Publication date:
January 2023
Author:
Alan Rodger

Sustainable Software Patching: Critical for Solid Security, Reduced Risk, and Meeting Compliance Challenges

Customers, battling with growing complexity and threat levels, need bulletproof support

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Oracle

Contents

Summary

In brief

Increasing investments across many industry sectors in transformational digitalization mean that software is more critical than ever to organizations’ fortunes and business reputations. At the same time, factors such as greater complexity around new technology opportunities (including more prevalent digital supply chains), the burgeoning threat landscape, and the competitive environment (which drives more frequent software updates from vendors seeking to introduce new features) accelerate the pace of software adoption and change cycles within user organizations. The resulting software estate is commonly characterized by a significantly larger attack surface. For example, Omdia forecasts indicate that over 25% of the servers shipped in 2024 will be located by organizations at the edge (an environment that did not exist to require protection only a few years prior). Also, malicious actors are increasingly focused on uncovering exploitable vulnerabilities in commonly found open-source components in the hope of achieving a “discover once, hack many” effect.

While numerous security solutions can be marshaled to reduce the likelihood of malicious exploitation, the timely application of vendor software patches is the indispensable foundation for avoiding the risk arising from unmitigated security vulnerabilities. Risk management and compliance are brought ever closer to software protection practices by the drive toward digitalization, and threats that remain unaddressed because of unpatched vulnerabilities constitute real business issues.

Omdia believes that many organizations need greater maturity and understanding of the value of proactive management in the patching workload and lifecycle. An essential step is a commitment to establish a security-patching window within priority scheduled maintenance and a means of understanding the relative risk that drives the selection of patches to be prioritized. Because patching is an increasingly crucial capability, this need for maturity should be reflected in the context of the organization's IT governance framework, which must include only sourcing patching content from the valid original supplier.

Omdia view

A process of rigorous review and due diligence is seen as justifiable and worthwhile before investing in enterprise software products, and rightly so, given the scope and cost involved in most projects. It is therefore a serious let-down that some organizations do not engage in similar care when it comes to properly securing these software investments by committing to the ongoing software patching and maintenance that is necessary to maintain software’s integrity. The approach to IT governance in any organization must guard very strongly against any tendency to "buy and forget" with respect to any element of the software estate, which can open up holes in enterprise protection and foster risk and compliance problems that lead to serious business issues.

Ensuring regular software patching and maintenance must be an imperative for every enterprise, enforced rigorously through management commitment to the importance of maintenance plans and to the maturity needed within the organizational culture to ensure regular and successful patching. Regular security maintenance allows customers to build a culture of compliance, where they can be confident of keeping up with industry regulations and compliance procedures. Failure to perform proper software patching and maintenance means putting a company's bottom line and its reputation as a secure and responsible enterprise at risk. But in addition to reinforcing these key business reasons for a commitment to patching, organizational culture must overcome any fears that patching could potentially be responsible for causing failures. On the contrary, the truth is that failure to keep patching up to date constitutes a far greater risk.

Of course, like any other IT management discipline, patching must be subject to strong control. A key element of a successful patching regime is adherence to the use of high integrity sources of patching information, not putting faith in poor-quality sources such as ubiquitous web-based advice. Another weakness to be avoided is any engagement of third-party service providers without the assurance that their processes and skills incorporate all necessary rigor in using only creditable sources of patching content, and have mechanisms to ensure the integrity of the patching content and their distribution. The consequences of poor governance of such relationships are likely to include increased cost to the client organization, as well as risk and compliance issues. Furthermore, organizations should not rely on unproven mitigative controls or unverified configuration changes to do away with patching.

Key messages

- Sustaining software security over its usage lifecycle is a key responsibility.
- Patching is a cornerstone of IT governance and its support of compliance responsibilities.
- Risk is avoided only if patches are acquired from reliable sources.

