

# *synnovation*



Vol. 1 Issue 3

## Beating the Odds

Leading an organization through a risk-laden environment is often a game of chance. But enterprise risk management can help your odds.

### EDS

Unwelcome Surprises

By Al Decker

### Towers Perrin

Coming of Age

By Prakash Shimpi

### Microsoft

Defending the Crown Jewels

By Ron Markezich

### Oracle

Protect, Detect, Deploy

By Vipin Samar

### Dell

Super Power

By Dr. Reza Rooholamini

### Sun Microsystems

Tapping Tag Power

By Jim Del Rossi

### Xerox

For the Record

By Charles P. Brett

### EMC

Reaching Out

By Gregg Therkalsen

### Cisco Systems

A Matter of Self Defense

By Bob Gleichauf

---

### EDS

Conversations

With Ron Rittenmeyer

### Microsoft

Up Close and Personal

With Ron Markezich



# PROTECT, DETECT, DEPLOY

By Vipin Samar,  
Oracle Corporation

Managing Compliance and Internal Risks

**N**efarious hackers bent on stealing corporate secrets. Natural disasters causing power outages and logistics disruptions. For years, outside forces like these have been the basis for an organization's security and risk management decisions.

But over the past few years, traditional security and risk threats have been augmented, even usurped, by two factors that most companies had previously ignored: compliance concerns and internal threats. In fact, compliance issues and internal threats are driving many organizations to reconsider how they address security privileged users, and overall risk management strategy. One result is a new approach to managing compliance and risk called protect, detect, and deploy. >>

We're not saying everyone's DBA or systems administrator is untrustworthy, but rather organizations need to ensure preventative measures are put in place.

Protecting is really about making sure that your data and systems are protected from both outsiders and insiders, whether inside or outside the database, and whether the data is at rest or in motion. This could mean encryption to ensure that nobody else can look at the data, or it could mean putting policies and authorization controls in place to keep unauthorized users from seeing the data. Detect means ensuring that one can detect what's happening within the environment, and audit it if

necessary. Normally, users are able to do whatever they're authorized to do, but the detect pillar would allow organizations to monitor what's done—even by authorized users—and provide auditing information to verify. Lastly, the deploy pillar simply means that organizations need to deploy security, compliance, and risk management capabilities in an efficient manner, while bringing efficiencies to the organization.

### The Compliance Challenge

All public companies in the United States today—and increasingly in Europe, Asia, and other parts of the world—must comply with regulatory legislations such as Sarbanes-Oxley. In addition, there are industry-specific regulations such as HIPAA, Gramm-Leach-Bliley (GLB), BASEL II, HSPD-12, PCI, and more. Outside the United States, there are regulations such as JSOX, and the EU and Japan privacy laws. These new regulations share a number of common requirements to provide greater control over business and IT processes:

- protect data from unauthorized access
- assess and monitor the risk that the business carries
- ensure separation of duty such that one person alone can't subvert the processes
- place compensating controls on privileged users to mitigate the risks
- demonstrate compliance to an audit team on a regular periodic basis

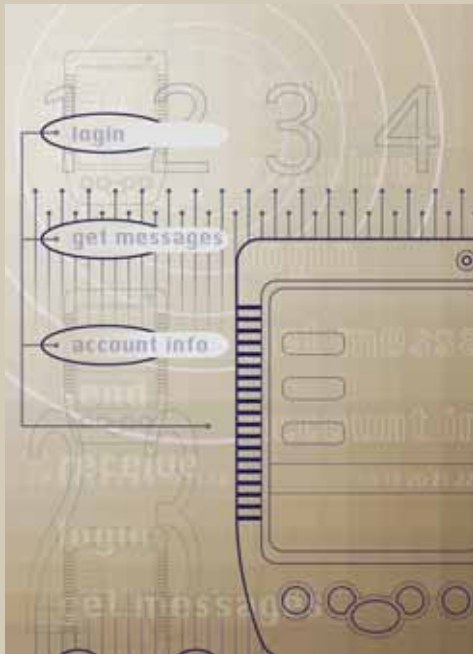
While regulatory compliance has been seen as a huge task faced by enterprises, one of the biggest benefits has been increased awareness of security and operational risks among the executives. These threats have forced organizations to



take a hard look at risks of their business practices, including the almost unlimited powers of privileged users, strong internal controls, and separation of duty. As a result, organizations need to document not only how they manage risks, but who has access to information—and how people can get into specific systems. This point brings us to the second change that's driving new security approaches: the increasing need to protect against insider theft, attack, or inadvertent modification of data, database records, or database structures.

