Avoiding security risks with regular patching and support services

Consistent software patching and maintenance services leads to higher levels of security and compliance -- and peace of mind for customers

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 services – selecting instead to patch on an ad-hoc basis, or only when a security threat arises.

Customers may shy away from addressing regular patching or overdue software upgrades because they have concerns about price, time or complexity. However, based on our conversations with customers, an "only as-needed" approach to software support is short-sighted, and could expose customers to security and compliance risks, not to mention losses in employee productivity and business revenue depending on the software involved.

Before deciding to forgo such software updates and vendor support services, we would advise customers to weigh the negative impacts that an inefficient and incomplete maintenance program can have on clients, employees and the overall business. In our view, customers that avoid patching or necessary upgrades because of short-term issues are ultimately risking long-term damage to their company's security and credibility – both of which in these times are easier to lose than they are to restore.

Key messages

- Running a business starts with secure enterprise IT – and it's not getting any easier
- Compliance is a way of life and software security controls play a vital role
- Successful businesses work closely with their enterprise software vendors to make full use of provided software updates, upgrades, and support tools to maintain security.

RUNNING A BUSINESS STARTS WITH SECURE ENTERPRISE IT

Security risks are higher than ever before

It's no secret that many CIOs and IT managers are being asked to do more with less in terms of their squeezed IT budgets. There remains an ongoing balance between investing in new applications and business processes, with the need to ensure the existing environment is operating securely and reliably.

For some customers, this balancing act is out of kilter – they spend much more time on securing existing environments than they would like, rather than concentrating on innovation or new investments, and are looking for methods and tools that can make their job easier. The need for robust IT security is even more critical when considering the complexity of most IT environments, with products from multiple vendors, and dozens of business processes affecting a variety of audiences (employees, customers, partners and suppliers).

It's not just one component or element of IT that must be secured. The entire stack – from operating systems, to hardware, to databases, middleware and applications – must be bulletproof, because it only takes one weak link to bring IT to a screeching halt.

In our discussions with customers on their IT environments (a few which are outlined later in this paper), security regularly emerges as among the most important considerations -- security for the entire IT stack and especially in software deployments. It's not hard to understand why. News of security leaks and hacks at multinational corporations are appearing more frequently than ever – with reports of stolen credit card data, personal information, health records etc. These events lead to lost revenue or a sullied reputation for the affected customer. And these security threats are not just linked to "traditional" applications or databases; social media channels such as Facebook and Twitter now are fairly regular targets. The bottom line is that many customers realize the need to protect themselves as much as possible from potential threats

Software patching is part of strong security profile

For some customers, the challenges of maintaining software environments that satisfy all security requirements is complex, time consuming, and seemingly never-ending. These tasks are even more difficult when you consider that there are multiple software vendors involved in heterogeneous environments, each of which provide varying levels of support, maintenance and security information, depending on a customer's licensing and support agreements.

However, even with these challenges, customers today simply cannot afford to bypass a rigorous software security and maintenance program. In a recent report, Ovum identified how customers should prepare to handle IT security in 2013, and some of these areas are identified in Figure 1. For software, overall we see a need for customers to avoid a "quick fix" approach, and consider software security in the context of a broad, robust and long-term security profile. External threats are ongoing and becoming increasingly sophisticated, requiring ongoing vigilance and maintenance. As security breaches appear to be more common, with more and more companies identified as victims of attacks in recent months, customers need confidence that their systems are secure – as the negative impact on a customer's business or reputation due to data loss or corrupted systems could be immeasurable.

