

BUSINESS VALUE AND RISK REDUCTION USING patchVantage

 *Oracle Enterprise Customer
Perspective*

Abstract

Taking risks can be an expensive business; in an increasingly complex regulatory environment, driven in part by evolving cyber - security threats, how can organizations remain compliant, current and secure? ... One answer is automation; software tools exist that can dramatically reduce the administrative burden facing IT departments, in particular those responsible for Database and ERP Application Support - this White Paper presents typical scenarios faced by such organizations and analyses the impacts of failure to avoid risk ...

RISK EXPOSURE

Risk Score

286

Across all
RDBMS

Estimate Cost Exposure (USD)

\$ 18,638,159

Total across all
RDBMS

27











Pending

162

Oracle RDBMS

83%

Compliant

OS	Oracle Asset	Package name	Security	Date	Patch Needed
	RDBMS 12.2	jan_CPU_2018_rdbms_121		03.28.2018	1
	RDBMS 12.1	jan_CPU_2018_rdbms_122		04.10.2018	2
	RDBMS 12.0	oct_CPU_2017_ebs_121		04.11.2018	12
	EBS 12.1	jan_CPU_2018_ebs_122		03.29.2018	12
	EBS 12.2	jul_CPU_2017_rdbms_121		04.15.2018	10

CONTENTS



Executive Summary	1
About patchVantage	2
Introduction	3
Part I – Cost Reduction (ROI)	4
1.1 Overview	4
1.2 Scenario A – US Health Care Insurer	4
1.3 Scenario B – US Technology Manufacturer	5
1.4 Financial Analysis ROI	6
Part II – Risk Reduction (ROSI)	7
1.5 Overview	7
1.6 How Risk Reduction is Achieved using patchVantage	7
1.7 Risk Model	11
1.8 Impact Risks and Costs – US Health Insurer Scenario A	13
1.9 Calculating ROSI	15
1.10 Financial Analysis ROSI US Health Insurer (* with GDPR) ..	16
Conclusions	17

Executive Summary

Today, more than ever, Oracle customers face a growing number of regulations and an exponential growth in cyber-attacks. The impact of a cyber breach has a long tail cost distribution which masks the true financial exposure most organizations have. In order to mitigate risk, they need to manage two dichotomous scenarios: (a) Maintaining the highest level of compliance with a rapidly expanding number of databases, and (b) reducing operating costs and provide better visibility of the Oracle assets. However perhaps the adoption of advanced automation tools can help meet these ostensibly conflicting demands.

The situation is compounded by new regulation such as GDPR will increase pressure on IT departments. In particular activities such as duplication of live production data and security patching - both of which are disruptive, time-consuming processes. Additionally, as enterprises scale up their use of the public cloud, they must rethink how they protect data and applications. The public cloud disrupts security models built over years. They will need to evolve their cybersecurity practices dramatically in order to consume public cloud services in a way that enables them to both protect data and exploit the speed and agility these services provide

The purpose of this study is to provide insight into how patchVantage software can provide autonomous features for Oracle, **on-premise** or cloud. The objective is to clearly quantify using financial data the cost savings **ROI**, and risk reduction value proposition **ROSI**.

In this way you can make better decisions when allocating cybersecurity budgets that compete with other technology investments.

Figure 1 Source Oracle Applications Users Group

Security has been a User's top concern regarding the Cloud



About patchVantage

patchVantage is a software solution for managing both the Oracle Enterprise **and** Standard Edition stack with fast agentless discovery of assets.

It can maintain the highest level of security and compliance SLA's for Oracle RDBMS and E-Business Suite endpoints using precise reporting and large-scale automation.





Specialized components also exist for the rapid cloning of Multi-Terabyte Databases.

Introduction

With more than 350,000 customers worldwide Oracle has been widely recognized as the leading database supplier for almost 40 years. It is mature and stable but also contains many innovative features to support evolving business requirements. It's used in many critical industries such as utilities, government and banking.

However, there are key pain points for many Oracle customers - primarily total cost of ownership (TCO) and security. In this regard, Oracle Databases and Applications have features more in common with a legacy system (see Table 1). This is sometimes referred to as the "Oracle Complexity Tax" or "Operational Debt".

