SECURING IP WITH CLOUD BASED TECHNOLOGY

August 2015

By Ben de Bont
Chief Security Officer | HP Cloud

> “Cisco Systems Inc. ranked law firms as the seventh most vulnerable industry to ‘malware encounters’”
>
> – Cisco 2015 Annual Security Report

Background: Focusing on What Matters Most

The ability to prioritize resources on what matters most is a common differentiator between elite and mediocre businesses. Successful companies know what is 'core' to their business mission and what is 'context'. One company's context is another company's core.

KEY TAKEAWAY

Most companies are not in the business of managing IT infrastructure at scale, and are smart to outsource these functions to the cloud providers whose core business *is* managing IT infrastructure at scale.

For example, few companies are in the business of human resources, facilities, or payroll. Rather than attempting to haphazardly fulfill these functions, many corporations outsource to other companies who specialize in these services, allowing each company to focus their resources on their core business.

Proficiency in shaping and scaling IT infrastructure and services to match business needs is key to the appeal of cloud computing. Cloud service providers specialize in one thing: outsourced infrastructure. They invest massive amounts of capital to offer customized, scalable IT services to downstream consumers, who may in turn build specialized services atop this bespoke virtualized infrastructure. Along with economy of scale, cloud service providers also have dedicated and specialized resources that are required to run and manage a successful cloud.

Security as a Barrier

Cloud services are now a mature, $100+ billion business. Today, 93% of organizations are actively using or experimenting with cloud technologies.[1] One of the few remaining barriers to the adoption of cloud computing is the perception of cloud security. This has been precipitated by the regular stream of well-publicized software vulnerabilities and breaches, creating an atmosphere of fear and suspicion of software quality that includes cloud technologies. In turn, this fear may hinder or prevent businesses from taking the next step in their journey to the cloud—a journey that is likely to lead to cost-savings, operational efficiencies, increased speed to market, and improved security.

KEY TAKEAWAY

Security is a fundamental pillar for top tier cloud providers. They invest millions of dollars in security technologies and expertise to protect the billions they have at risk. Very few private organizations can boast such heavy investment in security. When low-level security concerns are taken care of by the cloud provider, organizations can reclaim and reallocate resources to other priorities in their core business.

As with any defensive system, we must assume that today's shields may not protect us from tomorrow's weapons. This is why continuous, significant investments in security solutions are necessary for ongoing vigilance against increasingly advanced, persistent adversaries. Rather than looking for holes in the perceived imperfections of cloud solutions, companies should compare the ongoing investment required to squash the current and yet-to-be-discovered vulnerabilities of their own legacy solutions to the costs of outsourcing, especially if provisioning, managing, and maintaining infrastructure is not core to their business.

For cloud providers, infrastructure *is* their core business. Cloud providers invest vast amounts of resources and expertise in hardening their environments, services, and products, whereas many traditional on-premise data centers do not.

For a cloud provider to flourish, they know they must earn their customers' trust. It is in a cloud provider's best interest to ensure robust security in their offerings, as it is essential to the cloud provider's existence. Trust is oxygen to the provider; without trust, their offerings will remain bare of customer workloads. For this reason, serious providers will always hold security as one of their most critical concerns, and invest accordingly.

Increased Risk for Legal Entities

The Chinese government, now the largest filer of patents in the world, has a national goal of tripling its patent filings over the next five years.[2] In July 2015, US Democratic presidential candidate Hillary Clinton accused China of targeting and stealing vast quantities of both commercial and government intellectual property.[3] This follows a long line of claims against China, most notably since the inception of the Mandiant APT1 report on the People's Liberation Army Unit 61398.[4] These attacks were allegedly designed to steal large volumes of intellectual property, predominantly from affluent western nations.

Legal entities are particularly attractive to attackers such as those discussed in the Mandiant report, who attempt to accumulate repositories of confidential data on corporate deals and business strategies—information which can be extremely valuable to foreign intelligence agencies and criminal organizations. Attackers often target low hanging fruit during an initial compromise. Smaller legal firms that do not have hardened environments or full-time security operations personnel fall into this category, as security is not their core business or focus. Furthermore, legal entities almost never publicly disclose security breaches, despite the sensitivity of the information that may be exposed. This is understandable, as there are few requirements on law firms to disclose breaches, unlike a bank or retailer, who is held accountable by strict breach notification laws.

