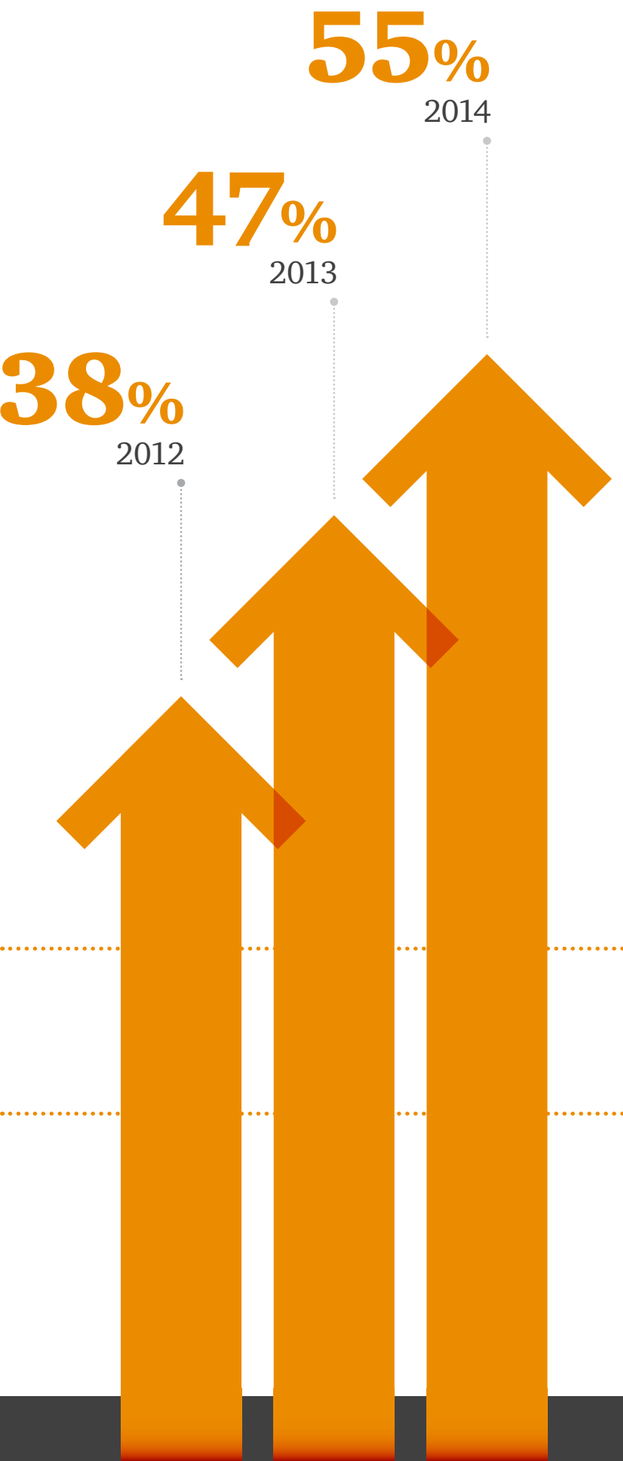
How cloud-enabled cybersecurity will transform your business

pwc



How cloud-enabled cybersecurity will transform your business

Cybersecurity is at a crossroads.

As more businesses discover and leverage the full capabilities and potential of cloud services, their cybersecurity models ultimately may be transformed. In recent years, cloud computing has become mainstream across many industries as organizations realize that the potential benefits are simply too great to ignore.

The cloud can help businesses achieve operational efficiencies, instant scalability, price elasticity, expanded computational and processing power, and cost reductions. Adoption of cloud computing also can help organizations transform a range of business processes. These can include high-performance customer portals, payment platforms, sensitive modeling and engineering processes—essentially any legacy process can be transformed.

Tentative early implementations of cloud services have given way to large-scale deployments of business functions such as customer relationship management (CRM), talent management, payroll, and enterprise communications and collaboration.

In fact, 55% of organizations across industries and across the world now use some form of cloud computing, according to The Global State of Information Security® Survey 2015.[1]

1. PwC, *CSO* magazine, *CIO* magazine, *The Global State of Information Security ® Survey 2015*, September 2014

While the cloud is officially mainstream, many executives still worry that provider security practices are not robust enough to protect sensitive data and mission-critical workloads.

This perception is shifting, however, as major cloud services vendors continue to develop and implement increasingly sophisticated security capabilities.

Our research shows that **59%** of businesses that use cloud services report that doing so has improved their information security program.

When applied to cybersecurity, the advances in cloud security technologies can be equally transformative. Cloud-based cybersecurity can improve intelligence gathering and threat modeling, better block attacks, enhance collaboration and collective learning, reduce the lag time between detection and remediation, and create secure communications channels. Factor in potential cost reductions, and the potential of cloud-enabled cybersecurity becomes all the more compelling.

