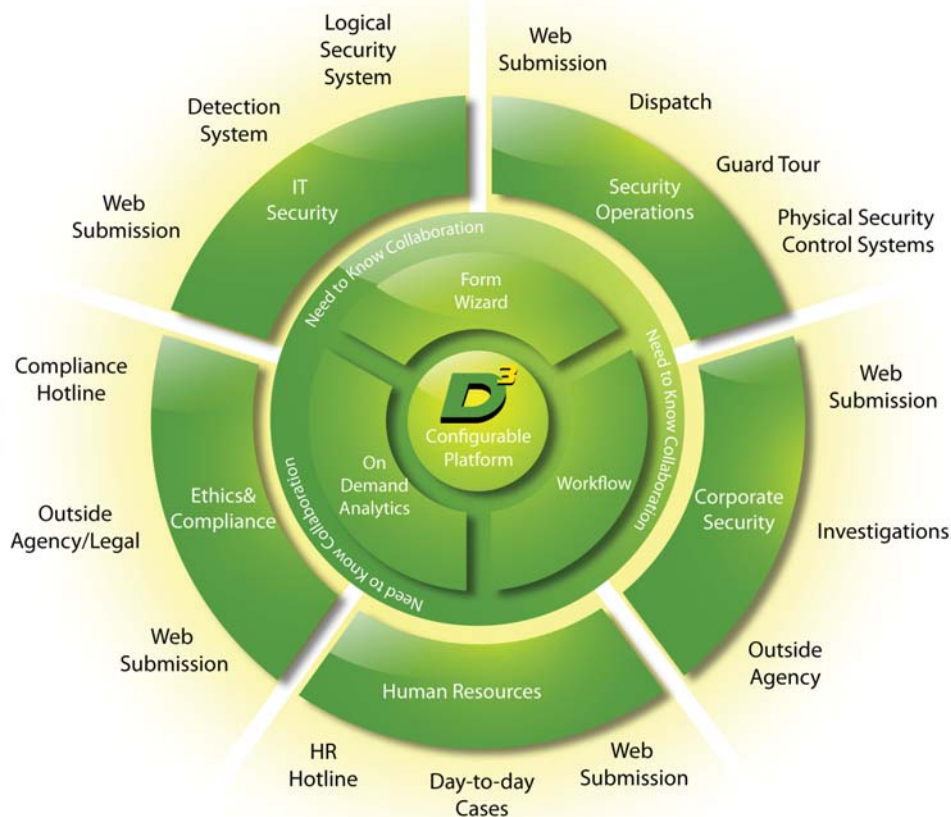


Enterprise Incident Reporting and Case Management

When incidents occur where individual behavior puts your organization at risk, a repeatable and discoverable incident management process is required. The Security professional requires an easy-to-use solution that solves the business need for configurable data collection, workflow and analysis. By enabling collaboration, ensuring compliance and permitting organizational convergence, D3's Incident Reporting and Case Management solution allows incidents and records to exist in a one-to-one ratio regardless of origination.

D3 Incident Reporting and Case Management also solves the business need to capture consistent data from multiple origination channels. Incidents originate from user input, complementary modules and third-party solutions (access control, alarm monitoring, CCTV and others). By providing a common incident repository, D3's Incident Reporting and Case Management solution eliminates redundant proprietary databases, increases efficiency and maintains data integrity. Finally, all incident activity is managed through a consolidated view allowing the creation of Tasks and Links.



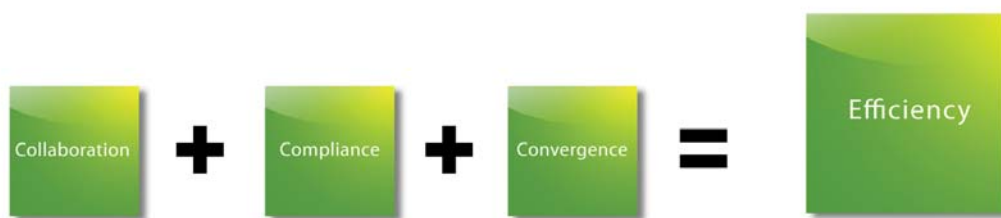
Vancouver Office:
Suite 602, 535 Thurlow Street
Vancouver, BC
V6E 3L2

Toronto Office:
Suite 4, North Service Road W.
Oakville, ON
L6M 2W1

Tel: 1-800-608-0081 xt 102
E-mail: sales@d3security.com
www.d3security.com

Through 3-tier access control, the D3 Incident Reporting and Case Management module enables clear definition of user privileges. According to a user's site, group or role membership, access to information and functionalities can be granted or denied to fit each customer's unique environment.