> "I divide the entire set of Fortune Global 200 firms into two categories: those that know they've been compromised and those that don't yet know."
>
> – Dmitri Alperovitch, former McAfee Vice President

Security research supports these claims. In their 2015 Annual Security Report, Cisco Systems Inc. ranked law firms as the seventh most vulnerable industry to "malware encounters".[5] In Mandiant's 2012 report, it was estimated that 80 of the 100 largest American law firms had some malicious computer breach in 2011.[6] Despite these and many other reports, when representatives from several large law firms were approached by the New York Times on the issue, they stated privately that the threat landscape for law firms, as indicated by security consultancies and government agencies, was overstated.[7] They referred to the most common attacks against their businesses as email phishing schemes to access personal information or account passwords, and that attacks of that nature were easily contained.

Such thinking is questionable, as sophisticated, knowledgeable attackers make it almost impossible to determine whether a breach has occurred. This is especially true in the case of nation states or intelligence agencies that have the ability to leverage vast resources and expertise to achieve their objectives. Dmitri Alperovitch, formerly McAfee's vice president for threat research, reinforced these conclusions in the company's 2011 report on a vast online espionage campaign. Alperovitch stated: "I divide the entire set of Fortune Global 200 firms into two categories: those that know they've been compromised and those that don't yet know."[8]

Case Study: Patent Security

The top seven patent filing companies made up 10% of all patents granted in the US in 2014.[9] Just 288 companies, primarily large corporations, develop more than 50% of patents in the United States annually. All of these organizations have a critical vested interest in protecting

their intellectual property as part of their core business. Some have the resources and expertise to adequately secure their architectures. Regardless of a corporation's internal resources, it is a common practice to outsource various functions to smaller third parties. This is particularly common in the patent industry, where many large corporations outsource their patent processing to law firms. Given that many legal entities in the United States are boutique, firms hired by large corporations may not be able to invest heavily in security. Additionally, it is a common trend in the legal industry for employees to work remotely, either from home and/or public locations. As a result, intellectual property is regularly stored on portable devices, which may or may not be adequately protected, monitored, or recorded.

Patent processing involves numerous documents, drafts, and reviews, as well as frequent communication with a wide range of parties (depicted in the following diagram). There are many potential attack vectors in this complicated, conceptual data flow, excluding network paths and specific infrastructure.

SECURITY POINTS

Document and email servers exploited

Lost/stolen/misplaced devices and notes

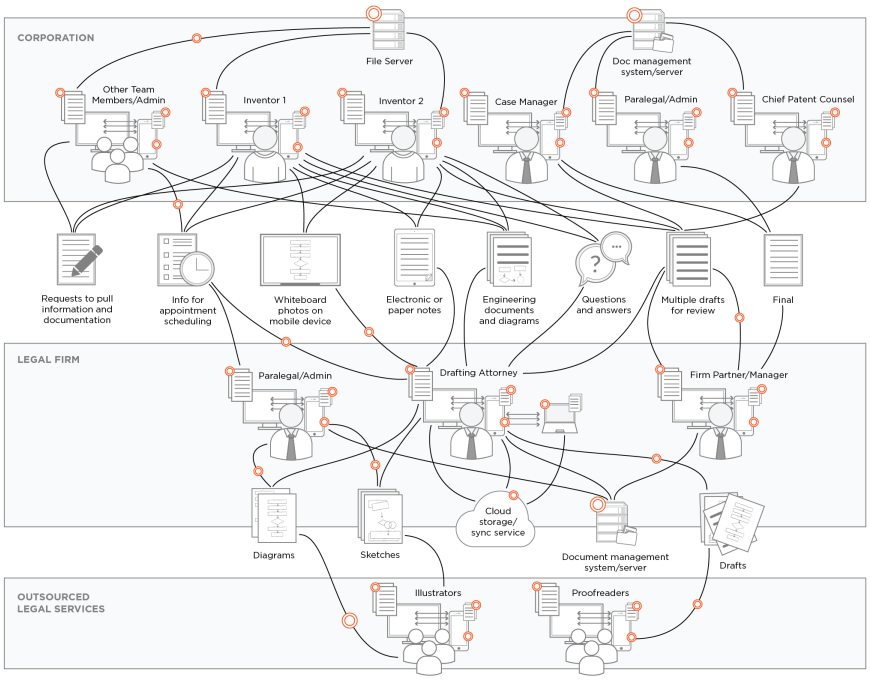
Various working copies on many machines increase likelihood of exposure to malware, malicious insiders, and poor data controls