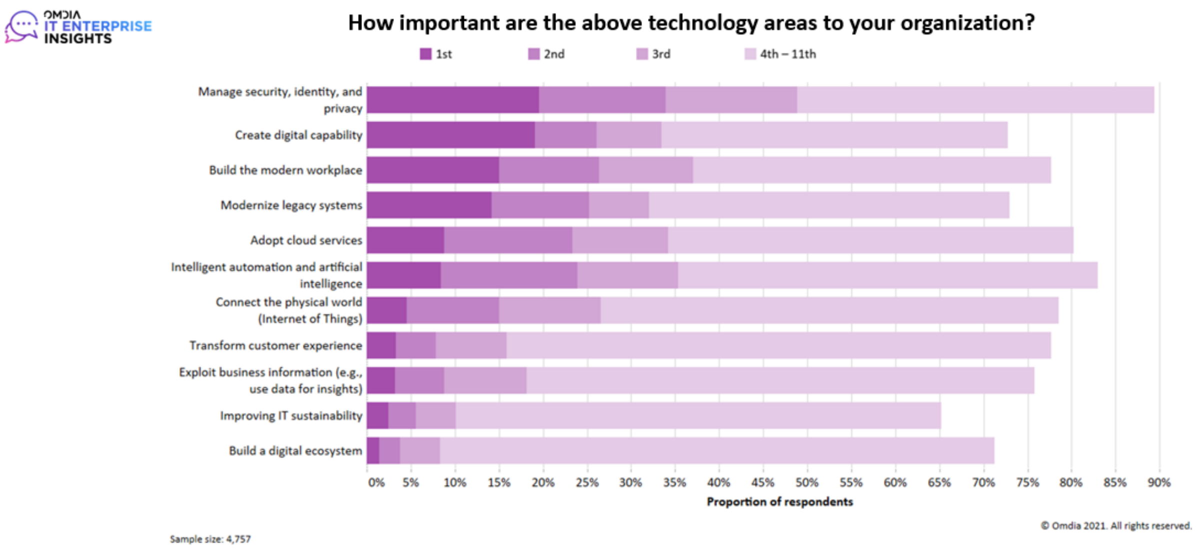
Sustaining software security over its usage lifecycle is a key responsibility

Security protection has become ever more business-critical

Many enterprise customers are attempting to transform their IT to keep up with the accelerated pace of change within their markets and business by leveraging technology opportunities such as cloud, mobility, and analytics. Commonly, there is an ongoing balancing act between investing in digital transformation initiatives (taking advantage of new and enhanced applications and business processes) and needing to ensure that the changing live environment is operating reliably with bulletproof security. The range of components of the IT infrastructure that must be secured is extending, not only encompassing the traditional "stack" from operating systems to hardware to databases, middleware, and applications but also including cloud-based and other third-party services. Outside the traditional IT boundaries, any enterprise presence in the consumer mobile environments must incorporate built-in security protection, because intentionally or otherwise, mobile users are prone to take actions that may open the device to compromise from threats.

Any lack of protection within the extended IT infrastructure can result in downtime that can impact the entire business and, in some circumstances, in security breaches that can cause violations of industry regulations and compliance procedures. Either outcome can lead to revenue loss—whether it’s an immediate consequence of downtime (i.e., loss of sales and customer engagement), or longer-term regulatory fines due to breaches or otherwise proven lack of security protection. Unsurprisingly in this context, responses to Omdia's ICT Enterprise Insights 2021-22 showed that managing security, identity, and privacy is the top IT priority compared to other key technology-related investments (see Figure 1).

Figure 1: Managing security, identity, and privacy is the top IT priority



Source: Omdia ICT Enterprise Insights 2021-22

With the IT industry itself becoming increasingly interconnected (e.g., via technology partnerships) to support digitalization, the cadence of software releases is now a lot faster than customers have historically been accustomed to. While customers benefit from vendors competing more keenly than ever with new features and functionality, their IT estate represents a broader attack surface that can be subject to a greater range of threats from malicious actors. Leading vendors are increasing their commitment to respond to threats by issuing patches for known cybersecurity vulnerabilities, and an organization keeping its estate up to date with vendor-supplied patches is the primary and timeliest means of protecting against software-related threats. New releases and patches may also require customers to retro-patch elements of their "stack" (e.g., middleware, OS, or database) to fulfill support conditions, and the chain of protection-related dependencies between stack components requires ongoing focus. For example, particular firmware updates from Intel have been known to require corresponding patches to OS and virtualization layers, and for older processor types, mitigation of processor issues does require disabling certain features (hyperthreading) if running untrusted workloads.