### The Internal Threat Challenge

Most enterprises are reasonably well protected from outside hackers, thanks to firewalls, DMZs, and so on. But detecting and managing key users—especially developers, managers, and even IT administrators, who may have extraordinary access levels—is a particularly important task. In many cases, organizations find that super users (anyone from IT administrators to managers to database DBAs) may have access to every piece of data within a system. For example, an e-mail administrator of any company can probably read the e-mail of every employee in the company, or the administrator of the financial system can read the financial records. The keys to the kingdom have to be protected from the insiders. Some research reports say that a full 80 percent of threats are now coming from insiders, and organizations



## IT Infrastructure for Compliance and Internal Threat Mitigation

### Protect

- control access to data
- protect data from tampering
- control configuration changes

### Detect

- audit and monitor sensitive events
- configure alerts and reports
- automate compliance policies

### Deploy

- centrally provision, authenticate, and authorize users
- streamline operations
- easy to manage

are much more concerned about the internal threat today than ever before.

We're not saying everyone's DBA or systems administrator is untrustworthy, but rather organizations need to ensure preventative measures are put in place. They need the ability to enforce operational policies on who can access data, and when and where.

In addition, most applications today were not designed with the principle of least privilege—meaning that the application should run with the minimum privileges necessary. In fact, the situation is exactly the opposite, opening up both the administrators and the organizations to potential risk.

### The Double Whammy

Compliance and internal threats are driving organizations to reconsider how they address security and privileged users. Even if the employees are trustworthy (they usually are), organizations need to put procedures in place to ensure that data is not stolen, leaked to unauthorized users, tampered with, or simply modified by mistake. As a result, organizations have started to place boundaries around administrative functions, typically through processes that provide some basic level of auditing and ad hoc tools, such as tools that provide passwords that can only be used during specific hours or at specific times for maintenance.

However, compliance and protection from internal threats, when done manually, is very expensive. It takes a lot of resources in time, money, and energy, and more than that, it still doesn't provide strong assurance. And, unfortunately, it's only going to get worse as new, tighter regulations are passed in future years.

### Protect, Detect, and Deploy

A good place to start managing risk and meeting compliance requirements is at the core—with the database. Databases are the foundation for all corporate information, and they play an important role in mitigating risk and ensuring compliance. Organizations should protect data by restricting access and maintaining tight control. They should put mechanisms in place to detect any unauthorized or suspicious activities or changes, and they need to be able to deploy such solutions in a streamlined and automated way that works seamlessly with existing applications, databases, and IT infrastructure components.

Let's take a closer look at each pillar of security and how it relates to databases:

- **Protect:** Control who has access to the data, automate access management, and if required, encrypt the data. An organization must establish and maintain control over user permissions and privileges, and >>

profile data in order to restrict access to data, applications, operating systems, and infrastructure to only authorized users.

- **Detect:** You need a private eye that is ON all the time—one that automatically flags suspicious activity and generates reports on demand. Audit and reporting capabilities essentially demonstrate that controls are in place and working. This helps provide proof of compliance.
- **Deploy:** You must be able to deploy systems easily to streamline operations alongside your existing applications and systems. For example, you must provide an environment where privileges are created, approved, and issued via a centralized process that ensures the proper process is followed, including requiring approval from all appropriate parties before access is granted.

These principles should guide any database-centric approach to segregating enterprise data and ensuring the necessary roles-based controls. Properly supported, protect, detect, and deploy aims to stop improper access to enterprise data—thereby mitigating the risk of internal threats.

### **PROTECT:** **Reducing Internal Threats**

One approach to greatly reducing the risk posed by employees with access to both the database data and the administrative functions of the database is through the use of database realms (or database vaults).

A realm is a protection boundary or data firewall that can be defined around one or more database objects or application accounts such that only authorized users can access this data. Here, even users with DBA privileges or other broad system privileges can't misuse their rights to bypass the protection boundary created by the database realm. Realms are easy to define for existing applications, and once in place, they prevent powerful users such as the DBA from getting at application data. In addition to a blanket control over who is allowed in, one can also attach policies, conditions, and rules for accessing the realm protected data.