Table 1 Features of a Legacy System

	Time Consuming to introduce new features
	Costly Support – Many Oracle customers on Sustained Support
	Integration with other systems cumbersome or complex
	Business processed typically work around, rather than vice versa

The other significant challenge is cyber security. The idea that attacks are increasingly likely – and perhaps inevitable – is forcing companies to mitigate IT security risks and threats, but there is also the misconception that the impact of a cyber-attack is mostly shaped by what companies report publicly. This is dominated by reporting of personal information theft and incident management. However, the most severe costs are less obvious such as loss of intellectual property, data destruction, downtime of core operations and loss of business.

In fact according to *Deloitte* ([Beneath the Surface of a Cyber Attack](#)) the cost of a breach can cost billions of dollars. They identify 14 *impact factors* that can be used to quantify the real costs. The integration of cyber and valuation principles provides a better insight that should inform an organization about how to plan for cyber incidents. Another report commissioned by *CGI and Oxford Economics* developed a rigorous model to show the long term effect of a breach on the company's share price ([Cyber-Value Connection](#))

The first objective of this study is to illustrate how the cost and complexity for the Oracle Customer can be significantly reduced using the Oracle Patch Accelerator product. The second takeaway is to demonstrate that even **small amounts of risk reduction** can significantly reduce financial exposure. We then explain how the product can reduce risk in 3 key areas: **Operational Velocity, Limit Data Controllers and Precise Unified Compliance Reporting.**

55% of attacks are SQL Injection (SQLi)



Figure 2 Source Alert Logic

Part I – Cost Reduction (ROI)

1.1 Overview

Two scenarios are presented which represent typical Oracle customers which run mission-critical applications and have to balance cost, availability and security. Frantic development cycles and the accelerated rate of business innovation require that data and insights be available at a moment's notice. In today's climate rolling out new products and services is critical to staying ahead of the competition. To do this, organizations need to rely on their applications and IT services. Behind the scenes are the administrators managing it all.

Enterprises who implement management and monitoring tools tend to be more engaged with the complex issues around security, governance and compliance. Keeping environments up-to-date is not a simple task. Organizations not using *patchVantage* found at a minimum they required and average of 100%, or double the effort, to manage their ongoing database administration workload.

The scenarios also depict organizations which have bigger footprints, both in terms of the sheer numbers as well as capacity. These organizations run in excess of 4 four different set configurations of patches databases/applications in production, test and development.

1.2 Scenario A – US Health Care Insurer

Sample organization is a US Health Care Insurer with a turnover of 6Bn USD. They have 300 Databases with 8 DBA's and need to cope with increased compliance patching. They have a major focus on compliance due to a previous cyber breach which affected 10M members. The Company is expanding at 20% per annum but there is a reduction in the response to new business requirements. There are major discrepancies in system patching, rising costs and an inability to meet service level agreements.

Table 2 Key Scenario Parameters US Health Insurer

Data	Values
Deployment	On-Premise and Public Cloud
Company Size	6Bn
Infrastructure Growth	10%
Database Instances	300
Number of DBA's	8
Members	10M
Cyber Insurance	\$3.75M for \$150M Cover
Issues	Compliance
Versions	10g,11g,12c on Linux and AIX
patchVantage Solutions	RDBMS Accelerator

1.3 Scenario B – US Technology Manufacturer

Sample organization is a US Technology manufacturer with a turnover of 40Bn. They have 2000 Databases and 40 DBA's with a plan to hire another 9 DBA's to cope with the increase in compliance patching. They are expanding at 10% a year. The manufacturing processes rely heavily on the ERP system which requires minimal downtime. In addition, significant amounts of intellectual property are contained within Oracle. The system maintains a global inventory which interfaces to all their suppliers; any operational disruption would have severe cost impacts. The company has also introduced the *Agile* methodology and require continuous cloning from the 5TB production data to facilitate rapid test cycles. This is consuming a lot of DBA time.

Table 3 Key Scenario Parameters US Technology Manufacturer

Data	Values
Deployment	On-Premise
Company Size	40Bn
Infrastructure Growth	20%
Database Instances	2000
Number of DBA's	49 (New Hires 9)
Members	N/A
Cyber Insurance	N/A
Issues	Compliance and Agility
Versions	EBS 12.1,12.2,11g,12c on Linux and Solaris
patchVantage Solutions	RDBMS and EBS Accelerator, Snap Clone

1.4 Financial Analysis ROI

The analysis reveals the capabilities of the product to automate existing tasks and perform work that could not be done before. The ROI increases in line with growth because of price breaks. In addition, there is an assumption that 50% of growth can be consumed without additional manual effort which increases the productivity. The cost of the DBA is estimated at \$115,000(salary.com).

