# iMaxSOFT Corporation

## VerticoData - Enterprise Security Solution

# White Paper

Business Partner hp invent

ORACLE PARTNER

## An Absolute Secure Technology

**iMaxSOFT Corporation**
**October 4, 2015**

**www.imaxsoft.com**
**Telephone: 1-408-253-8808**
**P. O. Box 1222, Cupertino CA 95015 USA**

# VerticoDATA

iMaxSOFT

VerticoDATA Technology White Paper

An Absolute Secure Enterprise Security Solution

An Absolute Secure Enterprise Security Solution

## Security Market Research

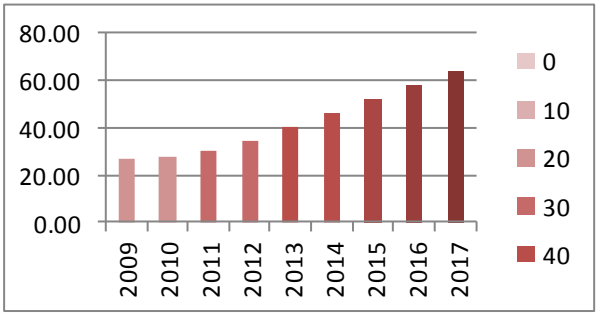
**GARTNER** - Security investments are going to dramatically increase. An already large security market is about to get much bigger, growing by 56% from current levels in five years time. Gartner analysts said a key reason for this is regulatory compliance. IT leaders need to anticipate and plan for the coming wave of government interventions and regulations. As information technology becomes pervasive in all operations, regulations from the analog world will come to the digital world.

There is an urgent need for companies to separate personal and business operations on consumer smartphones and tablets (both company- and user-owned) in ways that will be inexpensive to implement, easy to use, and robust in defense of company policies and data. Several technologies will provide partial solutions to support efforts to manage diverse consumer devices with various advantages to the user and IT manager, but no solution will simultaneously please both. It is too easy for a user to purchase a smartphone with a personal credit card, then use it to access sensitive data via a corporate network.

The only way IT staff can maintain control is by separating mobile computing devices (notebook PCs, PDAs, phones, pagers and others) into three distinct device classes: (1) trusted standard devices provided by the company; (2) tolerated devices, a portfolio of user-purchased devices; (3) unsupported devices that are used in small numbers or have a consumer orientation, for which the PC group cannot provide support. By 2016, 60% of large enterprises will implement limited access network zones to limit the connectivity of personally owned mobile devices.

**COMPUTERWORLD** - Security remains number one priority among CIOs per our 2015 IT spending survey. High-profile security breaches at Home Depot, Target, Michaels and myriad other companies — along with the explosion of mobile technologies — have propelled security spending to the top of the IT priority list for 2015. Nearly half (46%) of the IT leaders who responded to our poll said that they will invest more next year in access control, intrusion prevention, identity management, and virus and malware protection. "Whenever there are these high-profile incidents, it does tend to drive IT security spending even more quickly than it already was," says Stephen Minton, an analyst with the IDC Global Technology and Industry Research Organization. Security spending has been a constant growth area for the past decade — rising at double-digit rates every year, he adds.

**CYBERSECURITY - Spending Trend In USA Only ($billions).** In 2015, the IT spending is $52.2 billions, and by 2017, it will reach $63.5 billions.




iMaxSOFT Corporation

Tel: (408) 253-8808
Fax: (408) 253-4008
E-mail: lee@imaxsoft.com
www.imaxsoft.com
P. O. Box 1222 Cupertino, CA 95015 USA

An Absolute Secure Enterprise Security Solution

## VerticoDATA Security Solution

In today's fast pace industries where technology is rapidly advancing, security takes the highest priority among corporations due to vast amounts of data stored electronically. Lots of measures have been taken to safeguard and block un-authorized access to private data banks. As that technology advanced, there seemed to have been something that was over-looked. What we have been lacking is a universal and secure way of preventing potential security breaches from the corporate **back-office applications**.