The D3 equation - collaboration, compliance and convergence solves the Security professional's business needs with an easy-to-use and customizable Incident Reporting and Case Management solution.



Collaboration

When managing incidents, collaboration requires communication and data sharing while maintaining need-to-know boundaries for legal and privacy purposes. For Security, effective case management regularly requires collaboration with Corporate Security, IT Security, Ethics & Compliance and Human Resources teams. Traditionally, each function maintained its own case management system. Upon communication, each involved team created an incident in their own system. As a result, senior management received inconsistent analytics because multiple reports existed in various systems pertaining to a single event, making accurate statistics labor intensive and in-depth analysis impossible. Today, D3's Enterprise Incident Reporting and Case Management, when leveraged by multiple business units, solves the business need for rapidly accessible and consistent analytics where records and events exist in a one-to-one ratio.

Moreover, convergence results in Corporate Security, IT Security, Ethics & Compliance and Human Resources being colleagues, making collaboration imperative rather than tolerated. D3's Enterprise Incident Reporting and Case Management solves the business need for easy collaboration that enables ad-hoc, automated and secure information sharing through a common repository, eliminating redundant proprietary databases, increasing efficiency and maintaining data integrity. By capturing all incident activity through a consolidated view, actions and links are easily managed.

Employing forms and fields configured specifically to the Security professional's needs, D3's Enterprise Incident Reporting and Case Management fits any environment. Likewise, D3 accommodates business unit specific workflow for driving approvals, notifications, escalations and task assignments. D3's Enterprise Incident Reporting and Case Management facilitates awareness and minimizes security risk by empowering trend discovery.

Vancouver Office:
Suite 602, 535 Thurlow Street
Vancouver, BC
V6E 3L2

Toronto Office:
Suite 4, North Service Road W.
Oakville, ON
L6M 2W1

Tel: 1-800-608-0081 xt 102
E-mail: sales@d3security.com
www.d3security.com



Compliance

Compliance begins with repeatable and discoverable case management. A business that inconsistently captures front-line incident data increases its regulatory exposure. The nature of Security cases requires the collection of personal data for compliance with regulatory requirements. At the same time, the data collected poses other risks if compromised. D3's Enterprise Incident Reporting and Case Management provides the best solution to both business problems with its dynamic data entry and thin client architecture.

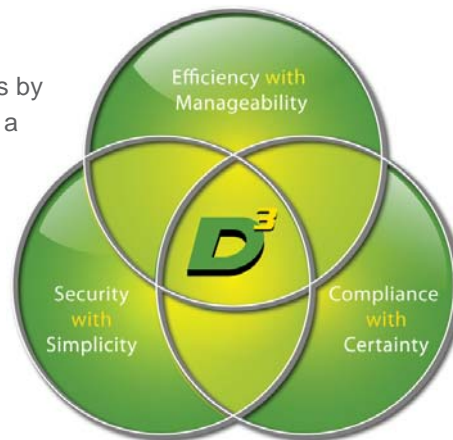
Dynamic data entry permits customization of the actual data requested from end users based upon the Incident Type or Field Option selected. Each response drives subsequent information requests. As a result, the granularity of data collected matches the requirement. The time wasted entering non-relevant data is eliminated and storing data that poses regulatory consideration is minimized.

Thin client architecture ensures all data resides at the server level. With D3's Enterprise Incident Reporting and Case Management, an accessing device never caches data. When the browser session ends, all data disappears from the desktop or laptop. Through this safeguard inherent in D3's architecture, your organization's case data remains safe on secure servers that do not travel with you or your team members where the data is subject to loss.