The data shows a very favorable ROI of between **112%** and **171%** can be obtained.

Table 4 Scenario A - US Health Care Insurer with high growth in membership and data requirements

Projected Benefit	Year 1	Year 2	Year 3	Year 4	Year 5	Totals
# of Databases	300	330	363	399	439	
□ to DBA Ratio	100	105	110	116	122	
Price Per Unit	1,025	1000	975	950	925	
License OPEX	307,500	330,000	353,925	389,318	428,429	1,808,992
Product Benefit	575,000	650,571	734,561	827,850	931,413	3,713,395
Net Savings	267,500	320,571	380,636	473,925	577,488	2,020,120
ROI	87%	97%	108%	122%	135%	112%

Table 5 Scenario B - US Technology Manufacturer with intellectual property and operational dependencies

Projected Benefit	Year 1	Year 2	Year 3	Year 4	Year 5	Totals
# of Databases	2,200	2,640	3168	3802	4562	
□ to DBA Ratio	100	110	121	133	146	
Price Per Unit	650	625	600	575	550	
License OPEX	1,430,00	1,650,000	1,900,800	2,280,960	2,737,152	9,998,912
Product Benefit	3,105,000	4,002,000	5,103,491	6,452,652	8,101,505	26,764,648
Net Savings	1,675,000	2,352,000	3,202,691	4,551,852	6,200,705	17,982,248
ROI	117%	143%	168	200	227	171%



On average DBA's manage around 25 Databases each

Figure 3 Source Unisphere Research

Part II – Risk Reduction (ROSI)

1.5 Overview

Patching is also a risk management exercise. Estimates vary but it's recognized that around 80% of attacks use vulnerabilities for which patches already exist. The statistics also show the majority of attacks use the most common exploits. This section attempts to quantify what level of risk reduction – using the product - will be delivered using the software as a security investment.

We also quantify how the three components **Operational Velocity**, **Data Controller Limits** and **Compliance Reporting** actually reduce risk. These components can only be achieved through automation.

Garrett Bekker, a cybersecurity analyst at 451 Research, says managing cyber risks from third-party vendors is becoming a “huge problem” for big firms. Some large enterprises are demanding that supplier's cyber risk can be quantified. This has led to another way of measuring cyber-risk called **FICO® Enterprise Security Score**. Since patching frequency is a component of this metric then automated patching will elevate the score.

1.6 How Risk Reduction is Achieved using Automation Software



Operational Velocity is all about reducing the timeframe for the patch window and closing the vulnerability gap by reducing the patch cycle time. Also, by reducing downtime and having intelligent scheduling it's much easier to patch updates. This applies to all instances – any unpatched database is a vulnerability.




Limit Data Controllers applies the **Least Privilege** concept. It reduces the insider threat, manual errors and holds historical information on activity.



Precise Compliance Reporting provides intuitive dashboards and formal compliance reports across the entire Oracle inventory. Reduce the chance of missing a patching and easily see delays and risks.

Table 6 How we Reduce Timeframe and Downtime for Installing Patches


	Discovery Oracle RDBMS(agentless)
 Operational Velocity	Auto Download Patch from Oracle Support
	Upload Patch to Server (and unzip)
	Perform up to 16 OPatch pre-requisite checks rapidly
	Control Database Shutdown and Startup
	Automated OPatch Version Detection and Upgrade
	Post Database Step Automation
	Intelligent Scheduler can be based on Historical Load
	Log file collection and Audit
	SMS/E-Mail Notification
	Large scale deployment using Gold/Master Image

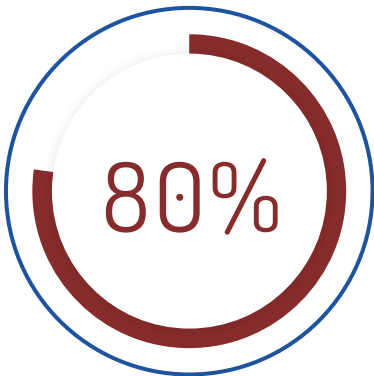


Managing more Databases per DBA will
be a major challenge

Figure 4 Source Unisphere Research

Table 7 Understand methods to reduce necessary access to instances


	Dramatically reduce the number of privileged users. Many fewer DBA's are now required to manage the Oracle stack
 Limit Data Controllers	Reduce Misuse of Privileges
	Audit and replay Controllers activity
	Provide Location Data on Controllers(Cloud)
	ROLE based Access
	Allow Operators to patch without having any password privileges
	Database scanner quickly identifies weak passwords on all Databases
	Reduce manual errors
	Consistent repeatable operations reduce chance of missing a patch



of organizations had at least one threat caused by an insider over the past 12 months

