful set of native security and compliance features tailored for organizations operating in regulated environments. With advancements in AI governance, data privacy, secure communications, and accessibility, Domino 14.5 supports frameworks like GDPR, HIPAA, and the European AI Act. To meet deeper audit and monitoring needs, SecurTrac extends these capabilities with forensic logging, real-time alerts, and regulator-ready reporting, creating a comprehensive compliance solution for sectors such as healthcare, finance, and government.

## Security and Compliance Feature Overview in HCL Domino 14.5

- **Domino IQ (Sovereign AI Extension)**
  This new feature allows organizations to deploy AI models locally or via trusted partners, rather than relying on public cloud services. It's designed to help meet compliance requirements like the **European AI Act**, ensuring data sovereignty and governance.
- **Data Privacy Enhancements**
  Domino 14.5 is tailored for environments where **data residency and privacy** are critical. It ensures that sensitive data remains within trusted infrastructure, supporting compliance with regional privacy laws.
- **Security Event & Incident Management (SEIM) Tools**
  Built-in tools for monitoring and managing security incidents help organizations maintain audit trails and respond to threats in a compliant manner.
- **BSI-Certified Security Architecture**
  Domino 14.5 aligns with standards set by the **German Federal Office for Information Security (BSI)**, reinforcing its suitability for secure and compliant deployments in government and regulated sectors.
- **Improved Secure Messaging & Virtual Meetings**
  Updates to deployment options now offer more secure configurations for messaging and collaboration tools.
- **European Accessibility Act Compliance**
  The platform now adheres to the **European Accessibility Act**, making its web-based services more inclusive while also satisfying legal accessibility mandates.

These features make Domino 14.5 a strong candidate for enterprises and government agencies needing robust, native compliance capabilities. If you're working in a regulated industry, this release is definitely worth exploring further.

# SecurTrac – A Compliment to HCL Domino 14.5 Security and Compliance Features

While HCL Domino 14.5 introduces impressive native security and compliance features like AI governance with Domino IQ, BSI-certified architecture, and enhanced event monitoring, these alone may not fully satisfy the rigorous demands of modern regulatory frameworks. For organizations in healthcare, finance, or government, real-time visibility, granular audit trails, and proactive intrusion detection are essential.

That's where **SecurTrac** steps in. It fills the compliance gap by offering forensic-level logging, mail, database, user activity monitoring, and alerting for unauthorized access. These capabilities are all critical for meeting standards like GDPR, HIPAA, and SOX. SecurTrac doesn't just complement Domino 14.5, it **elevates it into a truly audit-ready platform**, ensuring that every action is tracked, every anomaly is flagged, and every report is regulator-ready.

## How SecurTrac Enhances Compliance in Domino 14.5

### 1. Audit Trail & Forensic Logging

- SecurTrac provides real-time monitoring of mail and application databases and user activity, including document open/create/update/delete actions, and database access attempts.
- This complements Domino 14.5's Security Event & Incident Management(SEIM) tools, giving organizations a full forensic trail for internal audits or external investigations.

### 2. Data Privacy & Access Controls

- Tracks who accessed sensitive data and when, helping enforce data residency and privacy policies.
- Helps compliment Domino 14.5's BSI-certified architecture to ensure that data access is logged and controlled in accordance with GDPR, HIPAA, or other frameworks.

### 3. Regulatory Reporting

- SecurSearch, SecurTrac's companion product generates detailed compliance audit trail reports that can be used for regulatory submissions or internal governance.
- These audit trail reports align with Domino 14.5's Domino IQ AI governance model, helping document how data and AI models are accessed and used.

### 4. Policy Enforcement

- Alerts administrators and/or IT Security teams when users violate access policies or attempt unauthorized actions.
- This supports Domino's secure messaging and collaboration features, ensuring that sensitive communications remain compliant.

### 5. Retention & Archiving

- Helps enforce data retention policies by tracking deletions and archive activities.
- Complements Domino's native tools for managing secure document workflows and lifecycle governance.