It is not hard to understand why security is an urgent issue among enterprises of all types, given what a security incident or breach can mean for an organization's business and reputation. News stories 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 (e.g., incidents involving Equifax and CapitalOne). There have already been examples of compliance-related penalties being increased because of inadequate patching procedures, and this could happen again as regulations and legislation become more severe (e.g., 4% of global turnover for breach-related noncompliance under GDPR). Beyond the direct financial impacts, these events typically lead to lost revenue and a sullied reputation for the affected enterprise, with potential losses in business and customer loyalty that are difficult to recover from. Most enterprises recognize the need to protect themselves as much as possible from potential cybersecurity threats, but they must also realize that those threats can come not only from external hackers but from failing to maintain up-to-date internal security protection throughout the IT stack.

Individual technology trends bring particular patching challenges

More recent technology trends bring fresh patching-related challenges, the complex cloud market being a particularly strong example. This market has passed a major inflection point, with adoption moving from a significant minority of workloads (respondents stated that 45% of workloads were running in some form of cloud, according to Omdia's IT Enterprise Insights 2021-22 survey) to most organizations now having a cloud-first policy. It was clear even in the midst of the COVID-19 pandemic that it was accelerating the adoption of cloud services, particularly IaaS and PaaS. And with the increased reliance on services that enable remote working, Omdia raised its five-year SaaS growth CAGR to 16% (up from 10%), a 60% increase in forecast SaaS annual revenue growth rate. But with all variants of cloud services, we believe there is a considerable element of uncertainty or evolving awareness within organizations over related management obligations, with patching being a particularly concerning area.

Starting with an example from the IaaS variant of cloud offering, customers still have to manage the operating system (OS), and so manage patching of that level of software. Understanding the different patching issues that arise when using different cloud model variants introduces further complexity, and when lines of business (LOB) take the driving seat in aspects of cloud adoption, they may be ahead of the security and IT operations teams' capabilities to manage patching issues. In the realm of SaaS, organizations' migrations to cloud usage can involve transferring their on-premises license for software to the cloud environment—but they may not realize their continued responsibility for patching the application environment. As such migrations typically necessitate replicating legacy integration arrangements, including APIs, these too may involve different patching considerations post-migration, which can easily be overlooked. And of course, many organizations eventually transition to using multiple cloud providers for varying reasons, but patching-related considerations might be quite different across the different contractual arrangements.

Patching is a cornerstone of IT governance and its support of compliance responsibilities

Companies today cannot afford to bypass having a rigorous software security and maintenance program, especially since 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, because they have the most experience and expertise when it comes to patching, supporting, and securing their own products.

Companies of all sizes and in all industries need to partner with a trusted provider to put procedures in place to keep their software security current and to address potential vulnerabilities. Unmitigated software vulnerabilities can allow malicious 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 severity.

Grave concerns were exposed over the status of software in relation to threats when in 2021 the US Cybersecurity and Infrastructure Security Agency (CISA) issued a directive requiring federal agencies to patch known exploited vulnerabilities within specific time frames. The agency referenced a catalog listing approximately 290 vulnerabilities, originating as far back as 2017, which were being actively exploited in attacks against federal entities and other organizations. The catalog will be updated as new, dangerous exploits become known, and extend the period over which organizations need to act.

