



INQUISITIVE SYSTEMS

Preventing Insider Threats to Computer Systems

Version 1.0, March 2011

guard INQ[™]
www.inquisitivesystems.com
**Real time
information security**

guardINQ – Preventing Insider Threats to Computer Systems

The Problem

•48% of all computer system breaches were perpetrated by an Insider within the organisation;

•Only 1% of these breaches were detected by a network detection technology,

•Only 3% by security log analysis,

•the majority were discovered by an external party.

•It took an average of 3 months to detect and stop these breaches.

•Within that time frame, the Insider had uncontrolled access to data including employee or customer records, and/or sensitive commercial documents.

•Traditional approaches to security control methodologies force companies into reactive processes, almost always too late and punitive in nature.

•Until now existing vendors and solutions have not properly addressed the Insider Threat landscape.

The Cost Effective Solution

guardINQ provides a completely new perspective on tracking activity.

•Our patent-pending software solution enables the implementation of proactive processes and policies for controlling Insider threats in an enterprise.

•Breaches caused by Insiders usually have prior incidents which **guardINQ** monitors and reports in real time while the incident is occurring and so a breach can be prevented.

•There is little or no learning curve to adopt **guardINQ** and little technical expertise is required to use it.

•The alerts provided by **guardINQ** are a high level abstraction that needs no specialist know-how and can be used by senior management without having to rely of IT administration staff (who may well be involved in an incident).

A high proportion of data breaches are caused by employees. Only a very small fraction of these activities are detected by vendor solutions, typically reactive in nature. **guardINQ** fills a gap left by other vendors. By providing real time monitoring and alerting of detailed user behaviour and activities, **guardINQ** enables a proactive approach so allowing organisations to rapidly investigate and resolve potential data breaches.

The following technical overview;

•highlights the issue of the Insider threat to computer systems

•provides an understanding of who perpetrates these activities,

•the manner in which they conduct them, and,

•the manner in which they can be stopped by **guardINQ**.

Understanding the Insider Threat

The Insider Threat can be broadly divided into the following categories; Super-User IT sabotage, and users with unprivileged access (Unprivileged-Users). In the next few sections, these categories will be outlined by describing the type of individual who may perform this activity, their motivation for doing so, and the manner in which they perform the sabotage or access to data. Finally, we outline the features of guardINQ that can be used to detect and therefore prevent these types of attack.

IT Sabotage (Super-User)

Who

This type of insider is usually highly technical with administrator or similar privileges, in effect a Super-User. Senior management responsible for implementing security control processes usually rely on these individuals. This reliance results in the risk of having gaps left in the efficacy of the security model.

Consequently Super-Users (especially administrators) should be continuously monitored and audited using techniques not derived from traditional log monitoring and management systems. Traditional forms of log and audit file are currently used to monitor these individuals and relied upon to provide some form of situational awareness of their activities. This, however, may not be effective because they have full access to manipulating these security controls.

Super-User (administrators) need to be continuously monitored and audited

Why

Common factors contributing to the Super-User performing malicious activities include:

- The individual is disgruntled, disloyal or compromised in some way. Sabotage in such cases may be associated with previous factors such as conflicts with supervisor or co-worker, a decline in performance or absenteeism
- Even though the initial motivation might not be financial gain, it often can turn out to be the case.

Traditional Detection

These attacks are detected

- Mostly manually by observing system compromise, failure or irregularities²
- With only 25% by customer (after observing instability or system failure)²

25% detected by customer (after observing instability or system failure)²

How

The majority of these incidents used the following approaches:

- 48% involved privilege misuse¹
- 43% of incidents compromised an account using technical techniques²
- 16% of incidents used accounts they created previously²
- 11% used accounts used for testing and training left behind²
- Common technical techniques used were scripts, programs, logic bombs and creating backdoors²

48% involved privilege misuse¹

Effect

In the majority of cases insider attacks have a business impact, for instance disruption in business continuity.