Why we're not keeping up with the pace of change

By all counts, cybersecurity incidents continue to increase and show no sign of abating. Our annual security survey found a 66% combined annual growth rate (CAGR) in cyber-attacks over the past five years.[2]

As security incidents multiply unchecked, it is becoming clear that most organizations are not keeping up with the pace of change in cyber threats; the reasons will come as no surprise to most security executives.

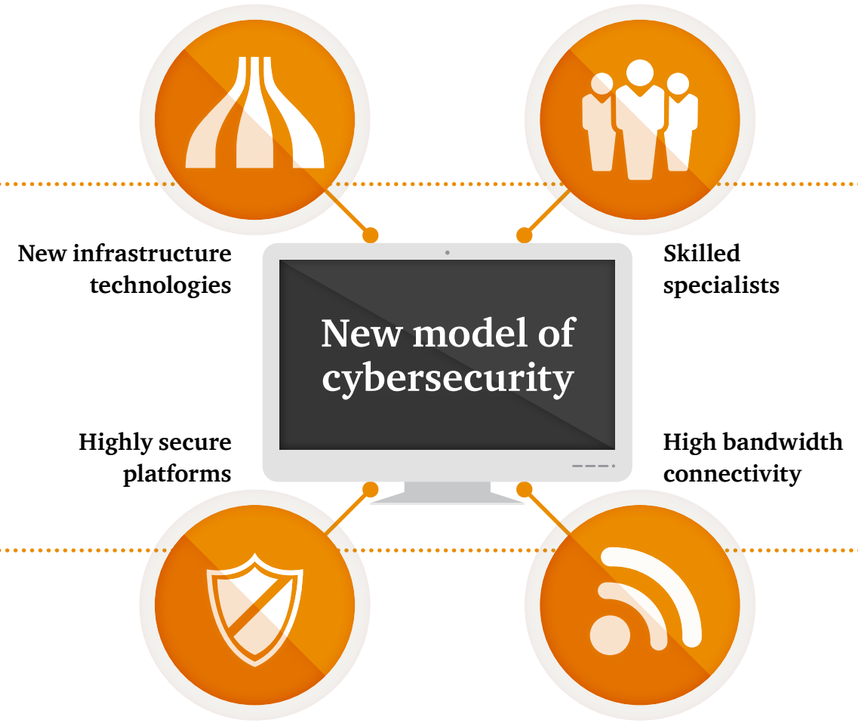
The systems, structures, and computer science that underpin today's business ecosystems have grown into a patchwork of layers, non-integrated tools and technologies, and overly complex architectures that are often ineffective. Management of this type of ecosystem requires financial resources and highly skilled security specialists, both of which are in short supply. As a result, many businesses may find it difficult to justify the total cost of ownership and return on investment.

Several factors are compounding this already challenging situation.

The proliferation of layers has expanded the attack surface—the points on which adversaries attempt to access data. Furthermore, the forces of digitization of information, mobility, and the nascent Internet of Things are pushing the technology perimeter far beyond traditional control boundaries, making information security exponentially more difficult. At the same time, well-funded threat actors are launching technically sophisticated assaults that, when successful, can siphon off valuable data undetected for months or even years.

Despite the rising risks, many businesses do not seem to be taking adequate precautions. Our annual survey found that information security budgets have decreased in the past year, and as a result organizations are falling behind in key technologies, processes, and personnel skills required to detect and respond to constantly evolving threats.

Clearly, a more effective approach is needed, and we believe that model is cloud-based cybersecurity. It will enable organizations to leverage world-class and highly differentiated operational security capabilities in an elastic and non-capital-intensive way.



2. Ibid

Harnessing cloud power to improve security

As cloud services become increasingly sophisticated and secure, businesses are shifting more of their traditional network architecture to cloud-based systems.

This changeover is much more than a "lift and shift" of old architectures and processes from on-premise systems to the cloud. Rather, it is a fundamental transformation in which businesses are leveraging the unique properties of the cloud model to achieve business advantages.

> If correctly adopted, cloud computing will enable organizations to take advantage of the flexibility and simplicity of cloud architectures that transcend the barriers of traditional IT. Creating this next-generation of IT capabilities is, in fact, the ultimate goal of cloud service providers.

Over the past decade, top-tier providers have reviewed the fundamentals of computer science and improved computing power and scalability through an architecture of simplicity.

From the beginning, they understood the power of newly built cloud platforms. What they did not foresee is how these advances and their innate capabilities, when combined, could potentially disrupt the traditional models for information security and managing cyber risks.