Figure 5 Source AT&T Cybersecurity Insights Insider Threat

Table 8 Enterprise reports which are intuitive for both operations management and auditors

Full Inventory Visibility	
 Precise Compliance Reporting	Precise Information on Oracle Patch Levels
	Full Compliance Reporting
	Dashboard with Compliance Alerts
	Intuitive Graphical Displays of Patch History
	Reports also available using Web Services(JSON)



of organizations haven't updated their security strategy in 3+ years

Figure 6 Source CIO Computerworld

1.7 Risk Model

In order to evaluate the return on a security investment (ROSI) it is first important to calculate the **cost of an incident** – referred to as the Single Loss Expectancy (SLE). Incident costs fall into two categories Direct and Indirect. In this whitepaper we are going to use the model from Deloitte called “[Beneath the surface of a cyber-attack](#)” because they are industry leading audit and consulting firm with a specialization in Cyber Risk Services. The model also allows the reader to adjust the parameters to their own business model and derive a reasonable estimate.

They identify 14 *impact factors* which contribute to the overall SLE. The nomenclature is described below.

01

Technical Investigation

The costs associated with technical investigations are direct expenses for analysis to determine what happened during a cyber incident and who was responsible

02

Customer Breach Notification

Customer breach notification costs include the direct expenses associated with informing and advising individuals whose data has been compromised, as typically mandated by state or federal law or industry regulation.

03

Post Breach Protection

Post-breach customer protection costs are direct costs associated with services to detect and protect against potential efforts to use an individual's compromised personal data for unauthorized purposes (Average Cost 20USD take up 9%)

04

Regulatory Compliance

Regulatory compliance costs are fines or fees levied as a result of non-compliance with federal or state cyber breach related laws and/or regulations. (If Adjusted for GDPR add 4% of Turnover)

05

Attorney Fees & Litigation

Attorney fees and litigation costs can encompass a wide range of legal advisory fees and settlement costs externally imposed and costs associated with legal actions the company may take to defend its interests

06

Cyber Security Improvements

The costs associated with cybersecurity improvements are direct expenses for technical improvements to the infrastructure, security controls, monitoring capabilities, or surrounding processes, specifically to recover business operations after an incident or to prevent a similar occurrence in the future.

07

Public Relations

Public relations costs are the direct costs associated with managing external communications or brand monitoring following an incident.

08

Impact of Operational Disruption and Destruction

Impact of operational disruption or destruction is a highly variable cost category that includes losses tied to manipulation or alteration of normal business operations and costs associated with rebuilding operational

09

Increase Cost to Raise Debt

Insurance premium increases are the additional costs an insured entity might incur to purchase or renew cyber risk insurance policies following a cyber incident.

10

Cyber Insurance Premium Increases

Insurance premium increases are the additional costs an insured entity might incur to purchase or renew cyber risk insurance policies following a cyber incident.

11

Loss of Customer Relationships

During an initial triage period immediately following a breach, it can be hard to track and quantify how many customers are lost. Economists and marketing teams approach this challenge by attaching a “value” to each customer or member to quantify how much the business must invest to acquire that customer or member

12

Value of Lost Contract Revenue

Value of lost contract revenue (or value of premiums, in the case of the health insurer, includes revenue and ultimate income loss, as well as lost future opportunity associated with contracts that are terminated as a result of a cyber incident.

13

Devaluation of Trade Name

Devaluation of trade name is an intangible cost category referring to the loss in value of the names, marks, or symbols an organization uses to distinguish its products and services.

14

Loss of Intellectual Property (IP)

Loss of IP is an intangible cost associated with loss of exclusive control over trade secrets, copyrights, investment plans, and other proprietary and confidential information, which can lead to loss of competitive advantage, loss of revenue, and lasting and potentially irreparable economic damage to the company. Types of IP include, but are not limited to, patents, designs, Copyrights, trademarks, and trade secrets.

1.8 Impact Risks and Costs - US Health Insurer Scenario A

Using the assumptions set out by Deloitte we derive the data below.