The new directive reflected the high level of concern within government and the private sector over attacks like the supply chain assaults involving SolarWinds and Kaseya, as well as exploited vulnerabilities in Microsoft Exchange, Pulse VPN, and other VPN products in the period prior to the measure. Those attacks affected a wide number of organizations and often involved vulnerabilities that organizations should have known about and patched against long ago. CISA has a process whereby departments and agencies are required by law to develop a plan to comply with binding operational directives, and to follow through with action, and CISA itself is accountable to the Secretary of Homeland Security and the National Cyber Director for success of the directive.

A number of other regulations and standards include patching-related stipulations, including:

- PCI DSS Requirement 6.2, which requires that an assessor examine organizations' policies and procedures to verify that there is an established process for patch management
- ISO/IEC 27001 Section 12, which mandates that technical vulnerabilities should be patched, and there should be rules in place governing software installation by users.

Many compliance obligations now stipulate organizations' responsibility to ensure appropriate security within third-party suppliers and partners. Unpatched vulnerabilities cause third-party risk, and therefore compliance issues within the digital supply chain, but monitoring this status as a primary partner is challenging. Contractual terms with partners, covering this issue, should ensure that best practices propagate, and constitute best efforts towards compliance.

Given this backdrop, companies increasingly tell Omdia 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. For many compliance regimes, it is essential that documentation is maintained to prove how measures undertaken (at both policy and operational levels) meet compliance requirements. Automation of patching is likely to provide the most effective means of meeting such reporting requirements in the future as well as ensuring efficiency and avoiding greater impact of increased resource demand related to expanding patching requirements.

Most regulations are either transaction based (e.g., in financial services and banking), data management based (e.g., data privacy and records storage in healthcare), or both. At Omdia, we regularly recommend that companies, 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 undertake transformative digitalization initiatives that will bring software to a more critical position in support of processes of all kinds. 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 company to work with its 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 five to 10 years ago.

Risk is avoided only if patches are acquired from reliable sources

Some companies undertake software patching and maintenance only when there is a degradation of performance, functionality, or reliability, or when a headline-grabbing security threat forces them to see what potential security holes need to be plugged. Sometimes in these circumstances, informal information sources, such as advisory web sites, might be used to research solutions and, potentially, also to source patching content. This can be a serious error that directly introduces risk if the patch turns out to be rogue or introduces technical error. Given ongoing security and compliance issues and the increased frequency of security breaches and attempted security hacks, many companies have decided they need a more formal approach, with regular software monitoring, patching, and maintenance as core functions of their IT operations. The breadth of scope of this kind of approach is well aligned with compliance and governance needs, incorporating a high-level view of the "lifecycle" of vulnerabilities and patches. This contrasts with some point solutions (e.g., database firewalls and web apps proxy) that claim to counter vulnerabilities but are limited in functional range and do not in any way provide a risk-oriented approach that is business aligned.

Numerous organizations provide Patching Management (PM) solutions, marketed as the necessary answer to the patching risk dilemma. However, these vary in the range of their technology coverage, and their logic can fail to “see the wood for the trees,” causing unmanageable volumes of patch-related alerts requiring action. Some solutions are known to recognize software versions improperly, or may fail logically to eliminate risks, causing false positives. A high proportion of known vulnerabilities are not exploitable in the context of which the software is deployed, but some PM tools could well highlight them as potential problems, especially if they misidentify core information such as a version number.

We should note, also, that the now-widespread use of open-source code within organizations brings further challenges in defining with any permanency where is the authoritative “source” from where any patches should be recognized.

Therefore, a considerable level of care is important when relying on any third-party services relationship for provision of software support. Inadequate definition of requirements could allow a service provider to get away with implementing "workarounds" as partial solutions to vulnerabilities to close down ticketed support requirements. In addition to constituting a potential risk because of their inadequate provenance, these are likely to cause increased costs of ownership because of their divergence from the software's standard development path, introducing regression costs at a later stage. Services vendors ultimately need to demonstrate that they are acting as a partner with customers and their software vendors around software patching and support needs, and they should demonstrate three important characteristics:

- **Trusted provider.** A trusted and tested provider has knowledge and expertise in securing data and enterprise IT environments and long-term experience handling enterprise-class security and support.