MITM opportunities: Wifi networks, especially public networks (e.g. coffee shops)

Firms with inadequate security controls in place, unlikely to be encrypted

Physical disk loss/theft, RMA VPN attack on firms with inadequate encryption

Repudiation issues, loss of control



Beyond the possible areas of attack during the patent application process, there is also the issue of discoverability of sensitive communication during litigation of a patent. With so many devices storing various drafts of patent applications, and the communication surrounding those drafts, it is difficult to purge potentially sensitive information that could invalidate a granted patent. During the 20+ year patent application process and patent life span, this sensitive data can continue to spread to a wide variety of individuals, devices, networks, and locations with potentially poor security controls. Data backup and redundancy systems are unlikely to be purged of sensitive data.

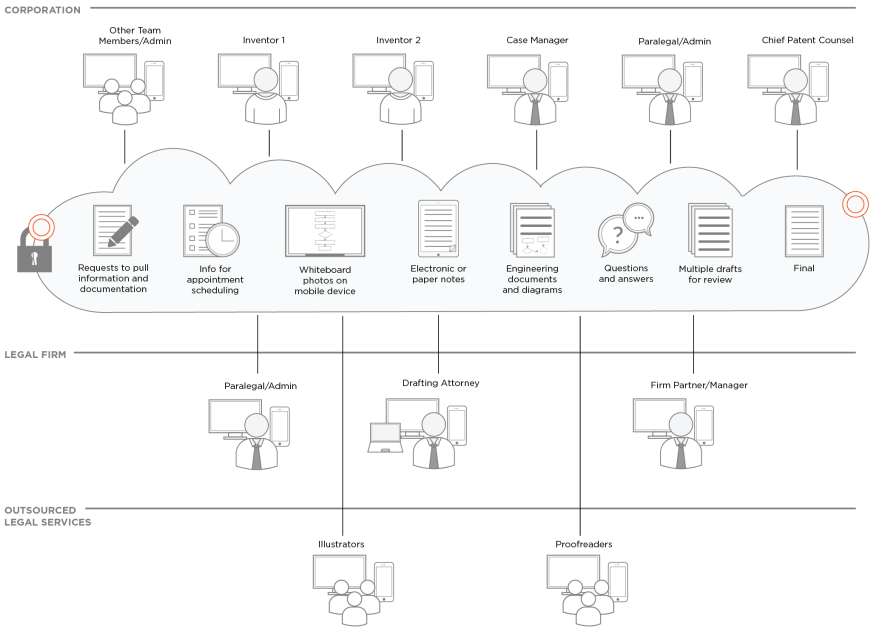
When converted to a cloud-based application, the attack surface of that same workload is dramatically decreased. However, if the cloud provider is compromised, then all sensitive data may be retrieved by an attacker in a single blow. This is why it is always important to assess the transparency, maturity, and effectiveness of a cloud provider's security controls, as they will vary by provider.

SECURITY POINTS

When migrated to a cloud application, the patent application process is a perfect demonstration of the benefits of cloud computing.

A convoluted, tedious, and highly vulnerable process is transformed into a powerful, globally accessible, easily tracked, and far more secure system. The most current version of documents can be viewed and edited on multiple devices, but stay in a secure cloud locker. Comments and communication can all be made within cloud applications.

Note: Attacks are still very possible, as no infrastructure is completely secure; however, the attack surface is greatly reduced.



With cloud providers, heavy investments are continuously made to provide customers with development tools, guidance, and a rich partner ecosystem of services. Security is of equal focus, with providers offering hardened infrastructure combined with detailed security guidance and tooling. Consumers can utilize additional security features such as encryption capabilities, region isolation, and add-ons such as WWH multi-authentication to further lock down their applications. Proactive security measures are also available, as many cloud providers offer security review, penetration testing, and workshops to guide consumers on how to build hardened, secure applications in the cloud.

