Ovum
TMT intelligence | informa

Software Patching Is Critical for Solid Security and Reduced Risk

Customers lean on trusted providers for bulletproof support

Summary

Ovum view

Customers often go through a rigorous review and due diligence process before investing in enterprise software products—and rightfully so—given the scope and cost involved in most projects. What's surprising, however, is that some customers don't engage in similar due diligence when it comes to properly securing those software investments through ongoing software patching and maintenance.

Ensuring regular software patching and maintenance should be an imperative for every enterprise. Patching provides customers peace of mind that known security vulnerabilities are mitigated, thus maintaining an in-depth defense posture. Regular maintenance allows customers to build a culture of compliance, where they can be confident that they're keeping up with industry regulations and compliance procedures. Failure to perform proper software patching and maintenance means putting a company's bottom line at risk, as well as their reputation as a secure and responsible enterprise. To achieve or maintain this compliance culture, companies should be investing in comprehensive software support and maintenance services from providers who are trusted and who have the necessary expertise and experience with the customer's software and systems.

In our view, customers who avoid patching or necessary maintenance due to short-sightedness or to save expense in the near term are risking long-term damage to their company's security and credibility. Ultimately, that damage could have a devastating impact on their reputation, revenues and bottom line.

Key messages

- Top-to-bottom enterprise security is a top priority.
- Compliance is a way of life and regular software patching plays a vital role.
- Businesses should work closely with their enterprise software vendors to make full use of provided software updates, upgrades, and support tools to proactively maintain security.
- In this paper, we will review:
    - The importance of regular software patching and maintenance.
    - Potential legal and business risks from not following such an approach.
    - How one customer, realizing the need for an appropriate level and type of support, is turning to its trusted software provider (in this case, Oracle) to help address any vulnerability and security issues within its own platform versus a third-party support provider.

Top-to-bottom security is an enterprise priority

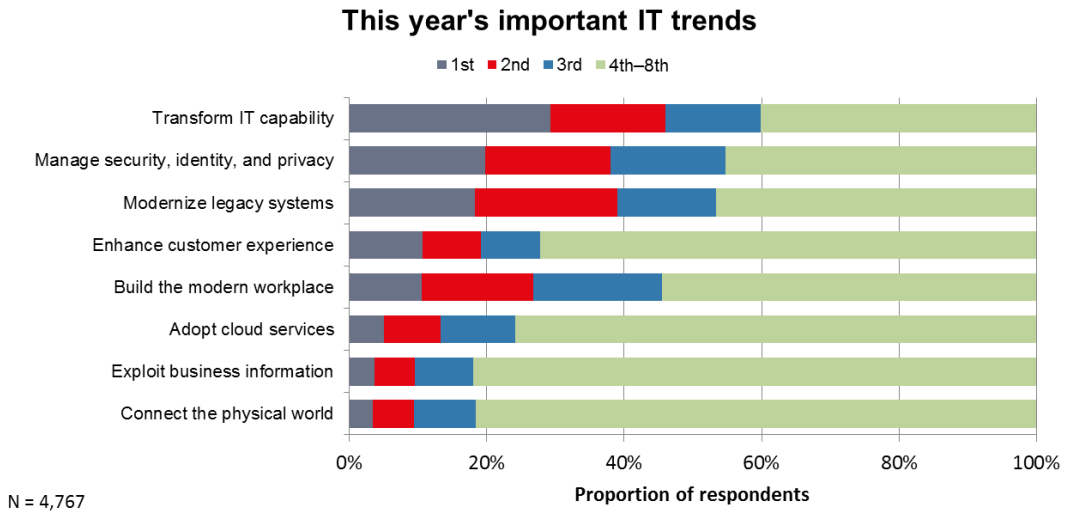
Many enterprise customers are attempting to transform their IT in order to keep up with the accelerated pace of change within their markets and business— leveraging technology trends such as cloud, mobility, and analytics. However, many of those digital transformation initiatives are running head-on into a fiscal reality where many CIOs and IT managers face flat or reduced IT budgets. There is an ongoing balancing act between investing in digital transformation initiatives and taking

advantage of new and enhanced applications and business processes, while still needing to ensure that the current environment is operating reliably with bulletproof security.

It's not just one component or element of IT that must be secured— it's a necessity for the entire stack from operating systems to hardware to databases, middleware, and applications. It only takes one weak link to bring the IT infrastructure to a screeching halt, resulting in downtime that can impact the entire business, and, in extreme circumstances, security breaches that can result in violations of industry regulations and compliance procedures.