- **Security expertise.** A provider must have experience in securing the entire IT stack, across infrastructure, databases, and applications, and expertise in providing proactive and real-time support resources whenever and however required.

- **Comprehensive offerings.** A provider should offer a full, integrated suite of security and support offerings that are constantly evolving and innovating and be able to help a customer establish a culture focused on IT security and compliance.

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

Furthermore, 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, because 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 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 roll out, software updates required a time-consuming update of the firmware and the entire platform because Exadata is an engineered system designed to deliver benefits as an integrated platform. Building on those experiences, Oracle introduced Platinum-level support for Exadata in 2012. This provides greater visibility into the backend 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 become critical.

The enhanced support level also provides the customer with 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 provide assurances that its systems are less vulnerable and more secure. Since 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 service level agreements 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 expects 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.

Recommendations

- **Make any culture change necessary to stop patching being viewed as an optional or merely operational consideration; ensure it is considered an essential element of organizational wellbeing.** Organizations need to realize that decisions to reduce their commitment to assiduous patching can adversely impact software integrity and so cannot be considered solely in an operational context. Inadequate patching can lead to exploitable vulnerabilities within organizational software, and while patches remain unapplied, the time available for malicious actors to cause loss continues to extend. The resulting security, compliance, and risk implications are impossible to resolve without completion of the necessary patching, and delay increases the likelihood of potential costs to the organization.

- **In light of these implications, decisions on patching policy need to be reviewed in a broad business context, not just by considering tactical and operational elements such as additional licensing or perceived support savings.** A fit-for-purpose patching process should be the objective, which avoids sole reliance on particular tools, ensuring that intelligence is continually applied. Practices such as use of unsupported software versions, poorly managed or partially executed third-party support, or reliance on poor advice sources need to be effectively eliminated.

- **While the ideal aim is to patch anything and everything necessary, any prioritization must be risk driven.** IT environments must be thoroughly understood from a risk perspective, in both a business and a technical context. The former considers the relative business criticality at the level of individual services, which clarifies the impact of related business-level risks (e.g., financial and reputational). The latter considers the technical characteristics of constituent service elements (e.g., OS, database, hardware, and applications) and any challenges due to particular vulnerabilities that are active as well as their exposure via networking to different threat environments (e.g., if resources are internet facing).

- **Patching information must be from authoritative sources, otherwise using it constitutes risk.** Governance of patching must stipulate what sources of patching guidance can be considered trustworthy. For example, software suppliers are the authoritative source of security information for their products, whereas the internet is not a source of dependable patching guidance. Additionally, sources such as the National Vulnerability Database (NVD) and computer emergency response team coordination center (CERT/CC) are managed and authoritative, whereas generic software-vulnerability scanning tools can be insufficiently specialized to deliver reliable information. For example, such tools can fail to appropriately recognize a software version specifically enough (and, as a result, the relevant release of security), causing inaccuracy in their reporting of outstanding issues and a “garbage in, garbage out” effect. In any case, reporting is the highest level of value that these tools can provide, and organizations are still required to assess and source requisite patches for themselves. The exception is where provision of outsourced patching services is in place: here, governing services agreements must stipulate that only the most reliable sources of patching information may be used.

- **Patching processes must not be the weak link in organizational protection.** Organizations need to commit to executing patching as part of regular security maintenance within their recurring maintenance activities. Patching is a key proactive protection measure and is a critical aspect of good IT security governance. Failure to plan and prepare for periodic maintenance activities will result in incomplete patching and, ultimately, a degraded security posture that links directly to increased board-level concerns over security. Conversely, a commitment to integrating that IT governance with the application of carefully sourced patches, driven by an overall process of excellence and intelligence around patching, will avoid many problems that can degrade the operations, finances, and reputation of any organization.

Appendix

Author

Alan Rodger
Senior Analyst, Infrastructure Solutions
askananalyst@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.