There is an ever growing necessity in modern day business to log and prevent security violations from **authorized personnel**. Policies and regulations such as the newly implemented HIPAA compliance regulation for US healthcare industry are becoming an increasing and more pervasive burden upon organizations in all industries. The pressures from both the government and consumers are forcing businesses today to find ways to safely protect sensitive data from not only outside intruders but inside trespassers as well while not hindering their existing IT infrastructure.

IMAXSOFT has recognized this as a crucial part in completing a comprehensive security solution. Our goal is to be able to provide secure and efficient logs for your private and confidential data while remaining transparent to the data sources and applications themselves. Due to the scope of legacy applications running on proprietary systems, a solution that can be easily integrated into existing legacy environments also becomes critical to our technology. IMAXSOFT's solution sits on top of our proven, patent pending technology that has been deployed by top Fortune 1000 companies occupying a variety of industries around the world. This powerful engine is designed for performance and offers a secured and high-performance logging facility and dispatching system.

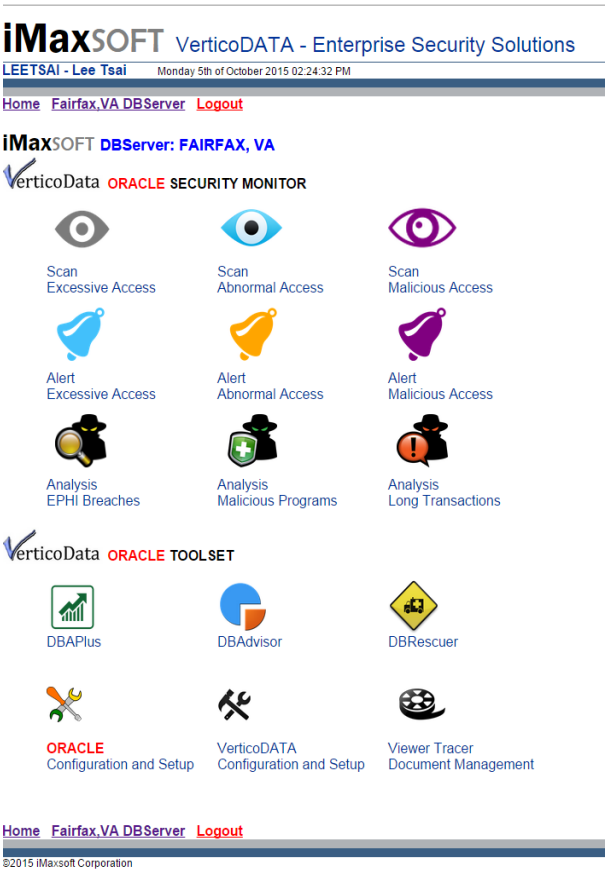
IMAXSOFT also offers an industry specific role based transaction monitoring solution that allows you to make detailed analysis of all **read**, write, and update transactions. Read transaction monitoring is rarely built into vendor applications due to design complexities and performance considerations. IMAXSOFT technology suffers from none of the performance issues experienced by other implementations. Not only will this system record and safeguard any illegal or abnormal access to your sensitive data, it enables extensive capabilities to analyze your day-to-day operations based on who is accessing your data at what time.

iMaxSOFT Corporation

Tel: (408) 253-8808
Fax: (408) 253-4008
E-mail: lee@imaxsoft.com
www.imaxsoft.com
P. O. Box 1222 Cupertino, CA 95015 USA

An Absolute Secure Enterprise Security Solution

## VerticoDATA Main Features




**Enterprise sensitive privacy data's ultimate protection** - VerticoDATA is the last line of safeguard that secures the source and the origin of sensitive privacy data bank.