Figure 1: Security Trends to Watch in 2013

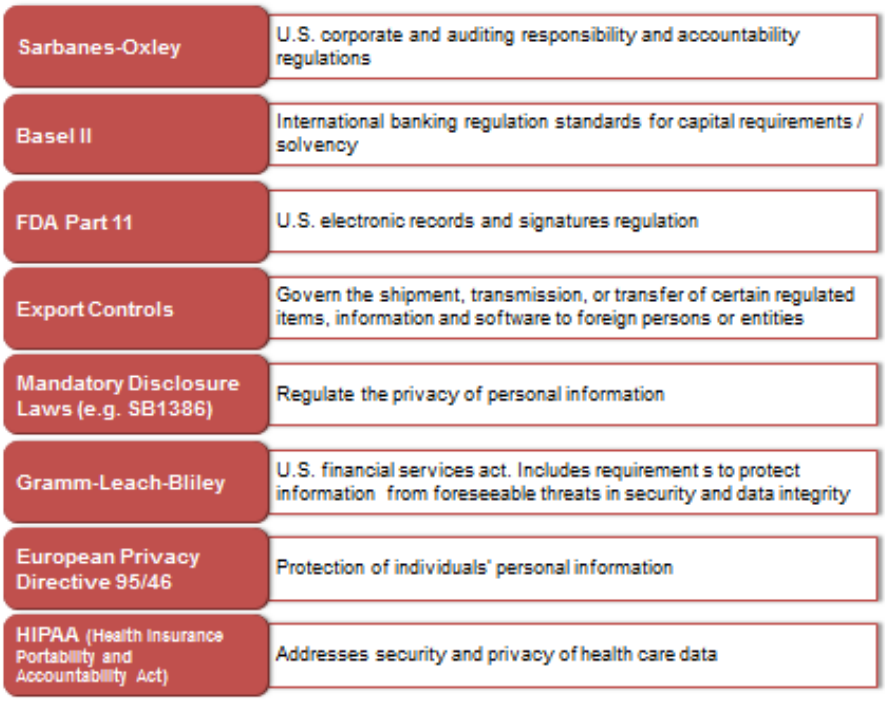
Source: Ovum 2013 Trends to Watch: Security

COMPLIANCE IS A WAY OF LIFE

Customers dealing with vertical industry demands

Customers regularly 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 governance. As seen in Figure 2, customers need to juggle a myriad of regulations and compliance issues, depending on the structure of their company and/or the vertical industries in which they operate.

Figure 2: Examples in the Regulatory Landscape



Source: Ovum

Most regulations are either transaction-based (for example in financial services and banking) or data management-based (for example for data privacy and record storage in health care), or both. Regardless of the regulation, complying with these rules cannot be achieved without strong security for software deployments. In many organizations, maintaining software that meets compliance standards and certifications maybe the primary responsibility of the CIO or CTO. However, we increasingly see compliance as a collective effort that ultimately involves all types of IT and business leaders, including the CFO and sometimes even the CEO, given the legal, auditing and financial issues involved.

Many of the above regulations have been on the books for some time. These regulations take on additional dimensions as customers think about investing in newer technologies – such as cloud, mobility and analytics. 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, if they ever hope to make these newer 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 which is designed to handle today's security threats – not those of five to 10 years ago.

CUSTOMER EXPERIENCES: BENEFITS OF REGULAR SOFTWARE SUPPORT AND MAINTENANCE

Regular patching schedule is essential to business and compliance

Some customers only engage in software patching and maintenance services "as needed" – 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 that this ad-hoc approach is simply unacceptable for their IT and business operations. Regular software monitoring, patching and maintenance are absolute core function of many IT shops these days.

One of the world's largest online retailers in photography, a customer that uses integrated hardware middleware and database products from a major enterprise vendor, is typical of many customers regarding the importance of regular software patching and maintenance. Simply put, if this retailer's IT systems – which the retailer deploys and manages itself -- are compromised in any way, or experience any unscheduled downtime due to a security breach, the company can definitely lose money and potentially lose customers that will never come back. The latter is especially true if customer data is stolen due to a software security issue.

The company's CTO recently told us that compliance issues, particularly involving transactions and PCI standards, are at the heart are what motivated him and his team to create a regular schedule of software updates and patches that happen virtually every day. Using automated capabilities available in his vendor's enterprise management portfolio, this retailer schedules regular patches and updates at its two redundant data centers.

The IT team will select a specific set of application functions or sub-functions, run the patches and updates at one data center, and then the other. The team views this procedure as something of a test of its overall disaster recovery strategy, swinging upgrades from one center to the other and thereby resulting in no disruption for customers or the business. Timing for the patches and updates depends on the software; some can be performed during regular business hours, some after hours or overnight.

Although compliance was the primary motivator, business value is an underlying influence as well. The company's CTO is keenly aware what it will mean if customers are unable to place orders or if the retailer is unable to process their requests: lost revenues, dissatisfied customers and a bruised reputation, at the very least. He also said there are advantages to patching a multi-layered and

redundant system, especially on those rare occasions when his patching program hits a snag. The CTO pointed to one recent incident where a regularly scheduled patch for database connectivity failed to correct an issue. The customer worked with his vendor's support services team to diagnose the problem and properly deploy the patch without any performance degradation to the retailer's web site – customers never even knew there was an issue.