Table 9 Summary of impact factors US Health Insurer with 10M member breach

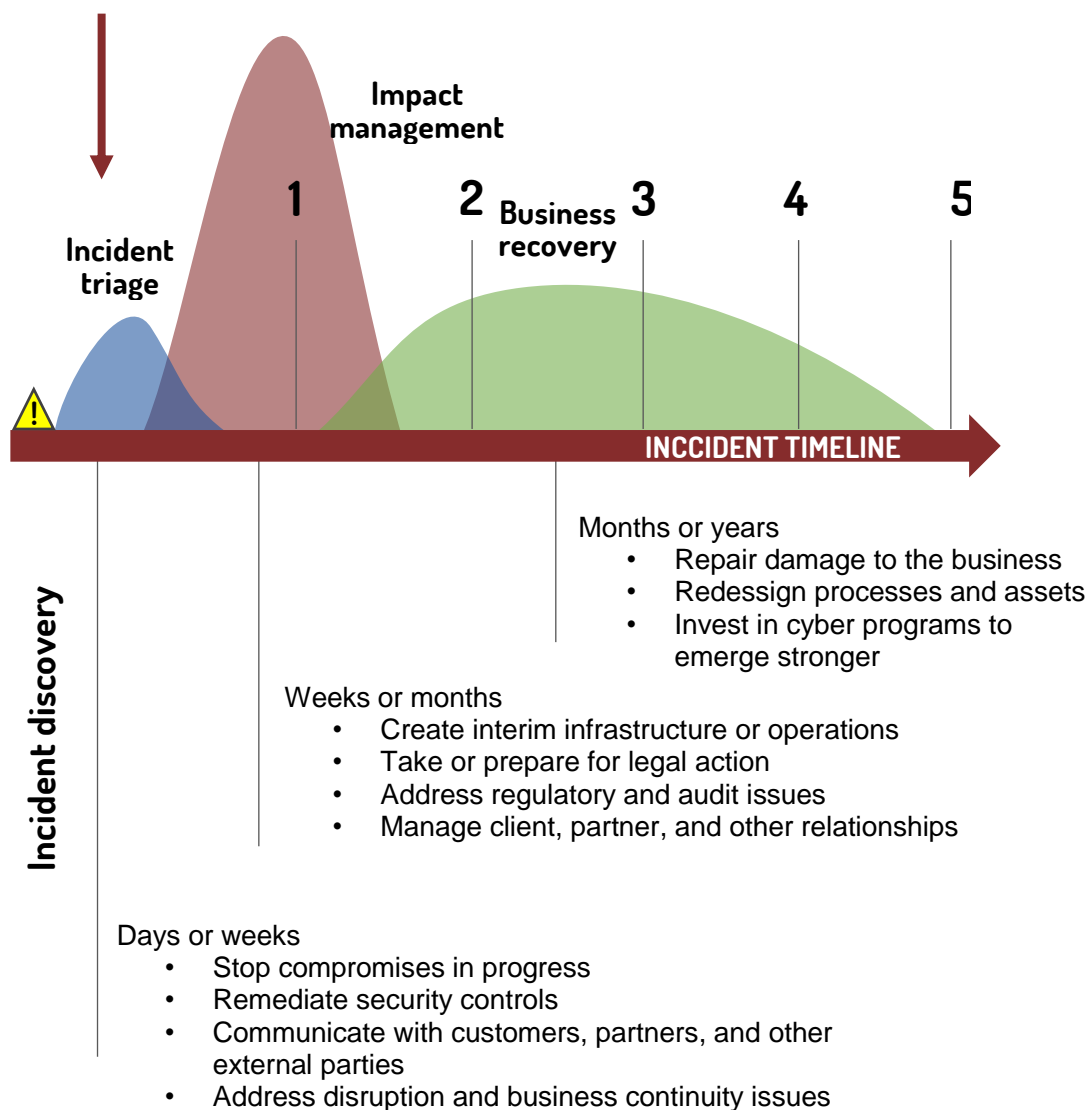
Impact Factor	Term	Cost(millions) USD	%Total Cost
Technical Investigation	1	1	0.13
Customer Breach Notification	6 Months	27.5	3.45
Post Breach Protection	3 Years	54	6.78
Regulatory Compliance	1 Year	2	0.25
Attorney Fees & Litigation	5 Years	20	2.51
Cyber Security Improvements	1 year	5	0.63
Public Relations	1 Year	1	0.13
Operation Disruption and Destruction	Immediate	12	0.13
Increase Cost to Raise Debt	5 years	10	1.26
Cyber Insurance Premium Increases	3 years	40	5.02
Loss of Customer Relationships	3 Years	180	22.60
Value of Lost Contract Revenue	5 years	348	53.69
Devaluation of Trade Name	5 years	96	12.05
Loss of Intellectual Property(IP)			