Let's take a look at an example of a database realm.

Properly supported, protect, detect, and deploy aims to stop improper access to enterprise data—thereby mitigating the risk of internal threats.



Perhaps we have a typical database with an HR application on it. The average DBA responsible for maintaining such a system typically has the ability to view salary and a whole set of privacy-related information about the company's employees. With a database realm around the HR application, access to the HR data is now restricted to only the authorized users. The DBA also can't create new users and assign privileges to those users. They can, however, continue doing their daily duties such as tuning, backups, and other maintenance tasks.

Another security issue is that application owners tend to have very powerful privileges. In a consolidated environment, it's likely that you'll have more than one application, and thus there are several powerful users in the database above and beyond the DBA. In this example, it's possible for the human resources DBA to look at the financial application data; something that would make the compliance team nervous. Obviously this wouldn't be a good situation, especially if it was during the financial reporting quiet period. Using a database realm, the financial application can be protected from powerful application owners.

With database realms, the administrators stay within their boundaries. No sniffing, no snooping. Everybody is protected—now the DBAs are no longer immediately under suspicion if something goes wrong—and they have the system-level protection that limits their exposure and liability.



## Audit Challenges

Today's organizations face a range of audit challenges regarding database security, access, and compliance, including the following:

### Security of Audit Data

- separation of duty
- tamper-proof, evident audit data
- data encryption

### Large Volume of Audit Data

- collection from multiple systems
- scalability, reliability, high availability
- intelligent archival process

### Analysis and Reports

- compliance reports
- efficient correlation mechanisms
- monitoring for insider threats

## **PROTECT:** Multi-factor Authorization

For greater security, organizations should couple the concept of a realm with the capabilities of multi-factor authorization. Multi-factor authorization enables a series of additional security checks prior to giving access to a database, application, or application table. For example, you can tell the security system to check user, session, or system attributes such as IP address and time of day before giving access to the database, application, or a specific realm. Such a system can be very flexible and a good way to specify conditions under which access is allowed.

For example, enterprises might want control over the conditions under which users access the database. You might want to restrict some of the most powerful administrative commands only to specific users that are logged in directly at the server, effectively blocking any request that is coming in from a non-local address, such as from a home. Organizations might also have many requirements about when and where even their authorized users can perform operations. For example, you may not want anyone to touch the system during the last week of the quarter, or you may not want people to do maintenance during work hours.

Thus, based upon your internal operational policies or compliance requirements, you can

specify rich access control policies on top of your existing applications with realm rules, command rules, and multi-factor authorization.

## **PROTECT:** Transparent Encryption

Organizations concerned about access by highly privileged individuals are probably also concerned about data loss. One of the key solutions to minimize the security risk of managing critical data is to consider data encryption, whether the data is at rest, in flight, or in cold storage.

Most organizations are willing to consider encrypting data to provide higher levels of protection and security, but they certainly don't want to reengineer all of their production applications in order to encrypt their data—it would be too costly and time consuming. And, they don't want to perform "key management" or the management of the keys that enable encryption/decryption of the sensitive data. The challenge is in providing encryption without the associated application modifications, and the key management burden and oversight.

An alternative to the traditional approach of "encryption using encryption application programming interfaces (APIs) at the applications level is transparent data encryption that allows organizations to indicate particular columns in database >>

Deploying applications and adding or removing users seems like a simple problem, until you consider the volume of users, applications, and changes that most organizations must deal with.



tables that they want to encrypt, such as a column that stores social security numbers, credit card numbers, or pricing. The rest of the encryption requirements—from the encryption itself to the key management—can all be handled transparently by the database, so the applications accessing that information don't have to be modified or altered. The only change is that the actual data, residing in the database, is now encrypted. Thus, if the database is lost or stolen, the encrypted data would still be safe—it couldn't be seen by anybody unless they had access to the encryption keys used for encrypting the data.

The same issues also arise with the backup media, whether using disks or tapes. If the keys must be managed separately, the chances of them getting lost are very high.

The network traffic similarly needs to be transparently encrypted either by using secure sockets layer (SSL) or other similar protocols. Earlier network encryption was not essential, as the database systems were well protected by firewalls, and within their intranets. But with new compliance requirements, it's essential to also ensure that nobody within the organization, and within the intranet can "sniff the wire" and view the sensitive data going across it.