# SecurTrac Features and Capabilities

SecurTrac is designed to help organizations meet a wide range of **regulatory compliance requirements** by providing robust audit trails, real-time monitoring, and forensic-level logging across HCL Domino environments. Here are the specific regulatory frameworks SecurTrac helps to support:

**Supported Regulatory Frameworks**

| *Regulatory Framework* | *How SecurTrac Helps* |
|---|---|
| ***GDPR** (General Data Protection Regulation)* | Tracks access to personal data, logs deletions, and supports data subject access requests with detailed audit trails. |
| ***HIPAA** (Health Insurance Portability and Accountability Act)* | Monitors access to protected health information (PHI), detects unauthorized access, and supports breach notification requirements. |
| ***SOX** (Sarbanes-Oxley Act)* | Logs changes to financial data and access control lists (ACLs), helping ensure integrity and accountability in financial reporting. |
| ***NIS2** (EU Directive on Network and Information Security)* | Provides intrusion detection and real-time alerts for unauthorized access, supporting incident response and risk mitigation. |
| ***Internal Governance & Corporate Auditing*** | Offers full visibility into user and admin activity, supporting internal policy enforcement and audit readiness. |

**Key Compliance Capabilities:**

- **Mail Monitor**: Tracks open/send/receive/delete email actions across HCL Notes client and Web access.
- **Database Monitor**: Logs document and design element changes, ACL modifications, and agent activity.
- **Intrusion Detection**: Alerts on illegal access, unauthorized server use, and suspicious behavior.
- **Full Admin Logging**: Captures all HCL Domino Full Access Administration actions for accountability.

Together, Domino 14.5 and SecurTrac form a **compliance powerhouse**, ideal for industries like finance, healthcare, government, and legal services.

# Scenario Spotlights for SecurTrac on HCL Domino 14.5

**Notice:** The use cases presented in this document are fictional examples created for illustrative purposes only. They are not based on actual deployments or real-world implementations of SecurTrac or HCL Domino. Any resemblance to real organizations, events, or individuals is purely coincidental.

## Scenario Spotlight #1: Patient Data Access Monitoring in a Regional Hospital Network

**Challenge:**

A regional hospital network in California faced scrutiny after a whistleblower revealed that staff were accessing patient records without medical justification. Although no data breach occurred, the incident raised serious concerns about **HIPPA** (Health Insurance Portability and Accountability Act) compliance and internal data governance.

**SecurTrac in Action:**

Imagine a healthcare provider using Domino 14.5 and SecurTrac to manage patient records:

- Every access to a patient file is logged.
- Unauthorized attempts trigger alerts.
- Reports are generated for HIPAA and PHIPA audits.
- Role-based access is continuously monitored to prevent data leakage and ensure clinical accountability.

**SecurTrac Deployment:**

The hospital implemented **SecurTrac** across its HCL Domino-based electronic health record (EHR) system to:

- **Track access to patient files**, especially those flagged as sensitive (e.g., mental health, infectious disease)
- **Monitor administrative changes** to patient demographics and treatment plans
- **Detect unusual access patterns**, such as repeated views of celebrity or VIP records

**Key SecurTrac Features Used:**

- **Real-time alerts** for unauthorized access to protected health information (PHI)
- **Detailed audit logs** showing who accessed what, when, and from which device
- **Compliance reporting tools** aligned with HIPAA standards

**Outcome:**

- The system flagged a nurse who had accessed over 40 patient records unrelated to her caseload.
- Internal review led to retraining and policy updates, preventing future violations.
- The hospital demonstrated full audit capability during a State health inspection, earning commendation for proactive compliance.

---

This kind of visibility is essential in healthcare, where privacy violations can lead to legal penalties and loss of public trust.

---

## Scenario Spotlight #2: Insider Threat Detection in a Multinational Bank

**Challenge:**

A multinational bank with operations across North America and Europe needed to strengthen its internal security posture after a near-miss involving unauthorized access to sensitive loan documents. The incident didn't result in data leakage, but it exposed a gap in visibility over administrator actions and privileged user behavior.

**SecurTrac in Action:**

Imagine a global bank using Domino 14.5 with SecurTrac to manage internal communications and financial workflows:

- Every access to sensitive financial documents is logged, including who viewed, edited, or deleted them.
- Unauthorized attempts to access dormant accounts or restricted portfolios trigger immediate alerts.
- Reports are generated for internal audits and external reviews under SOX and other regulations.
- All administrative actions are traceable, supporting forensic investigations and regulatory transparency**.**

**SecurTrac Deployment:**

The bank deployed **SecurTrac** across its HCL Domino environment to monitor:

- **Admin-level access to financial databases**
- **Changes to customer loan records and investment portfolios**
- **Unusual login patterns from remote locations or odd hours**

**Key SecurTrac Features Used:**

- **Real-time alerts** for unauthorized document access
- **Audit trails** of who accessed what, when, and from where
- **Tamper-proof logs** for regulatory reporting (e.g., SOX)

**Outcome:**

- The bank was able to **identify a rogue employee** who had been accessing dormant client accounts to prepare for fraudulent transfers.
- SecurTrac's logs were used as **evidence in internal investigations**, and the employee was terminated before any financial damage occurred.
- The bank passed its next **external audit with zero findings**, thanks to the detailed activity reports generated by SecurTrac and its companion product SecurSearch.