The total cost over 5 years is 796.5M USD aggregated over a 5-year period below

Year 1	Year 1	Year 2	Year 3	Year 5
\$235m	\$186m	\$186m	\$95m	\$95m

Incident triage
efforts comprise
<10%
of total impact

Recovery stretches over years



1.9 Calculating ROSI

In the previous section the ROI was used to show how your company can save money by automating the lifecycle management and compliance of the Oracle stack versus only a manual approach. However, security is not generally an investment that results in profit, but rather loss prevention. When you invest in data security, you do not anticipate benefits – instead you expect to reduce the risk threatening your Oracle assets.

The terms used below can be used to derive ROSI.

- *Definition of Cyber Risk* – A combination of the probability of an event and its consequence (ISO 27000) and the exception to loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result (RFC 2828)
- *SLE* – Expected Financial Cost if event takes places
- *mitigation ratio* – The percentage of threats deterred by the cybersecurity solution
- *ARO* – Is the annual rate of occurrence. We assume one breach a year at most
- *ALE* – Is the annual monetary loss = ARO * SLE

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

1.10 Financial Analysis ROSI US Health Insurer (* with GDPR)

Using the cost information from **Scenario A** and a discount rate of 3% we calculate the return on the product as a security investment. Since membership for the insurer is likely to growing potential breach costs will be higher so the actual return will be higher.

Modest effectiveness ratios have been applied but still reveal very significant returns.

Table 10 Return on Security Investment Analysis 10M member Cyber Breach Deloitte Model

Incident Category	Year 1	Year 2	Year 3	Year 4	Year 5	Totals[NPV]	Mitigation	ROSI [5 years]
Vulnerability Remediation	\$228m 229m	\$397m 175m 221m	\$555m 170m 170m 215m	\$623m 84m 165m 165m 208m	\$687m 82m 82m 161m 161m 201m	\$2.49Bn	1.5%	2165%
Cost	\$298,544	\$311,057	\$323,892	\$345,904	\$369,567	\$1,648,962		
ARO	1	1	1	1	1	5		
Internal Misuse	\$228m	\$397m	\$555m	\$623m	\$687m	\$2.49Bn	1.25%	1788%
ARO	1	1	1	1	1	5		
Compliance Management	\$228m	\$397m	\$555m	\$623m	\$687m	\$2.49Bn	2%	2920%
ARO	1	1	1	1	1	5		
GDPR	\$233m	\$226m	\$220m	\$213m	\$207m	\$1.1Bn	1.58%	955%
ARO	1	1	1	1	1	5		



55%

of DBA's consider improving security a top challenge

Figure 5 Source Unisphere Research

Conclusions

Endpoint Patch Management vendors in the Windows and Linux space can provide rapid vulnerability remediation through reduced patch cycle times. Given the potentially enormous costs of a cyber breach there are good reasons to invest in this technology. Until now the cost of managing Oracle has been excessive, in particular when viewed through the lens of competing, integrated products for other platforms that have better functionality and value.

Cybersecurity is only as strong as the weakest link, so it is necessary for Oracle customers to maintain compliance at the highest level and at the same time overcome the prohibitive complexity tax that comes with Oracle.

Additionally, as enterprises scale up their use of the public cloud, they must rethink how they protect data and applications. The public cloud disrupts security models built over years. They will need to evolve their cybersecurity practices to consume public cloud services in a way that enables them to both protect data and exploit the speed and agility these services provide. Delays in creating and securing databases will attenuate the public cloud's agility and reduce developer productivity.

The velocity at which attacks transpire is also driving the need for automation and orchestration.

patchVantage will be especially useful to organizations with the following characteristics

- High-risk industry sectors such as Healthcare, Pharmaceuticals, Military and Retail
- Have rapid growth, nonlinear scale, and increasing infrastructure stack complexity
- IT departments with growth in administrator headcount that need productivity gains
- Businesses that rely on technology to generate revenues and want a competitive edge
- Are planning to migrate some Oracle systems to the public cloud
- That require all their security products to be seamlessly integrated with Web Services

The data compromise at Equifax was due to their failure to install in a timely manner the available security updates - but patching can take time, even for large Corporations with dedicated security staff. Cybersecurity has become a team sport that requires trusted service providers and other entities.

Automation is a necessity, not a luxury.