Today it's clear that cloud platforms can provide a game-changing new model of cybersecurity. Their capabilities include not only very high-bandwidth connectivity among global data centers, but also the ability to develop high-performance cloud-based business applications that are elastic in performance and scale.

The cloud also can enable organizations to combine additional infrastructure technologies such as software-defined perimeters to create antifragile and highly secure platforms. These platforms can be designed to block most tools, techniques, and procedures (TTPs) used by malicious actors. In addition, principles of DevOps combined with communal learning can dramatically reduce the lag time between detection and remediation of incidents.

Cloud-based security will also significantly reduce the need to purchase, maintain, and enhance technology infrastructure and hire support personnel, enabling companies to address security fundamentals at a lower cost. These can include "clean pipe" solutions to protect against DDoS attacks, application of industry best practices around software development, and infrastructure-management processes like application and operating system patching.

The cloud also can boost the effectiveness of Advanced Security Operations Center (ASOC), a fusion of technologies and services typically created by large businesses to detect, analyze, and investigate cyber-attacks. A cloud-based ASOC that shares information among member organizations enables businesses to leverage and continuously learn from the collective intelligence.

The knowledge may be general and include all incidents and threats, or it may be specific, providing aggregated intelligence on specific threats and incidents gathered from all customers in a specific industry.

This collective model is new and represents a fundamental shift in how businesses approach information sharing.

In traditional models, organizations learn only from the intelligence gathered by their individual IT environment. We believe that the concept of collective learning will create a market-enabled information-sharing platform. That, in turn, will result in real-time, integrated security information sharing on a scale that has not been accomplished to date.

Cloud-enabled cybersecurity also will enable businesses to instantly deploy secure communication and collaboration environments using a cloud provider's infrastructure. This will create, in effect, a safe repository for sensitive information. It will also enable organizations to implement separate access and communications capabilities around key transactions such as mergers and acquisitions or research and development initiatives. These out-of-band channels also can be created on the fly to enable secure communications when businesses are under cyber-attack. Alternately, they can be employed proactively as disposable infrastructure, or used for one time only in connection with highly sensitive business transactions.

Taken together, cloud architectural advances can enable businesses to apply agile, dynamic responses that can be moved, hidden, hardened, dummied, and adapted when information assets and applications are threatened. It is a bold concept that very well may disrupt the current model of information security by outsmarting and rendering useless the majority of intruder attack tactics.

In addition to technology advances, cloud providers are increasingly gaining certifications and assessments from third-party guidelines and regulatory bodies to prove their security capabilities.

These include ISO 27001, Level 1 service provider under the Payment Card Industry Data Security Standard (PCI DSS), SSAE 16 (formerly SAS 70), various SOC audits, DIACAP Level 2 for Department of Defense Systems, and Federal Information Security Management Act (FISMA). Many providers also have the capabilities to enable regulated organizations to deploy solutions that meet industry standards like Health Insurance Portability and Accountability Act (HIPAA).

The safest place to store sensitive data

Advanced technologies and industry certifications are convincing more businesses—even those operating in highly regulated sectors like financial services and healthcare—to put sensitive data and mission-critical workloads in the cloud.

According to Verizon's Enterprise Cloud 2014 report, 71% of respondents from 988 companies run external-facing production applications in the cloud, up from 60% the year before.[3]

41% of enterprises that employ Infrastructure-as-a-Service (IaaS) use it for mission-critical workloads.

3. Verizon, *State of the Market: Enterprise Cloud 2014*, October 2014

Just because more businesses are entrusting sensitive data to cloud providers doesn't give every organization the green light to do so, however.

It's an individual decision that should be very carefully considered and discussed. In some cases, mission-critical workloads and intellectual property may still be safest in the locked-down confines of the enterprise. Similarly, regulated data like payment card information and healthcare records should be sent to the cloud only if the service provider has security controls that match or surpass those required by the organization and its regulators.

Increasingly, however, we believe that top-tier providers are creating ecosystems that are safe for sensitive data. They are building security into the core fabric of the infrastructure to create an entirely new class of defenses that are possible only with the game-changing properties of the cloud.

While traditional information security concerns are valid and addressing them is essential to develop a best-in-class cloud strategy, we would argue that not only can the cloud be secure, it can be one of the safest places to store your sensitive data and mission-critical workloads.

PwC and Google: A cloud-centered solution

While the potential advantages of cloud-based cybersecurity are compelling, most organizations do not have the expertise, resources, and reach to design and implement their own solution. It is an initiative that is simply too complex and costly for a single business.

