



## Protecting Insurance Systems and Data with Access Governance Framework

*It's the nightmare that keeps IT executives at insurance companies up at night: the news that thousands, or tens of thousands, of customer files have been stolen and are probably in the hands of identity thieves or other crooks. It means government sanctions, the expense of tracking and fixing the security breach, explanations and possibly compensation to customers, and the long-term loss of credibility and trust -- something no financial services firm can succeed without. Insurance firms need IT security that can monitor and prevent unauthorized access, but which doesn't take months to deploy and doesn't come with a huge price tag. Pinnacle Security Solutions' all-in-one pinSpark application was created specifically to provide an easy solution for reducing security risks, ensuring regulatory compliance, and enforcing access governance to pre-defined IT security and user access policies.*





## The \$35 Million Security Breach

Insurance company executives have plenty of reasons to be concerned about the security of their data. In their companies' IT systems, there may be hundreds of thousands of consumer identities, as well as their financial and employment data, past addresses, lists of assets and, in life insurance companies, information on relatives and other beneficiaries. Health insurance firms have medical histories that could seriously damage their customers if leaked or stolen. Any insurance firm has personal customer data that is vulnerable to identity theft, by hackers or even its own employees. Employee theft is often more difficult to prevent, and often just as damaging, as an outside hack: A major insurance company in California was victimized by an employee who secretly downloaded 20,000 customer profiles each week and sold them to an associate.

Insurance companies, like all financial services firms, are required by law to have security policies in place to protect their customers' personal and financial data, and safeguards against unauthorized access to the IT systems that houses that data. If a breach occurs, a company faces investigations and fines from government officials, legal fees, lawsuits, and a tarnished public image. According to a survey by the Ponemon Institute and reported in *Insurance Technology*, **the average cost of an IT security breach for a company is \$6.3 million, and for financial services firms, these costs tend to be even higher--as high as \$35 million in some cases.**

Pinnacle Security Solution's pinSpark application provides a fast and reliable solution for controlling access to your company's IT systems and preventing unauthorized users from getting near sensitive data. The pinSpark all-in-one suite includes an access governance component for managing user identities and their IT access role and entitlements, risk analysis and remediation capabilities, and compliance reporting on user access. The pinSpark solution protects access to data *without* costing a fortune in employee time, consulting costs or license fees

## The Three Components of IT Access Security

A sound system of IT access security must include three key components: IT governance, risk reduction and compliance management. This is often known as IT-GRC. CISOs and CIOs must implement a system of

governance over the granting of end-user access to IT systems in order to reduce the risk of security breaches and ensure compliance with federal and industry regulations. The IT Policy Compliance Group's *2008 Annual Report on IT Governance, Risk and Compliance*, found that companies with ***well-defined and automated governance and compliance systems had 96% lower financial losses from the theft of customer and competitive data, and 50% less in annual expenditures for regulatory compliance***

However, creating and implementing a set of effective security policies and enforcement mechanisms is a potentially complex and costly issue for firms with branch offices and multiple IT systems. But with pinSpark, the process is much easier and faster.

To help IT executives determine their current security risks, pinSpark creates a comprehensive risk profile, based on who has access to which applications, and at what security level. The CIO or CISO can use pinSpark's Business Intelligence Reporting tool to view reports and dashboards, and drill down into them for more details.

For CIOs who need proof of compliance with federal regulations, pinSpark's certification management component checks and certifies that IT processes comply with the set policies, whether federal, state or corporate

For example, under SOX, organizations must maintain Separation of Duties (SOD)—the person who bills a vendor should not be the same one who records a payment from that vendor. pinSpark's Access Certification Compliance component allows administrators to assign separation-of-duty warnings to different roles and will send an alert to the administrator when a separation of duty violation occurs. Depending on the severity of the SOD violation, the alert may take the form of an immediate email or a warning note in the monthly report.

## Pattern-based Role Engineering and Automation with pinSpark

To reduce the time and cost of provisioning employees, and to ensure it is done in accordance with regulatory and corporate policies, pinSpark provides automated role creation and management. IT and business managers can quickly create, change, assign, certify, and de-assign roles via a user-friendly interface according to a pre-determined system of access governance.