---

This kind of proactive monitoring is a game-changer for financial institutions, especially when paired with Domino 14.5 SEIM tools and compliance frameworks.

---

## Scenario Spotlight #3: Intellectual Property Safeguarding in a German Pharmaceutical Company

**Challenge:**

A leading pharmaceutical company based in Frankfurt, Germany had recently secured a European patent for a novel immunotherapy drug targeting rare cancers. With competitors across the EU and Asia aggressively pursuing biosimilar pathways, the company faced a critical challenge: protecting internal access to proprietary drug formulations, clinical trial data, and regulatory dossiers stored within its HCL Domino infrastructure.

Given the sensitivity of the data and the risk of industrial espionage, the company needed airtight controls to comply with EU regulations and defend its intellectual property.

**SecurTrac in Action:**

Imagine a pharmaceutical company using Domino 14.5 and SecurTrac to manage proprietary drug research:

• Every access to clinical trial data and formulation documents is logged across R&D and regulatory teams.
• Unauthorized access attempts, especially by contractors or external collaborators trigger alerts.
• Reports are generated for GDPR audits and inspections by e.g.: Federal Institute for Drugs and Medical Devices (BfArM) OR European Medicines Agency (EMA).
• Document-level tracking ensures compliance with EU Trade Secrets Directive and internal IP protocols

**SecurTrac Deployment:**

The company deployed **SecurTrac** to monitor and control access to:

- **Formulation blueprints** and **compound synthesis protocols**
- **Clinical trial results**, including adverse event logs and efficacy data
- **Regulatory submission documents** for EMA and national health authorities

**Key SecurTrac Features Used:**

- **Granular access tracking** for R&D, legal, and regulatory teams
- **Real-time alerts** for unauthorized document views, edits, or deletions
- **Audit trail logs** to support IP litigation and internal investigations
- **Access monitoring** to detect and report anomalous activity

**Legal & Regulatory Alignment:**

- **GDPR Compliance**: SecurTrac ensured that all access to personal data within clinical trials was logged and auditable, fulfilling Article 5 and Article 32 requirements for data integrity and security.
- **EU Trade Secrets Directive**: By maintaining detailed access logs and demonstrating proactive protection of confidential business information, the company met the burden of proof required to defend its trade secrets in court.
- **Pharmaceutical Law (AMG)**: SecurTrac supported compliance with German laws by logging user activity related to regulatory documentation and ensuring traceability of data handling.

**Outcome:**

- SecurTrac flagged an internal contractor who attempted to access restricted data outside approved working hours.

- The incident was contained immediately, and the audit logs were used to demonstrate regulatory compliance during a surprise inspection by the Federal Institute for Drugs and Medical Devices (BfArM).
- The company's legal team credited SecurTrac with preserving the integrity of its patent portfolio, helping maintain exclusivity across the EU and reinforcing investor confidence.

In Germany's tightly regulated pharmaceutical landscape, data protection isn't just a best practice—it's a legal imperative. SecurTrac empowers companies to meet that standard while defending the innovations that define their future.

## Scenario Spotlight #4: NIS2 Compliance in a European Government IT Agency

**Challenge:**

A national IT agency in Germany manages secure communication platforms for multiple government departments, including justice, finance, and public health. With the **NIS2 Directive** now in force, the agency is classified as an essential entity and must comply with strict cybersecurity obligations—including incident reporting, access control, and auditability.

**SecurTrac in Action:**

The agency uses HCL Domino 14.5 for secure messaging and document workflows, and deploys SecurTrac to manage secure communications and citizen data in order to meet NIS2's operational and reporting mandates:

- Every access to classified documents and citizen records is logged, including admin actions.
- Unauthorized access or misconfigured permissions trigger alerts and automated incident reports.
- Audit trail reports are generated for national CSIRT reviews and NIS2 compliance audits.
- System-wide visibility supports rapid response and accountability across departments.