No system is completely secure. However, successful cloud providers are experts in fulfilling the security and compliance requirements of their customers. Similar to the outsourcing of any other business function, by moving workloads that process sensitive data to the cloud, organizations can take advantage of cloud providers' expertise.

Where is Cloud Security Headed?

Regardless of the security claims of some cloud providers, consumer due diligence is an essential step of cloud adoption. Two of the most important fundamentals of cloud security are transparency into existing security controls, and an understanding that the consumer/

KEY TAKEAWAY

Cloud security is a shared responsibility. Cloud service providers will cover some, but not all, security controls. Even when dealing with the most recognized cloud services, it is ultimately the responsibility of the consumer to understand their role in securing their data.

provider relationship is a collaborative effort. Without transparency, there is no assurance that a satisfactory security program is in place. Consumer security requirements will often vary greatly, dependent on workloads, applications, data types, and their intended cloud use cases. They should not be driven by the latest breach or vulnerability notification in the press. Collaboration is also essential; it is the responsibility of the consumer to ensure that they have reviewed their cloud provider's security controls, and that their workloads are adequately protected from their end, as well as that of the provider. Advising bodies such as the Cloud Security Alliance provide solid guidance on cloud security threats, including a wealth of information about both consumer and provider security responsibilities.[10]

Conclusion

Attackers today are professionalizing, bringing vast resources and greater levels of expertise when attempting a data breach or compromise. It is unreasonable to expect smaller entities such as law firms to have sophisticated security controls on par with that of cloud providers. It is a concerning common practice to de-prioritize or ignore the validity of a threat until it is exploited and a data breach occurs. For cloud providers, it is essential to their core business that a robust security and compliance program is in place. For law firms, this is often not the case, at least until a public breach occurs. Clients of these firms may insist upon varying requirements, but without proactive security and compliance practices themselves, these mitigations are often inadequate. Moving workloads such as patent processing to the cloud can reduce the risk of a breach, and can be advantageous for organizations that are dedicated to protecting sensitive data, protecting their reputation, and driving continual revenue from new and existing customers.

"Moving workloads such as patent processing to the cloud can reduce the risk of a breach..."

[1] "State of the cloud report", RightScale [2015]

[2] China aiming to triple patents by 2020, Reuters, January 2015

[3] BBC News: "Hillary Clinton accuses China of "stealing US secrets" - 2015

[4] Mandiant Intel Report (http://intelreport.mandiant.com)

[5] Cisco Report 2015

[6] Mandiant Report 2011

[7] New York Times: "Law Firms Are Pressed on Security for Data" - Matthew Goldstein, 2014

[8] 2011 McAfee Report - Operation Shady Rat

[9] USPTO.gov -http://www.uspto.gov/web/offices/ac/ido/oeip/taf/topo_14.htm

[10] Cloud Security Alliance - https://cloudsecurityalliance.org/

Ben de Bont
Chief Security Officer
HP Cloud
Hewlett-Packard Company
www.linkedin.com/in/bendebont
twitter.com/bendebont

Executive Biography
Ben de Bont is Chief Security Officer for HP Cloud. He is responsible for all aspects of security for HP cloud offerings.

Prior to joining HP, Mr. de Bont led the MySpace Security Group as Director of Information Security (CISO), and sat upon the Global News Corporation Security Committee, working extensively with business units, including the Dow Jones and 20th Century Fox.

Mr. de Bont has also previously led the Incident Response Group for Microsoft's Online Services, and held security responsibility for Hotmail, MSN Messenger, and Search business units. He is an active and well-known member of the security community, contributing to groups such as OWASP, the Cloud Security Alliance, and OpenStack security globally.

Mr. de Bont holds a Master of Science degree in Computer Science from the Queensland University of Technology in Brisbane, Australia, and an undergraduate degree from the same institution. His thesis addressed 'Digital Watermarking Encryption Algorithms Attacks and Defenses'. He holds numerous security certifications and has contributed to many publications.

Mr. de Bont's current office location is Seattle, WA.