**Privately labeled and cloud based** - VerticoDATA can be privately labeled and customized as an integral part of the enterprise comprehensive security solution. VerticoDATA can also be enterprises' security forensic experts, auditors and operators thru IMAXSOFT's cloud data center, which is a VerticoDATA security hosting services center, and enterprises' security staff can access their security auditing information worldwide 24 hours a day from web and mobile.

**Concurrently monitoring entire enterprise's computing environment** - VerticoDATA manages all enterprises' ORACLE applications and databases from a central control console, any potential security breaches and threats will be immediately alarmed and alerts will be delivered to designated security officials promptly.

**VerticoDATA Enterprise Security Solutions** - is the main security control panel of an application server or a database server. The panel layout is generic, and it can be easily customized and integrated into the central enterprise operation console.

VerticoDATA offerings include a pre-built UI (user interface) as a general purpose model for enterprise's IT to adopt easily, and a set of building blocks which are used to established a proprietary security solution that meets each enterprise's specific business needs.

This document explores VerticoDATA technology by walking through "**VerticoDATA Main Security Panel"** module by module along with live cases in order to present precise processes for threats prevention and investigation.

Our goal is not to completely stop data leaks and cybercrimes, we believe to capture threats in early stage and to quarantine stolen data promptly is the best way to mitigate our security risks.

iMaxSOFT Corporation

Tel: (408) 253-8808
Fax: (408) 253-4008
E-mail: lee@imaxsoft.com
www.imaxsoft.com
P. O. Box 1222 Cupertino, CA 95015 USA

An Absolute Secure Enterprise Security Solution

## VerticoDATA - Threats Scan

**Sensitive and privacy data definitions** - define and figure out what the sensitive and privacy data are, where sensitive and privacy data are stored, how sensitive and privacy data are retrieved and managed, and who can access those sensitive and privacy data at what security level.

Does access of the last four digits of credit card **alone** constitute a violation of security? Simple question, but it is very difficult to answer. A hacker first fetches last 4 digits of credit cards along with internal member ID, then fetches names along with internal member ID, then fetches expiration date of credit cards along with member ID, and then on and on, pretty quickly the hack can establish a database that mimics a complete member credit card authorization database. So how to define a sensitive and privacy data rule is not just specify an column/item name, a table name, a program name, and so on, access volume constrain, access time constrain, access behavior pattern constrain, access process certificate (**DNA**), and accessor authentication level are equally important.

**ORACLE database transaction interceptor** - effectively and efficiently capturing sensitive and privacy data that are read and written from and to ORACLE database in addition to ORACLE logminer feature is crucial to the enterprise's entire security. When a threat is identified, we must know what has been stolen and how much in order to access and report the **scope of the damage**.

**Linux, HPUX and other flavor UNIX executable programs and scripts** - how to detect malicious programs, procedures, or subroutines that are accessing sensitive and privacy data from ORACLE databases. Do we really know what are the access objects are valid and what are not? Do we register each every access object on our application and database servers? How do we catch a malicious access object from our servers, do we call it virus?

A virus is not too worrisome, we lose a server, a backup server can take it over immediately and is almost unnoticeable (HA), but an implant and an embedded procedure that is routinely exporting sensitive and privacy data in accordance with enterprise security rules is the most dangerous killer. **VerticoDATA program DNA technology** is architected for eliminating them completely.

**VerticoDATA logging, threats pre-scanning, and potential threats staging** - VerticoDATA core engine capture sensitive and privacy data activities from application and database servers, log them to a secure vault permanently, then VerticoDATA threats scanner scans any potential violations against a pre-set of rules, and then collects any suspicious activities to a staging vault for further investigation from enterprise's security staff.

**VerticoDATA threats prioritization and management** - VerticoDATA breaks suspicious threats into 3 categories, excessive access, abnormal access and malicious access. Excessive access is that the access volume of sensitive and privacy data exceeds a pre-set threshold. Abnormal access is that the access time of sensitive and privacy data is outside accessor's authorized working hours. The malicious access is that the DNA of the access program, procedure and subroutine doesn't exist in secure accessor pool, a hacker's implant?

