Preventing Information Leaks at Source with Guardium

We are pleased to introduce a robust solution for safeguarding the application and database infrastructure, including activity monitoring, auditing, change control and leak prevention.

Guardium's real-time monitoring technology uses both policy-based controls and anomaly detection to prevent unauthorized activities by potential hackers, privileged insiders and end-users of enterprise applications such as Oracle EBS, PeopleSoft, and SAP.

Auditing and Compliance

Some organizations believe that reviewing their logs from time to time will be sufficient to pass their audit. But auditors are interested in three things that can't be fully addressed by traditional logging solutions. They want to know that you're actually protecting your data; they want you to monitor all database access and prove compliance; and they want to see that you've implemented a formal oversight process.

Change Control

Most organizations have formal change control policies and processes that govern how and when changes are made to production databases. Until now, however, your IT team may not have had effective tools for detecting when critical changes are made outside of your change control policies and processes.

Vulnerability Management

A core responsibility of the IT security organization is to protect the business from internal and external threats. But the threat environment is constantly changing – and enterprise application and database environments are particularly challenging to secure because their functionality and complexity are constantly increasing.

Database Leak Prevention

Most information leaks, even those that occur via stolen laptops or emailing sensitive information, originate with unauthorized or unusual queries to critical databases. Many organizations have formal access policies that govern how and when sensitive data is accessed, but lack practical solutions for detecting or blocking activities that fall outside these policies.

We believe that this is an important addition to an organisation's security defences, and we would be most happy to discuss database and application security with you. ◄

Two-Factor Authentication with RSA SecurID

IDsec now offers the world's most popular and secure enterprise authenticator solution.

IT managers are coming under a lot of pressure to provide two-factor authentication, driven by compliance and other regulatory moves in both the private and public sectors.

The first factor – "something you know" – is the familiar system password, but setting up the second – "something you have" – takes real effort.

Although this is nominally a security issue, the current economic climate means that there are genuine business concerns. An implementation needs to have a small footprint, avoid major user disruption, minimise cost and keep a tight rein on support overheads.

Proven Technology

RSA's SecurID tokens are very well established in the market, with millions of

TWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK

users and a 20-year development history.

Part of their success is the simplicity of the underlying approach: every 60 seconds the token produces a new, unpredictable numeric code that can be checked by the login process against an authentication server. This provides strong network security, and RSA's implementation has proved reliable and convenient for users.

User Convenience

In fact, recent product developments have provided a wide range of form factors so that IT managers can roll out the type of authenticator that is most suited to their users.

In addition to the original credit card sized unit, there are now SecurID key fobs, USB sticks and software tokens for smart phones such as Blackberry, Windows Mobile and Symbian devices.

IDsec can help you set up strong authentication using SecurID with the minimum of disruption, and integrate it with other security systems, including RSA's security event manager, enVision. ◄

Using RedSeal SRM to Analyse Network Risk

RedSeal's Security Risk Manager is an automated approach to understanding complex networks and their security risks.

Both network managers and security consultants need to map the corporate network, understand any vulnerabilities, determine how they can be exploited and what needs to be done to mitigate risk. More importantly, they need to be able to do this at regular intervals, without taking up precious staff time.

This means that effective network risk analysis can only be carried out with a large degree of automation, and this is where SRM comes in.

It uses both active probing, supplied device configuration data and vulnerability test results to provide a detailed topology overlaid with a graphical risk assessment.

SRM works with a wide range of infrastructure components, including firewalls and routers from Cisco, Check Point and Juniper.

Call us for further details: we can provide a simple demonstration that will illustrate the savings that can be made with this exciting new product. ◄

About Us

IDsec is an independent company specialising in network security. We have provided an expert service to all industry sectors since 1997.

Proventia	*Network Protection*	**Dragon**	*Intrusion Detection*
enVision	*Event Management*	**FortiGate**	*Firewalls*
Tripwire	*Change Auditing*	**Superwalk**	*Gateway Monitor*
V-Line	*Test Access Points*	**AppGate**	*Remote Access*
AppDetective	*Database Security*	**SRM**	*Network Auditing*
SecurID	*Authentication*	**PhoneSweep**	*Modem Scanner*
Guardium	*Database Protection*	**VMware**	*Virtualization*
EMC	*Enterprise Storage*		

IDsec

IDsec Limited
31-33 College Road
Harrow
Middlesex HA1 1EJ

Tel: +44 (0) 20 8861 2001
Fax: +44 (0) 20 8861 3433
WWW: http://www.idsec.co.uk

Copyright © 2009 IDsec Limited. All rights reserved. All prices correct at time of going to press

TWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK SECURITY NETWORK