Convergence

Incidents originate from multiple channels. D3's Enterprise Incident Reporting and Case Management empowers Security professionals by solving the business need for systemic data capture that maintains a discoverable audit trail and chain-of-custody, regardless of origination. In large organizations, convergence of Corporate Security, IT Security, Human Resources and Ethics & Compliance under the same reporting structure presents numerous business needs that D3 solves, including:

- Need-to-know policy enforcement through 3-tier access control
- Consistent analytics through common enterprise platform
- Customizable workflows that trigger repeatable actions such as:
 - Collaborations
 - Approvals
 - Notifications
 - Escalations
 - Task Assignments



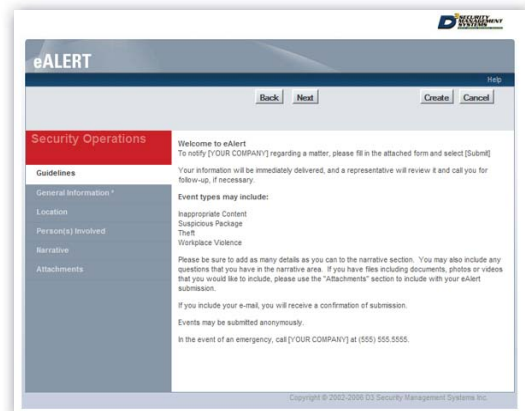
Vancouver Office:
Suite 602, 535 Thurlow Street
Vancouver, BC
V6E 3L2

Toronto Office:
Suite 4, North Service Road W.
Oakville, ON
L6M 2W1

Tel: 1-800-608-0081 xt 102
E-mail: sales@d3security.com
www.d3security.com

e-Alert

Opening incident submission to all company employees and the public is essential to many organizations. D3's e-Alert module permits any individual with access to an organization's Intranet or Internet to open a configured form to report an event. Upon submission, the data may trigger notifications and route the e-Alert to the responsible Security professional's virtual Security Operations Center (vSOC) Dashboard. Upon accessing his or her Dashboard, the system prompts a human audit where an event may be escalated to an incident report or archived.



Notification and Workflow Automation

D3's Enterprise Incident Reporting and Case Management contains an embedded notification engine. The D3 Notification feature enables information dissemination to appropriate persons based upon customizable triggers.

Similarly, the D3 Workflow feature permits the initiation of basic to complex scenarios for automating business processes. Utilizing a configurable wizard, D3's Workflow feature solves the business need to automate numerous tasks that previously required manual completion.

Scenario: If an incident of the type "Theft" were reported, and in the "Theft Details" section, the user indicated the theft involved an "Access Control Badge". Upon selecting "Access Control Badge", an automated notification could be sent requesting badge deactivation and a task assigned to create a new badge for the victim. Workflows may include approvals, escalations, routings, task assignments or collaborations.



Vancouver Office:
Suite 602, 535 Thurlow Street
Vancouver, BC
V6E 3L2

Toronto Office:
Suite 4, North Service Road W.
Oakville, ON
L6M 2W1

Tel: 1-800-608-0081 xt 102
E-mail: sales@d3security.com
www.d3security.com

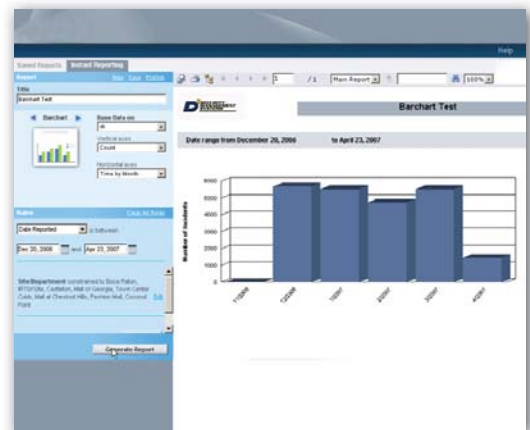
Analysis Reports

Security professionals need data to drive decisions. Until data drives decisions, the data adds no business value. D3's Analysis Reports feature solves the business need for ad-hoc, dynamic and real-time data analysis that can be used to make decisions. All data entered into D3's Enterprise Incident Reporting and Case Management may be queried to generate graphical and tabular reports for analysis purposes. Assessment of data leads to refinement of resource use, increased operational efficiency and pre-compiled data for risk assessment and planning. Of similar importance, D3's Analysis Reports, when leveraged by Corporate Security, IT Security, Ethics & Compliance as well as Human Resources, solves the business need for rapidly accessible and consistent analytics across business units.

D3's Analysis Reports Instant Report feature enables user-defined and ad-hoc reports, allowing users to set vertical, horizontal and columnar criteria using any data field. Users may save or publish Instant Reports upon definition, allowing rapid generation of commonly used reports. With powerful on-the-fly tools, D3 permits the creation of reports from any field.