Role creation and management entails grouping various account privileges and access rights into a single profile, or role, such as “New England Customer Service Rep.” Employees with the same job or, at least, similar IT needs, can be assigned the same role. By the same token, people may have multiple roles, such as “claims processing” and “senior manager,” that assign them additional privileges. Roles can speed the provisioning process by enabling IT to activate many employee accounts at once, rather than painstakingly assigning accounts by hand, one by one. A user-centric interface makes role creation especially easy in pinSpark, and provides role suggestions, role assignment, and customizable role-based reports. The role information is sent to the company's provisioning or identity and access management system, such as those by CA, IBM, Novell and others.

## How Does pinSpark Help Achieve Regulatory Compliance?

Pinnacle Security Solution's pinSpark enables insurance companies to achieve compliance, boost productivity, and drive down costs in five key areas:

**Usage Monitoring and Management.** pinSpark's Role Management and Usage Monitoring does periodic checks on user accounts, roles, and how often they are used. This allows IT to spot unnecessary, unused roles and account privileges and to delete them.

**Risk Profiling and Remediation.** The Risk Management module uses the role and usage data to assess potential risks, report on risk factors, and provide intelligent risk reduction.

**Compliance Certification.** The Compliance Access Certification function certifies that the company is in compliance with defined policies—including those based on regulatory requirements such as SOX.

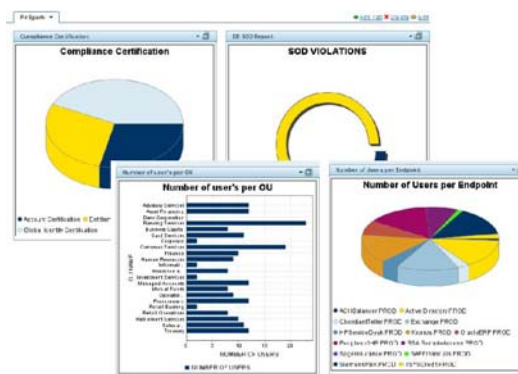
**Separation of Duties.** The former claims adjudicator who now works in office administration should not still be able to access to sensitive claims information. That's a potential security breach. But removing access from workers who are promoted or leave the company is time consuming and usually at the bottom of IT's to-do list. However pinSpark prevents this conflict of interest by performing Separation of Duty (SOD) checks based on corporate or regulatory policies, and reports conflicts, while also handling any

necessary remediation.

**Flexible Delivery Options.** The pinSpark is a modular suite and is available as an in-house application or as a Software-as-a-Service (SaaS) subscription. An organization can subscribe to pinSpark's SaaS version, saving it the initial capital investment and the cost of ongoing maintenance/support

**Assurance in Real-Time.** When it comes to your organization's critical business information, real-time visibility of user access is key. So pinSpark has user-friendly dashboards to make real-time monitoring and management of user access simple. Some of the features pinSpark provides are:

- Easily view compliance certification status and SOD violations with drill-through capabilities
- Ensure the escalation and remediation of user access threats
- Monitor current user access activities against historic data and trends
- Quickly build, generate and export customized reports based on the data you need now



## Role Management, Governance, and Compliance in One Package

Perhaps the most important value provided by pinSpark's role management and security features is that they are all included in a single, integrated suite. Our enterprise solution provides a comprehensive package of: role, risk, policy, certification, and reporting management functions suited for medium to large insurance providers. It's an all-in-one solution developed to meet the complex IT compliance and security needs of the insurance industry. pinSpark is user-friendly, easy-to-deploy, and an affordable solution to IT security and compliance concerns.



## **About Pinnacle Security Solutions, Inc.**

Headquartered in Alpharetta, Georgia, Pinnacle provides the industry's most comprehensive role-based access governance – pinSpark. pinSpark minimizes the user access risks that threaten large organizations by automating the complex processes that determine who has access to critical business information. This allows companies to reduce user administration cost, mitigate user access risk and enforce regulatory compliance in a way that's simple and cost-effective.

For more information on pinSpark, please visit [www.pinsecure.com](http://www.pinsecure.com). Or call 1-888-504-8472



**Pinnacle Security Solutions, Inc.**  
12600 Deerfield Parkway,  
Suite 100,  
Alpharetta, GA 30004  
[www.pinsecure.com](http://www.pinsecure.com)  
[sales@pinsecure.com](mailto:sales@pinsecure.com)