This retailer's CTO said IT customers should assume that software bugs and fixes are simply business as usual when it comes to large complex software deployments – regardless of who makes the product, how well a product works or how long a customer has used that product. That said, the CTO said attempting to catch those bugs with a reactive ad-hoc program, versus a proactive regular software patching program, would simply be too time-consuming, and put the company at a greater security risk.

Automation and tools can simplify the process

Once a customer has made a decision to initiate a regular software patching and maintenance program, what they want most is automated tools and support from their vendors to make such a program run as seamless as possible.

Another customer, who works in manufacturing and is a leader in a major vendor's largest user community group, said overall she is pleased with how her vendor issues timely security and software patches – not just in terms of the actual patches, but also in the amount of information available through made available through the vendor's global support organization. In addition, we should note that both this manufacturing customer, as well the CTO at the online retailer, specifically mentioned that automation tools are essential in order to effectively select, schedule, document and track software fixes and patches.

Like the online retailer, the manufacturing customer, who has longtime experience as a database administrator and other IT roles, advocated the use of a regular patching program among customers – at the very least on a quarterly basis. With a regular patching schedule, all patches and fixes can be deployed and documented in the same manner and on similar timeframes. A customer has the added benefit of aligning their software patching to a vendor's regular patch release cycle, keeping an up-to-date record of a customer's configuration data.

In fact, this approach also encourages a customer to stay on a fully supported version of a vendor's software products, where new patches are still available; if a customer falls behind they also can decide to upgrade and then engage in regular patching, so that their software has the most up-to-date features available. Not all vendors provide a high level of proactive software support or the patching processes, according to the customer, so it makes sense to take advantage of the services whenever possible.

Customers that may be struggling to justify the additional cost of a regular software patching and updating program, versus patching only as needed or when a security risk arises, can do so in several dimensions, according to the customer. The ROI for investing in regular software support services becomes clear when customer consider what the program can deliver in the long-term:

overall enhanced security, improved IT governance, the protection of intellectual property and sensitive company data, regulatory compliance, and ultimately business growth and benefits.

In addition, customers that take advantage of regular support services can divert time that would have been spent on operations and maintenance to other tasks that can contribute to a company's bottom line. As the manufacturing customer said, "We have better things to do with our time."

CONCLUSIONS

Software security is an investment for long-term protection

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.

Attending to software security issues in a reactive fashion is putting a company's bottom line at risk. Based on our conversations with customers, there are simply too many potential security threats to ignore a proactive software patching program. The first step is to make sure that a customer is using the latest software versions in their IT environments. In some instances, customers are using older product versions that are no longer supported or patched, so an upgrade is the most effective way to make sure their patching program, and their overall security profile, is optimal. As many enterprise software customers can attest, upgrades can be time consuming and costly. However, the potential dangers of using out-of-date software – products that are potentially full of security holes that need to be plugged – make the upgrade costs worthwhile. The cost seems especially justified as the increased use of newer technologies like cloud and mobility will undoubtedly bring new security threats.

Although it seems self-evident, we also regularly remind customers that vendors that create enterprise software are best suited to maintain and support those products, especially where maintaining strong IT security is a priority. Customers that create custom, home-grown applications that are maintained by internal IT support is one thing, but supporting complex software built to run critical enterprise systems should be left to the experts. Customers that have vendor-licensed software should avoid modifying those products on the fly and/or applying home-grown fixes; doing so might violate their license agreements and put them at risk of being denying vendor support.

In the last few years, vendors have made major investments in their support tools and services, with an emphasis on automated and proactive capabilities, making it easier for customers to remediate any security issues. The customers we spoke with said that if customers make the necessary investment in software support services, they have a high level of control in just how they handle an overall software security program, compared to past software patching procedures.

What’s more, these investments align with ITIL practices, reinforcing many best practices that are already in use across a wide variety of customers.

Even with this greater level of control, customers say in complex heterogeneous environments they cannot achieve the software security profile that they need with their own resources, or they do not have the internal expertise to know which systems need additional protection or monitoring. Customers tell us that working together with vendors and relying on their expertise in proactive support ensures that they don’t miss any critical software patches or fixes. And since software support services vary depending on the vendor involved, these customers advocated taking advantage of regular software support services when vendors make them available. Failing to make these investments is like leaving your best baseball player on the bench during the World Series.

APPENDIX

Author

John Madden, Principal Analyst, Ovum IT Services team

author@ovum.com

Disclaimer