- Leak of strategic information.
- Negative Media Attention.
- In over a quarter of cases individuals are harmed mostly through the false implication of management, supervisor or co-worker in the incident².

In majority of cases insider attacks have a business impact, for instance disruption in business continuity.

Information Theft (Unprivileged User)

Who

Normally this is for financial gain and/or business advantage. In order for this type of breach to be successful, the Insider has authorised access to the valuable data. Detection is mainly by customers and/or non-IT co-workers.

- 71% held highly technical positions and authorised access ².
- 29% were sales staff and had authorised access ².
- 75% were current employees ².
- 95% resigned right before or after theft².
- 70% took place within 3 weeks of resignation².
- 25% gave information to other companies or foreign governments ².

Why

•Financial gain. This can be further compounded by the personal situation of an individual employee. For example, an employee may be facing financial difficulties which in turn may lead them to be easily coerced into committing a criminal activity like stealing data for financial gain.

•Business advantage. The employee may have coerced or placed in the firm by a competitor.

How

The activities are not recorded in logs as the activities are usually very fine-grained. A fine grained activity is one which involves an interaction with the data such as copying it to a certain location, or accessing the data in a certain manner. Only 12% were remote access attacks. The majority was onsite and therefore could have been stopped if the appropriate technology had been installed ².

The Unprivileged-User;

- Had authorised access to information.
- Could circumvent traditional technologies due to the simplicity of copying and pasting data to a channel that allows extraction of data (email, USB, CD Drive).
- Did not require super user access to commit breach.

Effect

- Significant Financial Losses.
- Security, Business and Strategy Plans leaked to competitors.
- Technology and/or Intellectual Property leaked to competitors.
- Identify theft.
- Negative Media Attention.

In 28% of the cases individuals are harmed through mostly false implications of management, supervisor or co-worker²

Traditional Detection

- 26% detected by customers or external informants².
- 50% detected by Non-IT staff supervisor and co-workers ².
- Only 3% detection by security log analysis ¹.

26% detected by customers or external informants²

Why guard INQ?

- **guardINQ** takes a fundamental approach to security controls by recording digital fingerprints at a low level in the operating system which cannot be manipulated or hidden by a Super-User, or Unprivileged-User. This means that, unlike our competitors, we can provide a record of the fine grained activities undertaken by a Super-User, or Unprivileged User.

- We take a bottom-up approach to tracking activity, whereas our competitors take the traditional top-down approach. We provide the data in a manner that can be understood by senior management without relying on Super-Users.

- **guardINQ** monitors activities that occur at an endpoint (Server or Desktop) in a continuous and real time fashion.

- It runs at a very low level within the operating system such that any attempt at compromising the OS by high-tech individuals will be detected. The effect of this is that it is operating system and application agnostic and focuses entirely on activity. This means that we do not need to write a separate script for each new application or process that needs to be monitored.

- It defends against technical attacks like anonymous user accounts and scripts. The effect of running a program or script will be recorded in real time, and an alert can be generated. For example, a program written to create a backdoor will be observed and an alarm raised detailing the activity, the user, the process, the object, and the machine.

- Activities cannot be disguised or concealed by hiding or modifying log files. 86% of victims show evidence of the breach by highly technical staff in their log files. However, existing log analysis tools are incapable of alerting these activities as they utilise log files that do not provide the required level of detail.

- All the recordings are organised according to machines and users so a high risk individual could be monitored by simply ticking a box. Filtered alerts will be generated to a management dashboard (see **guardINQ** system overview) or through other forms of notifications, allowing management to focus on immediate problems or

86% of victims have evidence of the breach in their log files by highly technical staff.

risks.

- **guardINQ** provides simplified incident response through granular and continuous recording of PC activities through a fine level of detail in the Operating System.

File based data breaches are expected to be more prevalent than data breaches. **guardINQ** provides a simple, elegant, application agnostic and real time file access recording for these kinds of attacks.