### **DETECT:** **Who's Doing What, Where, and When?**

Over the past few years, auditing has taken on new importance and urgency as organizations scramble to meet auditors requests to verify all types of business processes and events, access controls, separations of duty, and more.

However, at an IT level, auditing can be tricky. First, it typically creates a large amount of data, which is good for capturing what happened and when, but such a large amount of data can make it

difficult to find what you're looking for. Second, trying to look at audit records of individual systems and trying to analyze them is both difficult and time-consuming. In addition to the problems of volume and collection, other key challenges from a compliance perspective include keeping the audit data secure (so it can't be tampered with), available for long periods of time (so that auditors can reference it), and searchable (so that users can actually find what they need).

One approach to cutting down the volume of audit data is through database systems that support fine-grained audit control so that administrators can specify the exact conditions under which the access is audited. For example, managers could specify that they want to log everything that the DBAs do during off-hours or on the weekends, or log every order with a dollar value beyond some specific number, say \$1,000.

Essentially you're specifying the conditions on when to create the audit data.

To support collection of audit data from enterprise systems, one can use an audit vault, or a centralized repository of audit information drawn from multiple database systems, operating systems, application servers, and applications. Once the data is collected, users can run specified compliance reports. The data in the audit vault can be protected by database vault technology so that nobody can tamper with the audit data—something that's especially important to auditors. As the audit vault stores audit information separately, and in a protected form, away from the originating systems, an administrator or other user is unable to cover his or her tracks because the audit vault would hold the trail of what actually happened.

An audit vault can significantly help in meeting compliance requirements and lessening the risk of internal threats by consolidating all the data together, finding the links between the events, creating reports that span multiple systems, securing the audit data from tampering, and finally, keeping the data outside the purview of the systems that are getting audited.



## DEPLOY: Managing Applications and Users Effectively

---

Deploying applications and adding or removing users seems like a rather simple problem, until you start considering the volume of users, applications, and changes that most organizations must deal with. For example, deploying a new application isn't just about deploying the application but it's also about managing the users who will have access to that application, including defining their authorization rights.

In the past, the entire allocation and assignment of users and privileges would happen on a system-by-system basis, frequently by individual administrators. Unfortunately, doing this entire task in a very distributed and ad hoc manner can introduce many critical holes. There have been some enterprises where it has taken up to two years to remove a user's credentials after the person has left the organization. Timely removal of credentials can be a big issue to auditors and the lack of it can expose an organization to much higher risk than it would experience if a user could simply be removed once from a centralized system and have that eliminate all access and privileges throughout the enterprise.

By centralizing all these activities through the use of an identity management system, organizations can gain strong security and compliance with policies by managing both the addition and the removal of users and their roles. While not necessarily needed for one or two individual applications, identity management provisioning and access control solutions can help make application and user management not only more secure and auditable, but it also eliminates ad hoc workflows. They can also provide single sign on capabilities so that users can sign on to hundreds of applications fast and easily.

## Knowing Where to Start

With so many options to consider when determining how to increase the security of your data and your compliance capabilities, it seems overwhelming. But it really isn't.

One of the places that many organizations are starting to reevaluate their database security and risks is by learning what the compliance officers have identified as the systems, areas, practices, or policies of highest risk, and then working to protect them first, using the types of methods and technologies detailed above.

In general, many organizations evaluate their financial systems first, because they may have some of the most sensitive information, followed by customer data (because of any breach of customer data can create a huge brand risk), and then employee and internal data. But each organization should evaluate its databases and assign appropriate levels of risk to each. Enterprises can start by initially protecting their individual databases—their key assets. Identity management systems can then be deployed to manage users and their permissions throughout the company centrally from one location.

The second step to take is to evaluate your data and organization against the risk of internal threats. This is particularly important since some studies show that up to 80 percent of industrial espionage and risk of data loss comes from internal threats and privileged users.

Regardless of where your organization is, or where it starts, extending your data protection capabilities through technologies such as data vault and transparent data encryption, and centralizing and extending your auditing capabilities through technologies, such as audit vault, will pay off immediate dividends by protecting your organization against compliance failure, and will mitigate risks from internal threats. |s|

About the Author: **Vipin Samar** is vice president of database security for Oracle Corporation.