What's needed is a partnership of industry leaders with complementary expertise. To that end, PwC and Google have developed a cloud-based cybersecurity solution that fuses the two companies' technical, business, and process capabilities. The Google solution can help provide unprecedented data protection by leveraging cutting-edge, scalable, and proprietary technologies to analyze and understand cyber activity and information. The solution is built around a risk-based cybersecurity strategy to provide advanced detection, analysis, and collective learning.

PwC and Google can help business stakeholders strategically identify their critical assets and quantify cyber value at risk (CyberVAR), then use this assessment to determine priorities and process steps to improve cybersecurity. Organizations can then examine their current-state technology platforms and infrastructure that support these processes, collect the "operational exhaust," and then pipe that exhaust up into the cloud platform.

Once the data is on the cloud platform, PwC and Google will help businesses leverage high-performance, scalable analytic processes, combined with Google threat-information repositories, to enable an advanced security operations capability (ASOC).

If the ASOC identifies anomalous or unauthorized activity, it will trigger an issue alert that can then be addressed. The benefit is that the collective system will continuously learn from experience, and this approach will likely create a highly effective market-enabled information-sharing platform.

» The Google Cloud Platform's capabilities can provide unprecedented data protection by leveraging cutting-edge, scalable, and proprietary Google technologies to analyze and understand cyber activity and information.

A safe harbor for the most sensitive information

Certain business activities require very sophisticated security and real-time detection.

Cloud-enabled cybersecurity will enable businesses to instantly deploy secure communication and collaboration environments using Google infrastructure—creating, in effect, a safe harbor for sensitive information. These out-of-band channels can be created on the fly to enable secure communications when businesses are under cyber-attack. Alternately, they can be employed proactively as throw-away infrastructure or used for one time only in connection with highly sensitive business transactions.

» At its most basic, this safe harbor can create a secure bunker that empowers and protects the business by integrating security-hardened laptops running Google's Chrome operating system, the power of Google's security-monitoring operations that protect the Google Apps infrastructure, and advanced analytics that enable real-time detection of activity by sophisticated threat actors.

An integrated ecosystem for security defense

An entirely new class of defense comes into focus when these innovations are viewed through the lens of security.

The final, and by far most powerful, scenario will be the transformation of business processes in the Google cloud via dynamic Infrastructure-as-a-Service (IaaS) capabilities wrapped around the application. These highly secure, Chrome-based applications are configured to instantly respond in appropriate ways when an analytic anomaly is detected. One response, for example, might be instant, imperceptible re-spawning of a new instance elsewhere in the Google cloud. IaaS also can enable software-defined perimeters that will likely allow businesses to implement high-side/low-side networking without hardware.

Taken together, these architectural advances can enable businesses to apply dynamic responses that can be moved, hidden, hardened, dummied, and adapted when information assets and applications are threatened.

It is a bold concept that very well may disrupt the current model of information security by outsmarting and rendering useless the majority of intruder attack tactics. This approach also is likely to cause disintermediation to the security solutions market.

Additional defenses against cyber attacks

Cloud-based cybersecurity also will enable instant creation of honeypots, dummies, and decoys that can maintain connections to the endpoint for analysis and learning, or distract and disrupt the efforts of the attacker.

Given its deep global business and industry-sector knowledge, PwC is well equipped to develop the dummy, decoy, and honeypot content. We can take advantage of real-time threat analysis and dynamic responses using the Google Rapid Response forensics tool running at the endpoint to capture short-term analytic inputs, in addition to the operational exhaust.

In the long term, PwC can work with Google and various vendors to ensure that their technology platforms natively expose this security data in a way that doesn't impact user experience and protects privacy. What's more, we can capture additional use intelligence from mobile devices, giving the analytic engine visibility across the entire operating horizon.

The solution can help deliver unprecedented data protection by leveraging cutting-edge, scalable, and proprietary technologies.

Finally, we can continually integrate information uncovered by the zeroday team to help quickly generate DevOps fix tickets for remediation of zero-day exploits in close to real time. PwC will leverage open-source code sharing to pass updates to participants so they can rapidly integrate the fixes, thereby reducing the efficacy of the exploit. PwC and Google will work together to leverage our unique positions in the marketplace to create new data sets that can be used by all participants. This, we believe, will likely help advance defenses in the cybersecurity battle.

One key weakness may be authentication at the endpoint. To address this, we plan to leverage many factor authentication capabilities combined with hyper analytics to enable real-time behavioral and anomaly-detection capabilities.

Security is the cloud

We believe the architecture of this new paradigm will likely negate a vast number of the TTPs employed by attackers and will eliminate the use of ineffective, expensive, and burdensome security tool overlays.

It also will allow organizations to disintermediate the layer of proprietary security tools that slow operations and undermine the customer experience. This, in turn, will pave the way for a new model of security that allows security strategy to directly affect operations and vice versa, potentially driving both massive cost savings and agility.

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.