IT security staff will be alerted and are required immediate examining and evaluating the risk factors of those threats, and then inform security officer accordingly. Snap short can be useful, comprehensive historical view gives more precise forensic information of a threat, **check-in suspicious alerts** for further threat investigation.

iMaxSOFT Corporation

Tel: (408) 253-8808
Fax: (408) 253-4008
E-mail: lee@imaxsoft.com
www.imaxsoft.com
P. O. Box 1222 Cupertino, CA 95015 USA

An Absolute Secure Enterprise Security Solution

## VerticoDATA - Theats Alert

**Pending alerts** - once security operators detect suspicious threats through their preliminary threat analysis, alerts are created and transferred from individual application or database server to the central security vault for further investigation.

Based on the origin of the alerts, we group them into 3 categories, excessive access of sensitive and privacy data, abnormal access of sensitive and privacy data, and malicious access of sensitive and privacy data.

**Excessive access** - excessive access is not how many rows fetched from ORACLE database, it is how many rows that are physically delivered to the end user. For the purpose of high performance and high throughput, ORACLE is architected with features like in-memory caching, pre-fetching, parallel query, and many more. The pre-fetching and memory caching are commonly used for database query, hence data fetched out of database are not all delivered to the end user. Therefore, to precisely identify **'what has been seen or stolen**' is lot more trickier. VerticoDATA excessive access alert is triggered by the threshold of '**the number of rows delivered to the end-user**', not by **'the number of rows fetched from the ORACLE database**'.

**Abnormal access** - in general, abnormal access is referred to the validity of the access time, for example, an access was occurred outside an employee's normal working hours. In reality, abnormal access covers far more scenarios than just access time, for example, with today's technology it is quite easy to obtain accessor's source IP and device ID, therefore, a mismatched access point of an individual is also treated as an abnormal access.

Since abnormal access is not only bound to sensitive and privacy data, so all **abnormal behaviors** should be recorded, alerted and examined by security staff. Abnormal behaviors like access time violation, accessor authentication violation, and execution of unknown program and script, they are all precursors of potential serious attacks. We should immediately collect auditing information and create a complete access map which includes source access point (IP and device ID), access path, servers, databases, tables, columns, queries and its execution flow, subroutines and its calling flow, query statements and actual data of *sensitive and privacy data accessed and altered*, query statements of **non** *sensitive and privacy data accessed and altered*, and the accessor's profile (is he/she still an active employee?). With this forensic access map we should be able to identify the severity of the breach and the possible consequence of the threat.

VerticoDATA collects and builds valuable forensic access maps for potential threats. VerticoDATA intelligent threat analyzer performs data-mining on the VerticoDATA security vault to prevent **gradual and methodical** data leaks and breaches.

**Malicious access** - according to our experiences, it is hard '**to clearly identify a threat**', and then **'to assess the damage**', and finally **'to block the threat and repair the damage**'. Invisible and unnoticeable threats are the most dangerous ones, we don't know their existence till it is too late. Most of data leaks were caught in average of12 to 24 months later, why? 12 to 24 months is a long time, the threat likes a silent cancer that grows exponentially inside our data bank, and we don't see it. Why? They act **normally** per our standard security measurements and rules, they may borrow a valid accessor's authentication and gradually and methodically transfer data out, after a long period of time, they can easily create a replica of our entire precious data bank.

VerticoDATA threat intelligent analyzer and tools are the answer for an absolute secure data bank.

iMaxSOFT Corporation

Tel: (408) 253-8808
Fax: (408) 253-4008
E-mail: lee@imaxsoft.com
www.imaxsoft.com
P. O. Box 1222 Cupertino, CA 95015 USA

An Absolute Secure Enterprise Security Solution

## VerticoDATA - Threat Intelligent Analyzer

**Security vault** - this precious data bank stores comprehensive and complete auditing information in order to catch threats and to protect our sensitive and privacy databases. It needs to be constantly mined and analyzed for potential threats and is where security forensic exports are replied on for investigation of those most sophistic and technologically advanced threats.