- In 2011 file based data breaches are expected to be more prevalent than data breaches. **guardINQ** provides a simple, elegant, application agnostic and real time file access recording for these kinds of breaches.

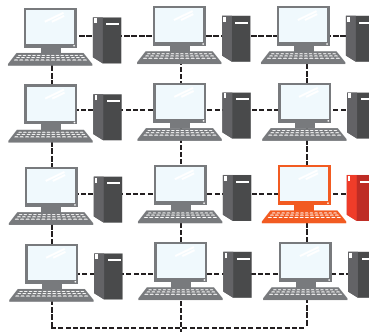


guard INQ™

The Solution

- Proactively detects and prevents insider attacks on servers and desktops.
- Provides real time monitoring and alerting of all activities.
- Monitors IT administrators.
- Is fully automated – No manual offline analysis required.
- Is audit and incident response ready.
- Has Advanced Reporting.
- Integrates easily into Identity Management (IDM) and Security information Event Management Solutions.
- Provides Tick box, user based, reporting.

1.



1. A lightweight agent securely streams continuous sequences of activity from the PC or Server under protection.

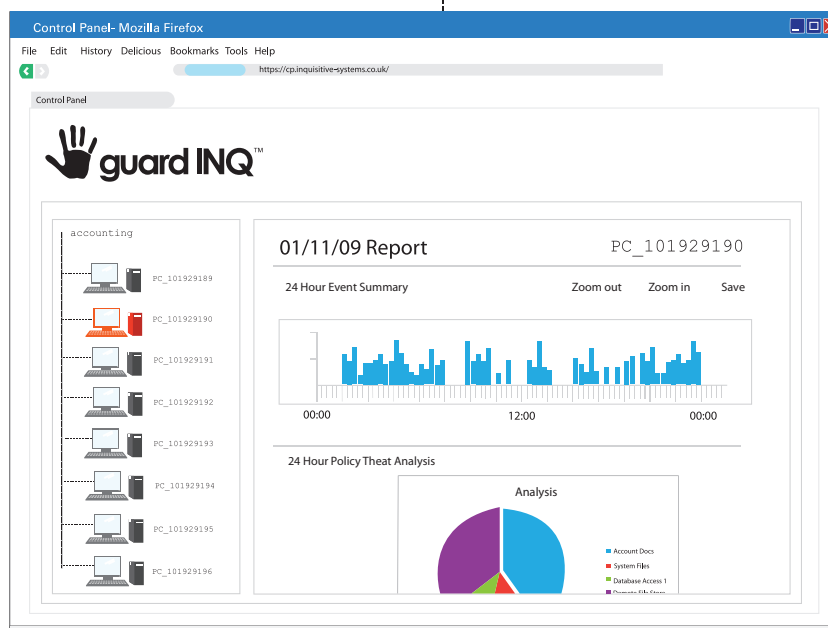
2. All activity is analysed by a centralised analysis component that utilises our advanced, patent-pending, sysDNA™ activity fingerprinting technology. These components are highly scalable, and can be offered as a service or in-house and can deal with the big data generated by an organisation. Easily integrates with existing IDM and SIEM components.

2.



3. Alerting, reporting and management is achieved through a web-based GUI. Events can be sent to existing reporting engines.

3.



Conclusion

A large proportion of data breaches are caused by employees. Only a very small fraction of these activities are detected by today's vendor solutions, and these are usually reactive in nature. guardINQ fills a gap left by other vendors in this solution space. By providing real time monitoring and alerting of fine-grained user behaviour and activities, guardINQ enables a proactive posture which in turn allows organisations to rapidly investigate and resolve potential data breaches.

References

1 Verizon report - 2010 Data Breach Investigations Report. (http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf)

2 CERT report - Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1. (http://www.cert.org/insider_threat/)

Version 1.0, March 2011

INQUISITIVE SYSTEMS

www.inquisitive-systems.com