**SecurTrac Deployment:**

SecurTrac is configured to:

- Monitor **access to sensitive government documents**, including classified memos and citizen data
- Track **administrative actions** such as database configuration changes and user role assignments
- SecurTrac's companion product, SecurSearch generates audit trail logs **f**or internal reviews and external inspections

**NIS2 Requirements Addressed:**

| *NIS2 Requirement* | *SecurTrac Capability* |
|---|---|
| *Risk Management & Access Control* | Tracks and alerts on unauthorized access to sensitive systems and data |
| *Incident Detection & Reporting* | Provides real-time alerts and detailed logs to support 24-hour “early warning” reporting |
| *Business Continuity & System Recovery* | Enables forensic analysis post-incident to support recovery and prevent recurrence |
| *Corporate Accountability & Oversight* | Supplies audit trail reports for board review and compliance documentation |
| *Asset & Data Handling Procedures* | Logs all user interactions with critical assets and sensitive data for traceability |

**Outcome:**

- A misconfigured access policy allowed a junior staffer to view restricted budget documents.
- SecurTrac flagged the anomaly instantly, and the agency submitted a **timely incident report** to its national CSIRT, fulfilling NIS2’s 24-hour early warning requirement.
- The agency used SecurTrac’s logs to revise its access control policies and demonstrate **full compliance** during a follow-up audit by the **Federal Office for Information Security (BSI)**.

---

In the age of NIS2, visibility and accountability are non-negotiable. SecurTrac empowers public and private entities to meet these standards with confidence. Want to explore how this could apply to a telecom provider or energy grid operator next?

---

### Scenario Spotlight #5: Confidential Document Access Monitoring in a Corporate Law Firm

**Challenge:**

A corporate law firm headquartered in Toronto faced reputational risk after a high-profile client raised concerns about unauthorized access to privileged documents. While no breach was confirmed, the firm struggled to produce a clear audit trail of who accessed sensitive documents and when. This exposed gaps in its internal data governance and raised compliance concerns under PIPEDA (Personal Information Protection and Electronic Documents Act) and Law Society of Ontario guidelines.

**SecurTrac in Action:**

Imagine a corporate law firm using Domino 14.5 and SecurTrac to manage client contracts, litigation files, and internal communications:

- Every access to confidential documents is logged with precision
- Unauthorized access attempts trigger real-time alerts to compliance officers

- Reports are generated for PIPEDA and Law Society audits
- Administrative actions are fully traceable, supporting ethical governance and client trust

**SecurTrac Deployment:**

The firm implemented SecurTrac across its HCL Domino-based document management system to:

- Track access to privileged case files, including merger agreements, litigation strategies, and client correspondence
- Monitor administrative changes to user roles, document permissions, and access rights
- Detect unusual access patterns, such as repeated views of high-profile client files by non-assigned staff

**Key SecurTrac Features Used:**

- Real-time alerts for unauthorized access to confidential legal documents
- Detailed audit logs showing who accessed what, when, and from which device
- Compliance reporting tools aligned with PIPEDA and Law Society of Ontario standards

**Outcome:**

- The system flagged a junior associate who had accessed sealed litigation files outside their assigned casework
- An internal review led to policy updates, role-based access refinements, and staff retraining on ethical data handling
- During a client-initiated audit, the firm demonstrated full audit capability and earned praise for its proactive compliance posture

---

This kind of visibility is essential in legal services, where confidentiality breaches can result in malpractice claims, regulatory penalties, and loss of client trust.

---

## Conclusion:

As regulatory expectations continue to evolve across industries, organizations must adopt solutions that not only meet baseline compliance requirements but also provide the depth, visibility, and responsiveness needed to safeguard sensitive data. HCL Domino 14.5 delivers a strong foundation with its native security and governance features, offering enhanced privacy controls, certified architecture, and secure collaboration capabilities. However, for enterprises operating in highly regulated sectors, these features are most effective when paired with the leading compliance solution for HCL Domino, which is SecurTrac by Extracomm Inc.

SecurTrac extends Domino 14.5's compliance posture by delivering real-time monitoring, forensic-level audit trails, and actionable alerts, ensuring that every access, modification, and administrative action is fully traceable. Its alignment with key regulatory frameworks such as GDPR, HIPAA, SOX, and NIS2 makes it an essential tool for organizations seeking to maintain operational integrity and audit readiness.

Together, Domino 14.5 and SecurTrac offer a comprehensive, scalable, and regulator-ready compliance ecosystem, empowering organizations to move beyond reactive security and toward proactive governance.

If you would like more in-depth technical information or wish to learn more about SecurTrac or other Extracomm products, please visit our web site: http://www.extracomm.com

**Extracomm Inc.**

**1730 McPherson Court Unit 6**

**Pickering, Ontario**

**Canada, L1W 3E6**

**Tel: 905-709-8602**

**Fax: 905-709-8604**

http://www.extracomm.com

***Product names, logos, brands, and other trademarks featured or referred to within this document are the property of their respective trademark holders.***