The rule of thumb of choosing a security solution is 'can it catch threats **in-time** for minimum or no damages to our sensitive and privacy data'. In order to maintain an up-to-date and efficient VerticoDATA security vault, it is highly recommended that we constantly mine and analyze our security vault for exploring the characteristics of threats in order to prevent new threats and mutated old threats.

**Electronic Protected Health Information (EPHI)** - is mainly used in healthcare industry and is the synonym of protected sensitive and privacy data. **VerticoDATA security solution crosses industries and supports internationalization**. VerticoDATA kernel is NLS ready, and the front-end UI is UTF8 NLS driven and can be toggled from language to language by design.

**VerticoDATA threat intelligent analyzer** - '**full log** of all database transactions and data' is unrealistic and is proven to be operational impossible. VerticoDATA kernel can be trained to differentiate online versus batch processes, and is able to self-tuned security rules' criteria and thresholds in order to capture meaningful auditing information **efficiently**.

For example, a weekly batch process accesses 5 databases and 113 tables, calls 64 subroutines and takes about 6 hours to run. VerticoDATA learns and records the process's statistics for a few weeks and establishes a reasonable and reliable rule for this weekly batch process. Thereafter, when this process is not started on Friday night, when this process takes 10% more time than its average runtime, when this process invokes un-known or un-registered subroutines, when this process accesses un-authorized databases and tables, when this process's DNA doesn't match the one registered in the rule database, upon its security level setting, VerticoDATA may block the process, or issue an alert and block pending on resume authorization, or simply logs as a warning event for further security investigation.

**VerticoDATA rule engine** - static rule based engine is no longer capable to handle today's highly technology driven data hacking techniques. The self-learned and self-trained technology is the core of VerticoDATA dynamic rule based engine. VerticoDATA rule engine adjusts and re-aligns rules according to the changes of the security environment, the requirements of business needs, and the advances of IT technologies.

The smarter the rule engine is, the more valuable the auditing information is. The quality of auditing information drives the efficiency of threats catching. **Catching threats before damages occurred** is our only focus and is the core design base of VerticoDATA security solution.

VerticoDATA rule engine knows what to log and audit, when to act and block, and how to prevent and protect. There is no way to stop cybercrimes, and there is no solution that can 100% protect us from data leaks. Security becomes a challenge of 24X7X365, cyber hackers and thieves don't have downtime, we can be hit at any second, and unfortunately **sometimes one hit may cost our entire business**.

iMaxSOFT Corporation

Tel: (408) 253-8808
Fax: (408) 253-4008
E-mail: lee@imaxsoft.com
www.imaxsoft.com
P. O. Box 1222 Cupertino, CA 95015 USA

An Absolute Secure Enterprise Security Solution

## VerticoDATA - ORACLE Toolset

**ORACLE toolset** - VerticoDATA **toolset building block** is crucial for enterprises to create proprietary and unified tools for their end-users, constituents, associates, and partners to transfer *sensitive and privacy data* in a secure and auditable domain.

It is also our responsibility to provide security measurements for our business constituents, associates, and partners to protect *sensitive and privacy data* distributed from us. Simple, secure, auditable and enterprise specific database piping tool is a must for our users to move sensitive and privacy data across the internet.

**VerticoDATA DBAPlus** - is a replica of ORACLE sqlplus utility tool from the functionalities perspective. The generic version of DBAPlus is focused on quick data query, data download, query performance evaluation, and database objects management. This tool and its building blocks enable enterprises to create their own dynamic query and data exporting end-user tool, it is not only a web and mobile ready and ease of use, but also has built-in row count and query runtime constraints, so users will never be able to create a crazy query that runs forever and drains all ORACLE database resources.