In our discussions with customers on their IT environments, security regularly emerges as among the most important considerations. In one of our more recent surveys, the global ICT Enterprise Insights, we asked customers to rate the most important IT trends, as seen in Figure 1. Respondents selected the need to manage security, identity, and privacy second only to the need to transform IT capability. To us, this reflects the balancing act referenced above, where customers want to invest in the new while still protecting what they already have.

Figure 1: Important IT Trends Among Enterprise Customers



Source: Ovum ICT Enterprise Insights 2017

It's not hard to understand why security is an urgent issue among our surveyed enterprises, given what a security incident or breach can mean for an organization's business and reputation. News of security leaks and hacks at multinational corporations are more frequent than ever, with reports of stolen credit card data, personal information, health records, and more. These events typically lead to lost revenue and a sullied reputation for the affected customer; losses in business and customer loyalty are difficult to recover from. Most customers realize the need to protect themselves as much as possible from potential cybersecurity threats, but must also realize that those threats cannot only come from external hackers but from failing to maintain proper internal security throughout the IT stack.

Software patching plays a critical role in compliance

Customers today simply cannot afford to bypass a rigorous software security and maintenance program, especially as external threats are ongoing and becoming increasingly sophisticated—requiring ongoing vigilance and maintenance. To have a rigorous security profile, companies should be working closely with their software vendors, as they have the most experience and expertise when it comes to patching, supporting, and securing their own products.

Companies of all sizes and industries need to partner with a trusted provider to put procedures in place to keep their software security current and to address potential vulnerabilities. Software vulnerabilities can allow hackers or unauthorized personnel to bypass security controls, which can directly result in theft, fraud, and immediate financial loss—not to mention the tarnishing of a company's brand.

Beyond those losses, companies that fail to keep up with software security face potential fines for violating government or industry regulations and compliance procedures. And those consequences are becoming more costly as security incidents increase in frequency and seriousness. In the US, government regulators have taken to levying heavy fines following security and data breaches, costing companies in various industries millions of dollars.

In fact, security breaches and their outcomes have become so frequent that the Federal Trade Commission has issued extensive guidance on how corporations should approach IT security throughout the entire IT stack. To cite one example, the FTC has published "Start with Security: A Guide for Business," a Top 10 compilation of lessons that can be learned from the fines and settlements they've enacted in cases of past violations, as shown in Figure 2.

Figure 2: FTC Recommendations for IT Security

www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

Source: Federal Trade Commission *Start With Security: A Guide for Business*

While some of this guidance is fairly intuitive, some of the lessons deserve closer inspection when viewed through the lens of proper product patching and support. When discussing sound security practices in product development, the FTC references companies that were cited and fined for failure to follow IT product platform guidelines for security. When discussing security procedures to address vulnerabilities, the FTC specifically recommends updating and patching third-party software, heeding any security warnings from vendors and addressing them immediately. Failure to do so could mean that a company will come under scrutiny from regulators and other parties, ultimately earning the company a substantial fine if a serious security issue occurs and the company failed to adhere to compliance policies beforehand.

Given this backdrop, customers increasingly tell us that security and compliance go hand-in-hand as they consider software deployments and that both play an increasingly larger role in overall IT support and maintenance. Most regulations are either transaction-based (for example in financial services and banking) or data management-based (for example, data privacy and record storage in health care), or both.

At Ovum, we regularly recommend that customers, regardless of the vertical industries in which they operate, need to create a strong foundation and culture of compliance as a matter of course for their existing IT and software deployments, especially if they ever hope to make newer digital trends a regular part of their business. Our view is that such a foundation cannot exist without regular software patching and maintenance services, preferably ones that are automated and scalable and that free up time for CIOs and IT managers to concentrate on other initiatives.

To that end, it makes sense for a customer to work with their software vendors—the companies that actually create, update, patch, and support their products on a regular basis—to achieve that goal. For older products, getting there can include an upgrade to a more modern and fully supported version of the vendor's software that is designed to handle today's security threats—not those of 5 to 10 years ago.

Customers that are proactive with patching have peace of mind

Some customers engage in as-needed software patching and maintenance services only when there is a degradation of performance, functionality, or reliability, or a when a headline-grabbing security threat forces them to see what potential security holes need to be plugged. However, given ongoing security and compliance issues, as well as the increased frequency of security breaches and attempted security hacks, many customers have decided they need a more formal approach, with regular software monitoring, patching, and maintenance as core functions of their IT operations.

