Security: Cloud-based or Home-grown

What to look for in a cloud-based CPM app

The fast-changing number and nature of potentially devastating data security threats has led many organizations to conclude that home-grown measures to protect their critical data and applications just can't keep up. This is especially critical for companies that use a Corporate Performance Management (CPM) system for financial management and planning. When choosing cloud-based CPM, what do decision-makers need to know about the application and data security?

The stakes are high. Mishandled data exposes companies to risks of data theft, extortion, denial-of-service attacks, corporate espionage, and malware, among other threats. Decision-makers must understand that only the very largest and technologically sophisticated organizations are likely able to build walls thick enough to defend against most risks. Unless your business is data security, your organization is not going to get ahead of the threat curve. Best practices change weekly as new threats emerge. The people you hired last month to defend against one type of threat may not have the skills you need for next month's attack.

This checklist of best practices is a good place to start when choosing cloud suppliers for your applications and data.

How robust is the underlying platform?

Whether securing an entire application or the organization's financial planning & reporting tools in the cloud, look at the service provider's underlying platform. Is it one of the established giants, like Microsoft Azure, IBM Web Services, Amazon Web Services or Google, or is it a small operation like Joe's Really Neat Cloud Hosting? Are the security controls of the underlying platform up to speed? Can it expand and contract when you need it to? What can it accommodate?

Is it SOC 2-certified? The American Institute of Certified Public Accountants designates different levels of Service Organization Control Reports. SOC 2 is an auditing procedure that ensures your service providers are securely managing your data to protect the interests of your organization and the privacy of your clients. SOC 2 defines criteria for managing customer data based on five "trust service principles." They are security, availability, processing integrity, confidentiality and privacy.

A SOC 2 Type 2 report is in-depth and valuable. A 3rd party auditor is required to test the effectiveness of the security controls; really look at how they work, and review samples to see how they are functioning. This means you can be confident that the appropriate security controls are in place and actually working. Many organizations start their SOC 2 process by having a SOC 2 Type 1 report done, and later move on to a Type 2. But SOC 2 Type 2 is a must.

Align certifications

About the underlying platform, are all security certifications aligned? What information framework underpins the system? Is it ISO 27001:2013 compliant (formally known as ISO 27001:2005)? Is there a specification for an information security management system (ISMS)? An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. Are they being re-certified on a regular basis?

Does your provider have a third-party auditor?

Robust information security and breach security must also be subject to regular third-party audits that are shared with you. An auditor will offer informed opinions and disaster recovery will also be tested. A good cloud services provider will share its audit report and results from regular SOC disaster recovery testing. With robust information security and breach security, your auditor will weigh in on its effectiveness. A good cloud provider should also share its SOC 2 Type 2 reports with its customers when requested.

A third-party auditor should assess your provider on at least a six-month rolling basis to ensure its security controls are up to date and providing the protection you require.

Require transparency throughout

Understand operationally how transparent your cloud vendor is. For example, with regard to service level agreements on up-time, your provider may report it has a five nines level of availability. That means it has an uptime of 99.999 percent. But does that up-time include your application? Your provider's cloud services may be available 99.999 percent of the time, but if the application you are running in that cloud is fully functional less than that time, it will interfere with your ability to securely conduct business. Look for application up-time of 99.5 percent or greater.

Does your provider have a dashboard or status page that reports availability statistics?

How often does your vendor patch the system all the way up the stack to the application? Less than every 30 days and you may be at risk.

Avoid the shoe-horn model

Some cloud vendors that operate a multi-tenant style of cloud have difficulty segregating all their customers and ensuring an impact on one customer isn't going to affect another. In a multi-tenant model, you can have data bleed and other integrity and security issues. Multi-tenant vendors may find themselves playing catchup on security issues. Seek a vendor with security built in from the ground up; in which each customer has its own unique instance. With scores of customers each on the same instance, the actions of one can affect others.

Flexibility

Can your provider expand or contract to meet your needs on the fly? Can it meet the needs of businesses or business units of any size?

A culture of security

In most cases, a CPM cloud vendor with good underlying security reduces risk compared to a home-grown solution. Even the largest organizations can't maintain the aggressive patching model of the right cloud provider, nor is it likely to be able to maintain rigorous synchronization of all systems, especially those with automated processes, or effectively address zero-day attacks -- attacks that take advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

Even the largest organizations are challenged to maintain a security depth comprising concentric rings of security -- physical security; perimeter security; host intrusion prevention; file integrity management; identity and access management and automated anomaly response – all while having a centralized place where everything gets logged. This in-depth strategy may take years to implement and would cost millions of dollars to do in-house, even if an organization could find and keep all the right people with the right skills.

Corporate Performance Management has proved its value in making organizations faster, more responsive, more effective, and more insight-driven.

But greater reliance on data means a requirement for greater attention to security to achieve those benefits. Risk management must permeate the organization, from the C-level throughout. That means identifying, reviewing and mitigating all risks in today's constant cyber battleground. But CPM with the right security-culture and partners is the approach that enables the most competitive organizations to take advantage of major operational, financial and planning benefits.

Kristofer Laxdal
Director, Information Security

Kristofer is an experienced Director of Information Security with a demonstrated history of working in the computer software industry. He is an information security executive skilled in cyber security, vulnerability management, IT service management, IT strategy, and data center operations.

Head Office

350 Burnhamthorpe Road W,
Suite 1000 · Mississauga, Ontario
Canada · L5B 3J1
+1 (905) 279 8711
+1 (800) 387 5915
info@prophix.com

Additional Offices

USA: +1 (800) 387 5915
UK: +44 (0) 118 900 1900
Europe: +45 7023 2375
DACH Region: +49 69 509 565 605
Brazil (Rio de Janeiro): +55 21 3094 3900
Brazil (São Paulo): +55 11 3583 1678

Prophix®

www.prophix.com