VerticoDATA security solution does consume extra ORACLE database resources and its does affect applications' performance and overall system throughputs. DBAPlus, a performance measurement and tuning tool is created to assure a healthy and well-performed database environment at all time.

**VerticoDATA DBAdvisor** - OTACLE tablespace and partition management has direct impact to the overall throughput and performance of the databases. DBAdvisor makes the task so easy and is particularly handy for very large data warehouse space and performance management, i.e. VerticoDATA security vault.

**VerticoDATA DBRescuer** - a real-time ORACLE transaction recovery tool. We need this robust toll when a database is sabotaged by hackers. In today's non-stop computing environment, this is a must for us to maintain and to protect the integrity of our databases in real-time mode. DBRescuer supports REDO and UNDO for all ORACLE DML updates, and its building block can be used to create an enterprise specific **time machine for bulk repairs and rollbacks.**

**VerticoDATA viewer tracer** - VerticoDATA document management system is a prototype for demonstrating 'how to manage and establish traceability for text, audio and video multi-media documents' on the net. The powerful building block can be applied to document and raw data, and our traceability engine can be easily integrated into enterprise's auditing platform.

iMaxSOFT Corporation

Tel: (408) 253-8808
Fax: (408) 253-4008
E-mail: lee@imaxsoft.com
www.imaxsoft.com
P. O. Box 1222 Cupertino, CA 95015 USA

An Absolute Secure Enterprise Security Solution

## VerticoDATA - Conclusion


**Facts** - we cannot completely prevent threats and data leaks. There is no bullet-proof security solution. Enterprise IT security infrastructure covers hundreds of thousands of devices and people, any access point can be the weakest link, once a link breaks, the entire enterprise will become a vulnerable target for hackers. It is impossible to 100% stop data leaks, what can we do to mitigate our risks?

**What can we do** - we must first identify what's our the most sensitive and privacy information, where are they stored, and how do they get created and accessed. Next, we need to layout an access road map of our *sensitive and privacy data* and see whether we can create an isolated and secure domain to streamline the management of *sensitive and privacy data*. At last, an access authorization map is required in order to create a enterprise wide comprehensive security authentication rule base.

For the sake of efficiency, an in-house IT security team is required, and we must understand that conducting a thorough inventory of enterprise's *sensitive and privacy data* is very time consuming. But, in order to protect, we must first know what to protect.

**VerticoDATA deployment** - VerticoDATA can be deployed as it, and makes enterprise specific customization concurrently. The sooner we deploy VerticoDATA, the quicker VerticoDATA learns and strengths the quality of enterprise's security rule base.

Security breaches will never go away and it is a forever war. We must learn how to live with it comfortably. When an cyber attack occurs or a data leak incident occurs, as long as we learn it soon enough to reduce our risk to minimum, we win.

We should not act like that our customers' *sensitive and privacy data* is 100% protected and our security system is bullet-proof and data never leaks. When data leaks occurred, we shouldn't downplay the seriousness of those leaks, lie about the impacts to our customers, and misleads our customers with meaningless recovery solution. A successful business ranks the security of customers' *sensitive and privacy data* as the highest priority, and is dead serious about pretesting the invaluable customers' trust and business goodwill.

In today's digital world, the *sensitive and privacy data protection effort* is vital for the survival of a business. Public can be very quickly to loss faith of a business that is not properly protecting their sensitive and privacy data, and a business can be totally destroyed, if a business is not telling their customers and the public the real impacts caused by a data leak promptly and honestly. **Promptly and precisely detection of what has been stolen and leaked is a fundamental requirement of any security solution.** We should never challenge the intelligence of the public.

iMaxSOFT VerticoDATA Development Team
October 2015, Saratoga California USA


iMaxSOFT Corporation

Tel: (408) 253-8808
Fax: (408) 253-4008
E-mail: lee@imaxsoft.com
www.imaxsoft.com
P. O. Box 1222 Cupertino, CA 95015 USA