Reports may include:

- **Trend**
- **Problem Areas**
- **Successful Mitigation Strategies**
- **Resource Allocation**
- **Performance**



Mobile Incident Reporting and Case Management

D3 Mobile Incident Reporting and Case Management solves the business need for front-line personnel to create an Incident Report while roaming, synchronize and continue modification upon return to a computer terminal. Synchronization updates the server and may trigger notifications and workflows, reducing lag time between an officer recording an incident and action. With Windows Mobile devices featuring cameras or microphones, officers can efficiently document incidents by attaching relevant pictures or voice-recordings to an incident report.



Vancouver Office:
Suite 602, 535 Thurlow Street
Vancouver, BC
V6E 3L2

Toronto Office:
Suite 4, North Service Road W.
Oakville, ON
L6M 2W1

Tel: 1-800-608-0081 xt 102
E-mail: sales@d3security.com
www.d3security.com

Administration Tool Kit

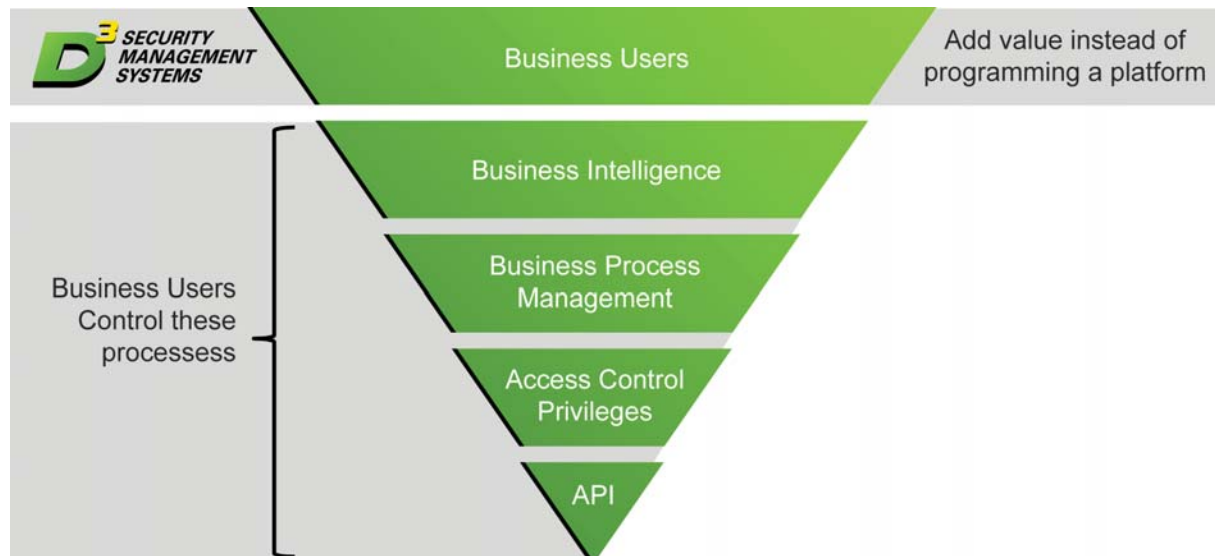
A single back-end framework used to configure all D3 Modules, the Administration Tool Kit empowers system administrators to change and grow the system to reflect the requirements of a dynamic environment. In addition, the D3 Administration Tool Kit uses the same business unit logic as the front-end solutions, allowing multiple levels of access control for adding, editing or viewing system configurations.

In creating the Administration Tool Kit, D3 invested significant resources to develop a Flexible Form Generator allowing full configuration of all application attributes. As a result, configurations are in the hands of business users designated as administrators. D3 does the initial configuration as part of our Total Customer Care experience, and any additional configurations can easily be performed by system administrators. As such, scarce IT resources are not required.

Key functionality of the Administration Tool Kit:

- **Configure data collection forms**
- **Manage user access control privileges**
- **Manage functions users may execute**
- **Configure Notifications and Workflow**

WYSIWYG form Wizard + Configurable Workflow + On-demand Analytics = Empowered Business User



Vancouver Office:
Suite 602, 535 Thurlow Street
Vancouver, BC
V6E 3L2

Toronto Office:
Suite 4, North Service Road W.
Oakville, ON
L6M 2W1

Tel: 1-800-608-0081 xt 102
E-mail: sales@d3security.com
www.d3security.com