However, not all third-party support providers are able to offer the same level of software support and maintenance as the software vendor, whether with proactive support or dealing with potential support issues in real-time. In surveying the vendor landscape, vendors ultimately need to demonstrate that they are acting as a partner with customers on their software patching and support needs. Vendors should demonstrate three important characteristics:

- Trusted provider: A trusted and tested provider with knowledge and expertise in securing data and enterprise IT environments, with long-time experience handling enterprise-class security and support.

- Security expertise: A provider with experience in securing the entire IT stack, from infrastructure to databases to applications, with expertise in providing proactive and real-time support resources whenever and however required.

- Comprehensive offerings: A provider with a full, integrated suite of security and support offerings which are constantly evolving and innovating, and who can help a customer establish a culture focused on IT security and compliance.

Customers we speak with say Oracle is working to dedicate a wide array of resources to demonstrate those characteristics in its support offerings across the Oracle stack, as it recognizes the critical part that Oracle systems play in many organizations.

What's more, Oracle support provides levels of capability and security that are far above offerings from third-party, non-Oracle software support vendors. Those third-party vendors cannot provide security fixes, as Oracle points out, because those vendors cannot alter Oracle's source code and they are unfamiliar with the technical details of the vulnerabilities that Oracle fixes. Customers of those third-party support vendors also do not benefit from Oracle's ongoing security assurance efforts, as all previous fixes and patches are already part of each subsequent Oracle software release.

One longtime Oracle customer, a major cable and communications company based in the southern US, has a large deployment of 450 Oracle servers, including six Oracle Exadata systems. Those systems are used to support the company's enterprise data warehouse, supplying a critical backbone for all of the company's internal and external business processes. In fact, the customer was one of the early adopters of Oracle Exadata, and has watched Oracle's support services evolve over time.

Upon the initial Oracle Exadata rollout, software updates in those early days required a time-consuming update of the firmware and the entire platform, as Exadata is an engineered system designed to deliver benefits as an integrated platform. From those experiences, Oracle introduced the Platinum level support for Exadata in 2012. This provides greater visibility into the back-end system and includes proactive elements such as the "phone home" capability that allows Oracle support engineers, working with the customer's support staff, to detect potential issues before they became critical.

The enhanced support level also provides the customer greater capabilities around software patching— the customer typically patches once or twice a year depending on need and criticality. (Platinum support provides for four patch cycles per Oracle Exadata full rack.) The customer can coordinate any patching with Oracle support engineers to ensure proper change management within the systems and limit any disruption to the company, its employees, and its own customers.

The customer says that a regular patching schedule, and a strong emphasis on IT security company-wide, provides assurances that their systems are less vulnerable and more secure. As Exadata is powering some of this customer's most essential systems, downtime would have a direct impact on internal IT's ability to deliver on its SLAs to internal and external customers (even with robust storage, disaster recovery, and redundancies in place). Working with Oracle's Platinum-level support also allows the customer to offload some of the internal support to Oracle support engineers, freeing up its own IT staff to concentrate on other projects and initiatives. The customer anticipates additional innovation in Oracle's patching and support procedures with even more automated functionality. Oracle continues to work with the customer through regular meetings and other methods to ensure the customer's patching and support are properly addressed.

Conclusions

With security and compliance dominating the IT agenda, the need to ensure a strong overall security profile—one that encompasses a customer's entire IT stack—is greater than ever. Regular security support, maintenance, and control are essential not only to protect a customer's current IT investments, but to ensure the security of the business in the long term. This strong security profile is even more important as customers consider and undertake digital transformation programs that may have fundamental impact on their IT infrastructure, applications, and business processes.

Attending to software security issues in a reactive fashion puts a company's bottom line at risk. Customers tell us they feel a great sense of urgency to properly protect their IT environments, given all of the potential risks and threats. They also want to avoid any chance of violating industry regulations and compliance procedures due to shoddy security or patching procedures.

Although it seems self-evident, we regularly remind customers that vendors who create enterprise software such as Oracle are best suited to maintain and support those products, especially where maintaining strong IT security is a priority. Customers who create custom, home-grown applications that are maintained by internal IT support are one thing, but supporting complex software built to run critical enterprise systems should be left to the experts. We would advise customers avoid any potential risk and turn to providers who are tried and trusted, have strong security expertise, and have a comprehensive portfolio of integrated support offerings.

Author

John Madden, Practice Leader, IT Services

john.madden@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright Notice and Disclaimer

Ovum
TMT intelligence | informa

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo