# Practical Methods for Securing the Cloud

**Edward G. Amoroso,** AT&T

*Combining the various methods of securing the cloud infrastructure, services, and content can help meet or exceed the protection benefits of a traditional enterprise perimeter.*

The advantages of virtualizing servers, databases, and applications into the cloud are well known: hardware costs are reduced, content becomes more ubiquitous, and IT services can better adapt to an organization's changing needs. Such benefits have led to many new cloud initiatives, ranging from private cloud efforts behind corporate firewalls to the widespread use of publicly accessible cloud services such as Amazon Web Services (AWS).

Despite the success of these cloud-based initiatives and services, concerns remain about security protection. The financial services community, for example, is engaged in a vigorous debate about whether public cloud services are secure enough for financial applications.[1] The specific cloud threats generally cited include the compromise or unauthorized modification of cloud-resident financial data, as well as the possibility that denial-of-service attacks will cause cloud-resident financial data to become unavailable.

2325-6095/14/$31.00 © 2014 IEEE

Enterprise organizations and cloud service providers today are using several practical methods to secure their cloud infrastructure and services:

- *A private cloud with enterprise perimeters* is the most common large enterprise approach to securing cloud content.
- *A public cloud with service gateways* involves popular cloud services used by millions of individuals and businesses today.
- *Content encryption* focuses on protecting data stored in the cloud from unauthorized compromise and leakage.
- *Session containers* ensure that data are properly removed from client devices such as mobile devices after cloud access.
- *Cloud access brokers* integrate security measures such as authentication or access monitoring for users accessing cloud services.
- *Runtime security virtualization* integrates dynamic runtime virtual security functions directly into virtual entities in the cloud.

By properly utilizing these practical cloud security methods, an organization can meet or exceed the existing security capabilities offered by its enterprise perimeter. The goal of this survey is to provide cloud decision makers with broader insight into how best to mitigate cloud-specific security threats, thereby making this technology more acceptable to a wider range of industries, environments, and applications.

## Private Cloud with Enterprise Perimeters

The most common solution for enterprise organizations seeking to mitigate cloud security threats currently involves building a virtual infrastructure inside an existing corporate firewall (see Figure 1). With this approach, enterprise perimeter-protected datacenters host cloud services and/or are used to virtualize applications. These services and applications are accessible only to users who have been properly authenticated and securely admitted to the corporate intranet. This is a mature security approach that's consistent with existing protection strategies for all other enterprise assets.

Using a private cloud infrastructure within the enterprise, an organization gains the advantages of software virtualization, such as reduced hardware costs through shared virtual machines with high utilization, but without the security concerns that come from ubiquitous, open access. Enterprise auditors and regulators approve of this architecture because the familiar perimeter remains a primary control for security compliance. The safeguards inherent in the private cloud approach include the following:

- *Identity and access.* A private cloud available for internal enterprise users is easily integrated with existing identity and access management functions, such as corporate directory services. Products such as the IBM Security Identity Manager and Security Access Manager, for example, provide customizable identity and access management support for private cloud deployments.
- *Firewall, IDPS, and DLP.* Private clouds mediate external access from untrusted, nonenterprise users via the corporate firewall, an intrusion detection/prevention system (IDPS), and a data loss prevention (DLP) tool. Cisco Systems, for example, offers intrusion detection and prevention signatures that protect private clouds utilizing an enterprise perimeter.
- *Encryption.* Private clouds can integrate enterprise encryption capabilities, including key management to further protect cloud-resident content. Encryption solutions from companies such as Checkpoint Software support integration into cloud-resident data storage.
- *SIEM analytics.* Integration is usually straightforward between a private cloud and the enterprise security information and event management (SIEM) system, providing data analytics and incident response processes and tools. HP's ArcSite SIEM, for example, is often used in conjunction with a private cloud deployment.

Figure 2 illustrates the security architecture for a typical private enterprise cloud.

The challenge associated with private cloud implementations is that, despite the perimeter solutions available to protect the enterprise, the typical organization is still unable to stop attacks such as advanced persistent threats (APTs) from the Internet. In addition, complex policy-based decisions

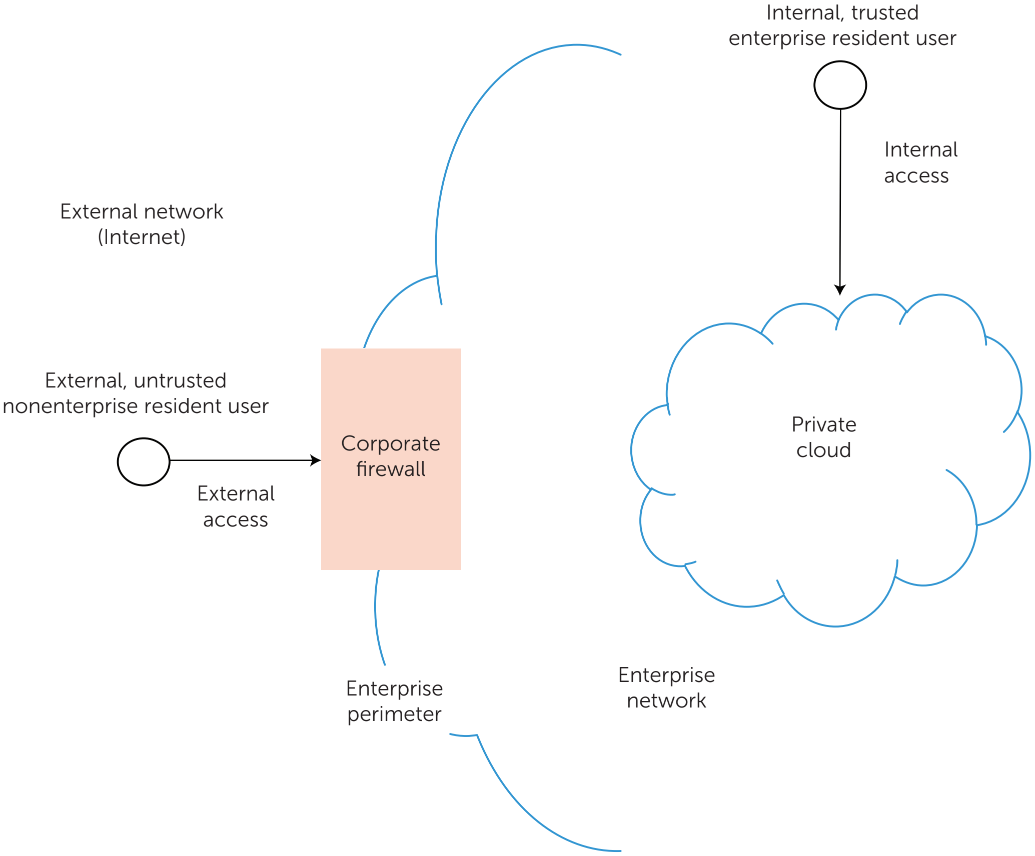
Internal, trusted enterprise resident user
Internal access
External network (Internet)
External, untrusted nonenterprise resident user
Corporate firewall
External access
Private cloud
Enterprise perimeter
Enterprise network

FIGURE 1. Private cloud with enterprise perimeter. As the most common solution for enterprise organizations, this mature security approach is consistent with existing protection strategies.

made over long periods of time to allow a multitude of enterprise services and approved exceptions through the corporate firewall, combined with the increasingly common method of bypassing the perimeter using mobile devices, have rendered the enterprise perimeter essentially useless from an advanced threat perspective.[2]

An additional fatal issue with private clouds is that enterprise security teams can't stop determined insider attacks. Even in the presence of segregation of duty controls, as with Sarbanes-Oxley relevant systems, the approach is vulnerable to collusion, which is easy to achieve with malware on multiple compromised systems. Thus, by situating a private cloud inside the enterprise and assuming that internal access can be trusted, an organization places its cloud infrastructure at direct risk of compromise.

The result is that private cloud infrastructures have devolved into architectures that are indistinguishable, at least to the security engineer, from public cloud systems. Purveyors of private clouds may have control over vendor selection, cloud service features, degree of sharing between users, and day-to-day system administration, but the idea that they're immune to external attacks because of enterprise perimeter protections is no longer justifiable. As such, private cloud deployments should never rely on an enterprise perimeter as their sole security control.

## Public Cloud with Service Gateways

A second approach to cloud security involves using the native protections in a public cloud service. Public cloud service providers generally differentiate their services via the familiar "XaaS" designation, where X is a wildcard for "infrastructure," "compute," "software," "storage," or even "security." For the purposes of this discussion, we can abstract such distinctions to focus on the common underlying architectures in the various public cloud services.

The primary public cloud security solution involves dedicated service gateways in front of the cloud platform, customer data, and business support systems (see Figure 3). Specifically, cloud users log into their accounts through dedicated

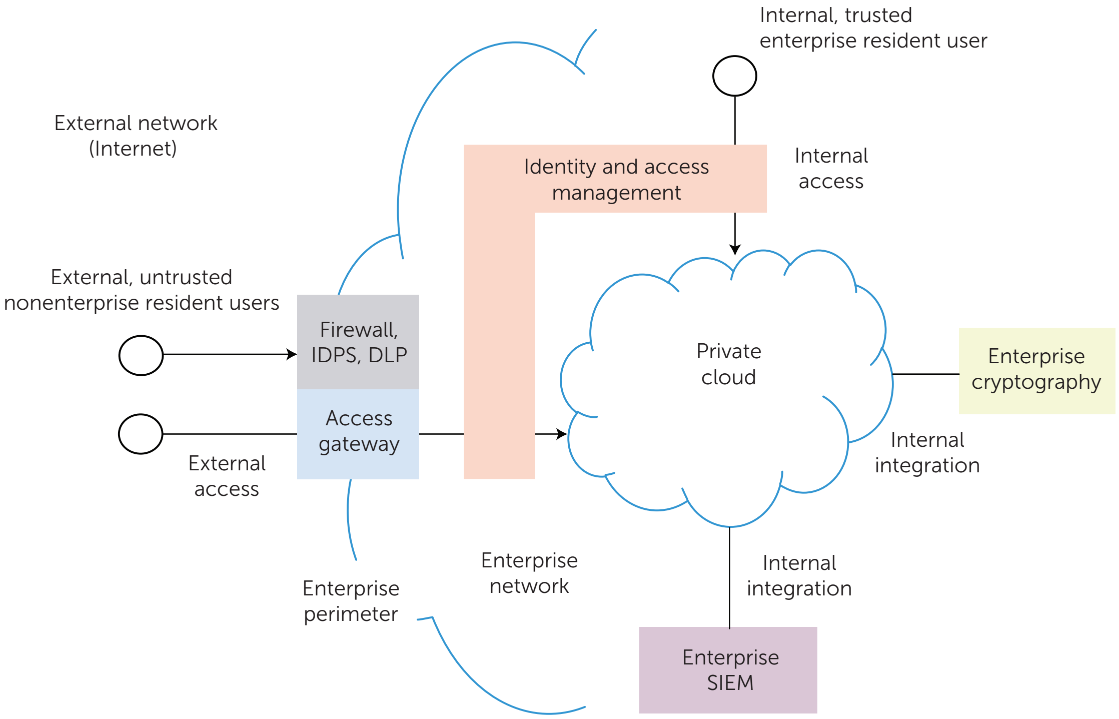

FIGURE 2. Private cloud security architecture. Private clouds may incorporate additional enterprise safeguards such as encryption and identity management to protect cloud-resident data.

service gateway interfaces, cloud administrators log into their accounts via side channel infrastructure gateways, and cloud developers gain access to services and infrastructure through API gateways.

Admittedly, the gateway approach to protecting public cloud services is similar to the enterprise perimeter because chokepoints separate trusted, internal networks from untrusted, external users. The difference, however, is that public cloud service gateways are dedicated to the cloud service and aren't subject to the security risks of everyday enterprise usage (email phishing, firewall exceptions, direct mobile access, and so on).

Organizations such as financial services firms (as mentioned earlier) have expressed low confidence in public cloud security because of a perceived loss of infrastructure control. Such lack of confidence is inconsistent with the common reliance of business entities on shared services such as the Domain Name Service (DNS). Similarly, every organization must connect to the Internet through a service provider, which may introduce shared risks. The security controls in public cloud services include the following:

- *Service provider perimeter*. Cloud service providers, like all service providers, run an infrastructure behind gateways integrated with perimeter security functions, such as firewalls, IDPS, and DLP. Public cloud services also typically deploy SIEM functionality inside the provider enterprise.
- *User account security*. The most basic security primitive for cloud service provision is the user account. Key security issues include user authentication, provisioning controls, and the administrative and access controls used to manage accounts.
- *User separation*. Cloud services include logical separation mechanisms that prevent cascading of malware across user accounts or break-ins from one user's cloud assets to another.
- *Content distribution*. A content distribution network (CDN) reduces distributed denial-of-service (DDOS) risk for public cloud services. DDOS controls offered by Internet service providers can complement a CDN as well.
- *Virtualized security capabilities*. Public cloud offerings can bundle advanced security functions, such as incident response, that some smaller enterprise customers or individuals might not be able to afford.

Figure 4 illustrates the typical security architecture for a public cloud service offering.

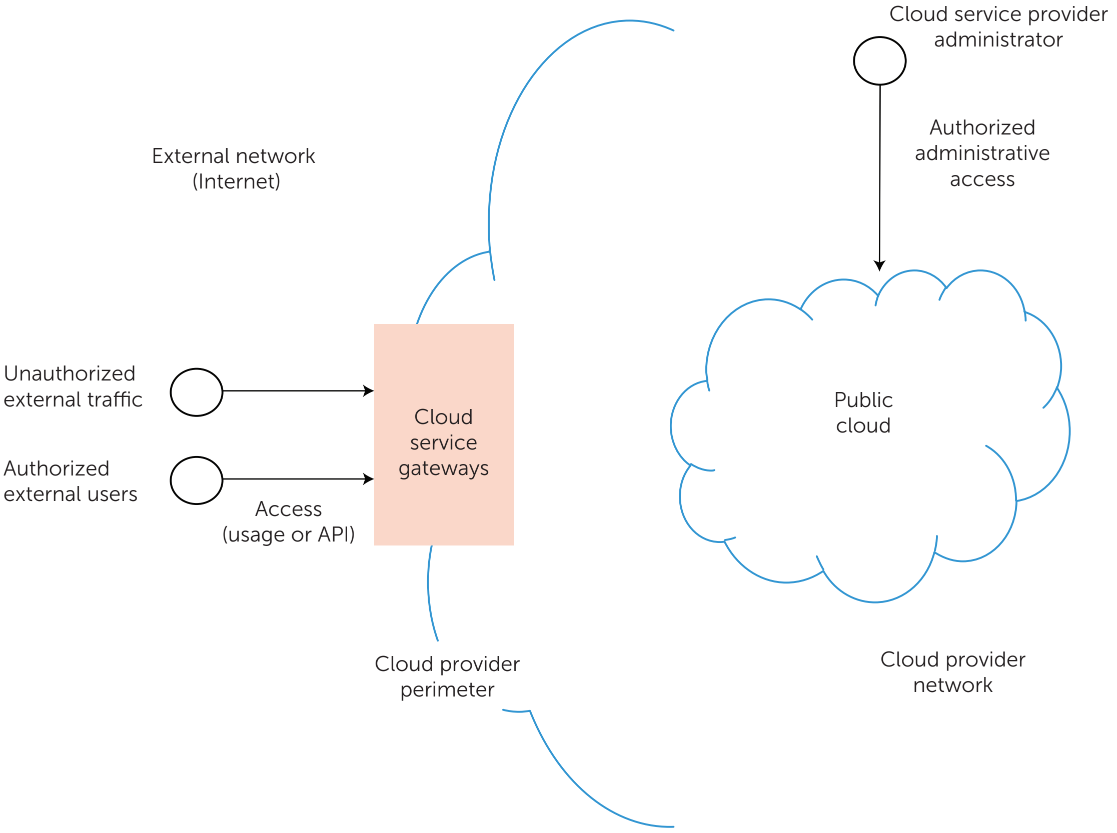

FIGURE 3. Public cloud with service gateways. The gateway approach isn't subject to the security risks of everyday enterprise usage.

Many organizations choose to combine public and private clouds into a hybrid arrangement. Hybrid clouds introduce orchestration issues for security mechanisms that differ between the component clouds. For example, identities established in one cloud will require federation to other hybrid elements. The adoption of a public cloud for dedicated or even hybrid arrangements thus requires a degree of transparency on the part of the public cloud service provider.

Organizations considering the use of public cloud services must analyze whether advantages such as Internet-facing ubiquity outweigh the risks inherent in any shared, external service. These risks will vary between providers—as in, for example, the ability of that provider to fend off denial-of-service attacks. Dropbox is a popular public cloud service that provides security solutions, including strongly authenticated user accounts through gateways and user control of permission settings through an account management tool. Nevertheless, public cloud users should integrate additional security controls such as the ones described in the remaining sections here.

## Content Encryption

To address data confidentiality, cloud encryption is generally designed to ensure that cloud-resident content can't be retrieved as plain text by APT malware or by compromised insiders with direct access inside a perimeter. The encryption algorithm's strength and key management should be based on risk analysis. Encryption tools can be integrated on top of a public or private cloud infrastructure or can be selected from native encryption features offered by the cloud service provider (see Figure 5). The over-the-top encryption approach lets users maintain control of key management and infrastructure, but it usually increases costs.

Cloud encryption works only if the underlying cryptographic algorithm or supporting key management can't be broken. Strong, resilient ciphers that utilize expert cryptanalysis are readily available, so the primary focus is generally on the security of the underlying key management. Stated simply, if malicious actors can easily gain access to decryption keys, then encrypted cloud storage is useless. The primary security requirements for encrypted content in the cloud are as follows:

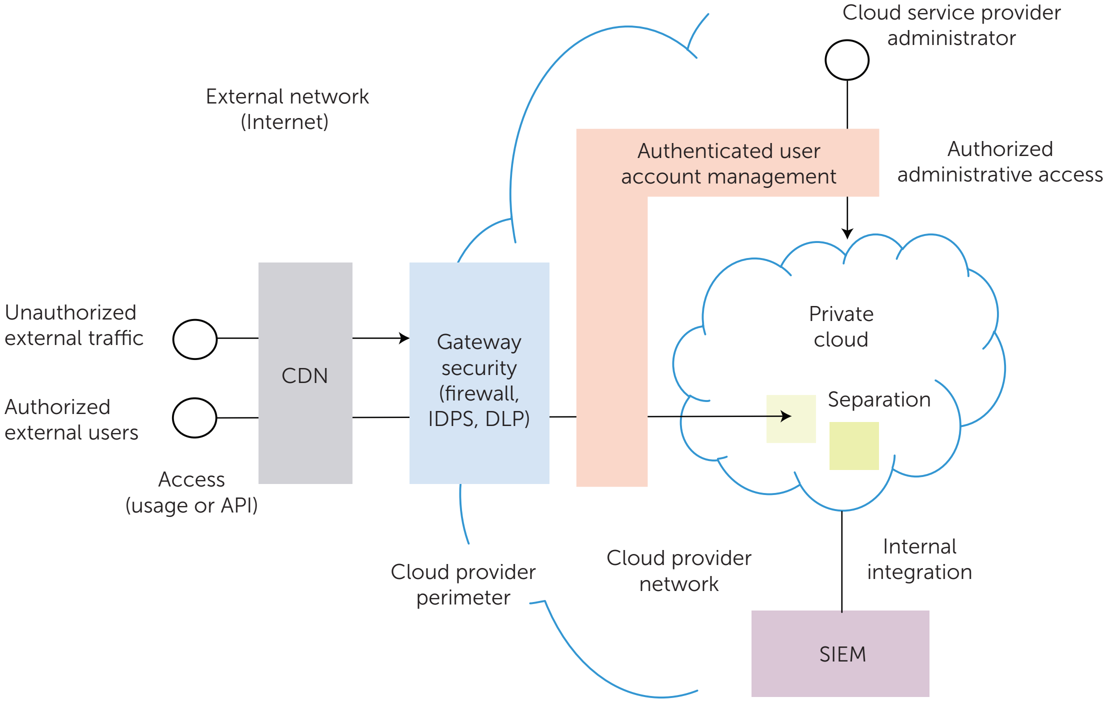
Cloud service provider administrator
External network (Internet)
Authenticated user account management
Authorized administrative access
Unauthorized external traffic
CDN
Gateway security (firewall, IDPS, DLP)
Private cloud
Separation
Authorized external users
Access (usage or API)
Cloud provider perimeter
Cloud provider network
Internal integration
SIEM

FIGURE 4. Public cloud security architecture. Cloud service providers run an infrastructure behind gateways integrated with perimeter security functions.

- *Stored data secrecy*. Encrypting cloud data prevents backdoor leakage and restricts access to privileged users and administrators. Many companies provide encryption for cloud systems data at rest, including Pawaa, which encrypts files at the device before they are sent off to the cloud infrastructure for storage.
- *Cloud storage malware resistance*. Encryption provides malware resistance for stored data, especially in the case of remote access tool (RAT) attacks that target individuals with authorized access to data. Additional tools exist to ensure that malicious users don't insert malware directly into the cloud. Companies such as CipherCloud, for example, include filters that scan in-bound and outbound cloud content for the presence of malware.

The functional requirements for most cloud ciphers include maintaining search capabilities for stored data as well as the ability to perform big data analysis. CipherCloud's Searchable Strong Encryption (SSE) is one example. Such interoperability with public, private, or hybrid cloud capabilities and associated business processes is an important requirement for encryption solutions. Cloud federation and orchestration of key management infrastructure in hybrid systems require a bit more attention, but they're still practically workable.

## Session Containers

A cloud security solution for mobile access to a public cloud involves a *session container* (see Figure 6). The idea is that any user interested in obtaining access to cloud services or content would initiate a secure connection that would maintain end-to-end closure, not unlike the way HTML5 sessions are encapsulated between the browser and website. Such closure usually requires a software client-server arrangement with the provision that no residual information exists on the client device after the session has been completed.

A key consideration for session containers involves support for multiple personas. Bring-your-own-device (BYOD) environments, for example, require differentiation between corporate personas, where session-contained access to proprietary applications such as payroll systems is done under a corporate persona. Correspondingly, access to nonbusiness relevant applications such as games or YouTube is done under nonsession-contained access in a noncorporate persona.

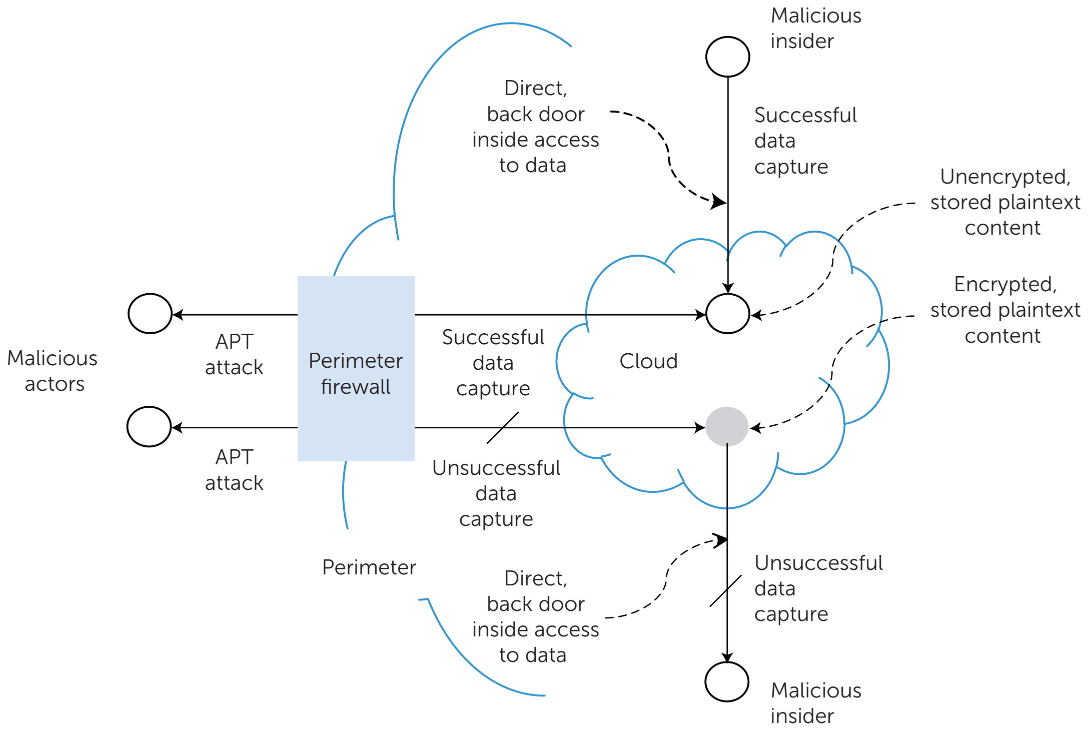
Malicious insider
Direct, back door inside access to data
Successful data capture
Unencrypted, stored plaintext content
Encrypted, stored plaintext content
Malicious actors
APT attack
Perimeter firewall
Successful data capture
Cloud
APT attack
Unsuccessful data capture
Perimeter
Direct, back door inside access to data
Unsuccessful data capture
Malicious insider

FIGURE 5. Encrypted content in the cloud. Encryption tools integrated on top of a public or private cloud infrastructure can further protect cloud-resident content.

One additional consideration is the degree to which data that temporarily reside on client systems are properly wiped. Algorithms for secure wipe are available, and session container users should check with their vendor to ensure acceptable implementation of well-known standards.[4] Session containers provide security benefits for cloud services in the following functional areas:

- *Client system data wipe*. Session containers ensure that, once a user has completed access to a cloud-resident object such as an application, the associated data are properly wiped from the client device. Invincea, for example, provides a session container solution that allows for access to cloud applications from a variety of devices, such as mobile smartphones, and wipes the data securely afterward.
- *Data separation*. Session containers provide dynamic separation of different user activities within the cloud. The separation is enforced at the client and server levels by controls that keep data from being intermingled with resources outside the container. The company Bromium uses hardware assistance to ensure trusted separation during user access to cloud resources.
- *Multiple persona support*. The idea of compartmentalizing different personas on a client device is long established in computer security. Modern implementations of BYOD programs using session containers generally allow granularity at the persona or application level. AT&T's Toggle product, for example, provides flexible multiple persona support with the ability to create customized server controls.

Most session containers include support for end-to-end encryption, although this may not be required for less critical applications, especially in private clouds. Encryption might incur minor additional overhead and additional key management infrastructure support. When end-to-end encryption is employed, integrity, secrecy, and authentication functions are supported on a per-session basis.

The biggest practical issue with session containers is whether they work with legacy computing. In complex environments, session containers often can't create the runtime support environment required for user access and local computing requirements. Thus, local testing is necessary to determine the feasibility of this approach. Nevertheless, organizations are advised to integrate session containers into their use of public, private, or hybrid clouds.

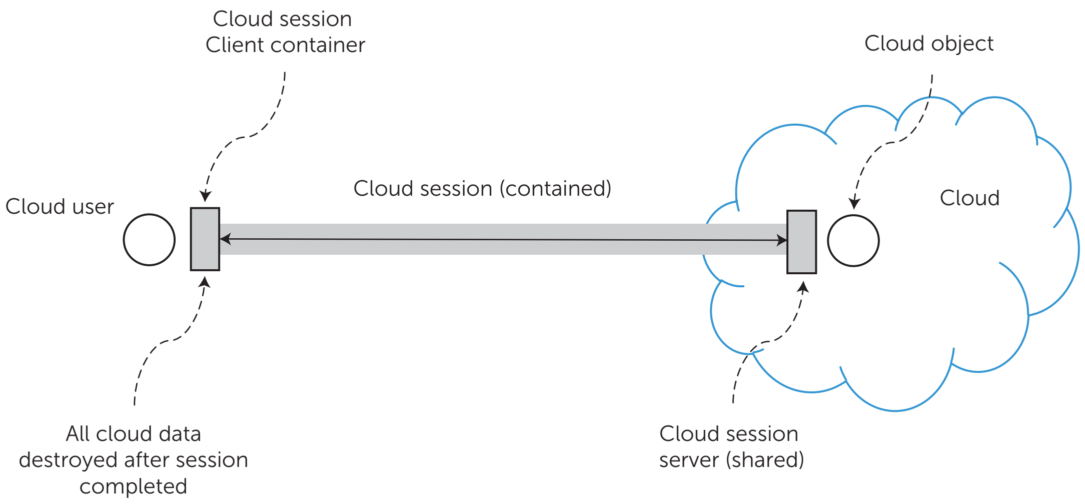

FIGURE 6. Session container. The user may obtain access to cloud services or content via a secure connection that maintains end-to-end closure.

## Cloud Access Broker

A security method that provides additional security capability for cloud application usage involves the use of a broker that either observes or integrates with the authentication path from users (see Figure 7). For example, the Gartner Group has introduced a concept called a Cloud Access Security Broker, which includes more functionality (such as encryption support) than just proxy or simple gateway services.[3] Nevertheless, this article uses the terms "gateway," "proxy," and "broker" synonymously. The idea behind such man-in-the-middle security functionality is that when any user decides to access a cloud-based application, a special broker, often implemented as a forward or reverse proxy, can be used to provide enhanced security.

Brokers can be *passive*, in which case indicators and security statistics are provided, or *active*, in which case in-line mitigation is possible. If the cloud access is encrypted, as in a session container, the cloud access broker will require the ability to interrupt the end-to-end secrecy. Providing certificates and keys to brokers has always been an issue of some debate, because it breaks the end-to-end nature of the client-server secrecy.

Brokers implemented as proxies have been included in security architectures for many years. Positioning proxies at the perimeter has been the basis for several growing successful companies, such as Blue Coat Systems, which offers a proxy solution for enterprises that works well with private clouds. With cloud access to public or hybrid clouds, the proxy must be more ubiquitous and virtual because no perimeter exists. Blue Coat has successfully virtualized their proxy capability to support this type of use.

The specific security advantages of the cloud proxy method include the following:

- *Passive security monitoring*. Off-line cloud access brokers can passively collect statistics about the use of cloud services. This may be desirable for organizations that want to better understand the intensity and nature of public cloud use from the enterprise. Adallom provides a cloud access proxy tool that resides in the authentication path between clients and cloud applications for the purpose of collecting information for security teams.
- *Active security mitigation*. Cloud access proxies in active mode can mitigate malware or policy violations in real time. Generally, such a capability is similar to a Web application firewall (WAF), even when the solution resides between clients and cloud solutions, rather than applications on Web sites. Qualys offers a WAF solution called QualysGuard that integrates well with common cloud services such as AWS.

Cloud access brokers allow for flexible integration of new security capabilities. A provider can modify an existing broker collecting information about one attribute to collect information about another property. Similarly, an in-line broker such as a WAF can be adjusted to meet a changing policy or maintain consistency with changes in an application. This is a double-edged sword, however, because changes in applications require that the WAF also be adjusted. Thus, WAF maintenance is more complex than tradi-

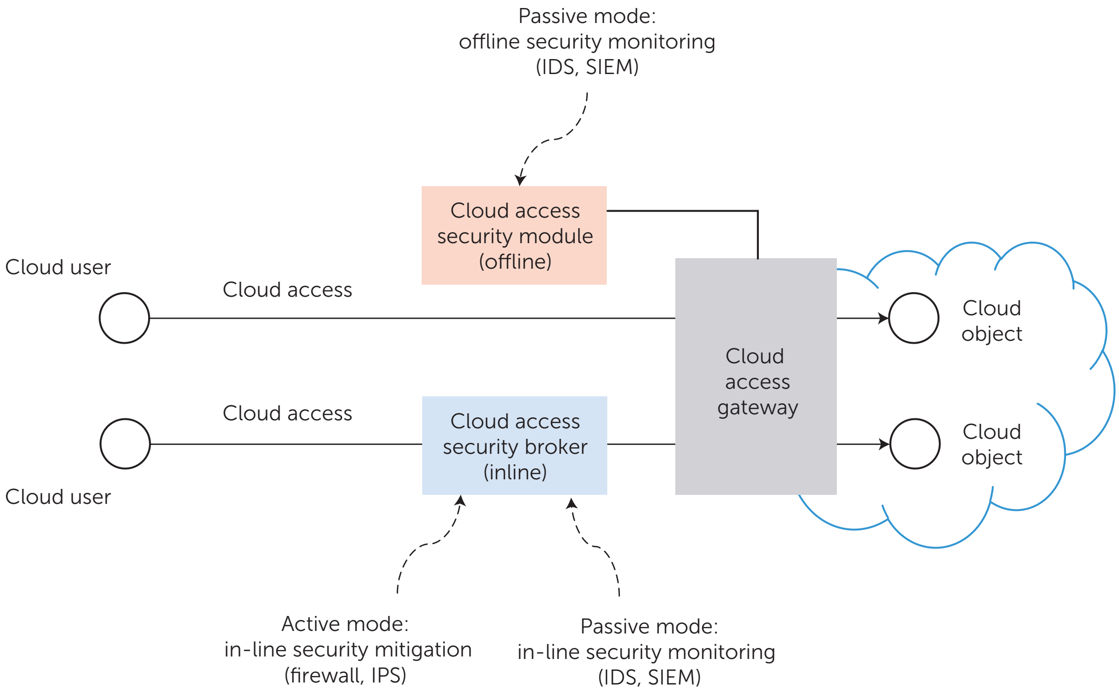

FIGURE 7. Cloud access broker. Brokers, often implemented as a forward or reverse proxy, can provide either passive security monitoring or active security mitigation.

tional five-tuple firewalls, which often require no rule changes when applications are modified.

Nevertheless, broker solutions for cloud access will likely be important components in cloud security architectures in the coming years. They can help simplify access from an organization to multiple vendor clouds, for example. They're also comparable in their operation to familiar security tools such as firewalls, so compliance auditors should accept brokers as suitable control replacements as organizations virtualize on the cloud.

## Runtime Security Virtualization

The most innovative security solution in the cloud ecosystem involves the dynamic creation of runtime security virtualization. The idea is that as the computing, storage, and infrastructure are embedded in a virtual runtime system, security functions such as firewall, IDPS, and DLP should be embedded in the same environment (see Figure 8). The result is the dynamic creation of runtime security components that are virtualized alongside the cloud objects they're intended to protect.

An example of runtime virtualization involves the provision of a virtual WAF to protect an HTTP application. Traditionally, the application resides on a physical Web server, accessible by users with browsers. Any WAF can be inserted physically into the network access path, either as a proxy or gateway function. If we port that application to a virtual machine on a hypervisor-based system integrated into a cloud platform, then the WAF can be virtualized as well. In particular, the WAF would exist as a virtual machine appliance woven into the execution, tracing all users accessing the application from their mobile, desktop, or other device.

The primary security controls offered by the runtime virtualization approach to cloud security include the following:

- *Security for dynamic objects*. As objects such as virtual machines are created into the cloud, the security protections associated with such objects are created dynamically. In essence, they create a customized runtime environment for the cloud object. AWS offers this type of protection for many of its services in conjunction with companies such as Tenable Systems and AlertLogic.
- *Tunable policy based on assets*. With runtime security virtualization, different assets that reside together in the same cloud can be associated with different security protections. Because providers can customize security, an object with a low security risk might have light functional

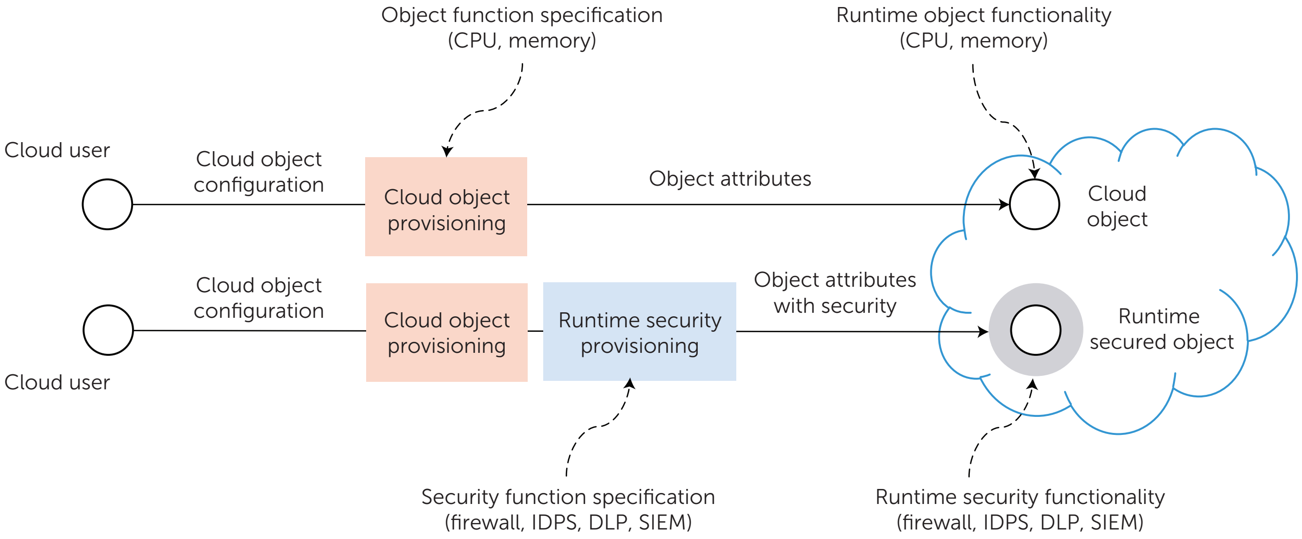

FIGURE 8. Runtime virtualization. Runtime security components are virtualized alongside the cloud objects they're intended to protect.

protections, whereas another object with high risk might include multiple, more intense security functions. Catbird provides a cloud security platform that includes virtual machine appliances that allow for customization of protection across different assets.

- *Flexible security vendor management*. The dynamic nature of virtual runtime protections allows for multiple layers of defense using different security vendor products. In addition, if a vendor is no longer desired or needed, it can be easily decommissioned from the runtime environment by simple changes in API calls.
- *Expandable security protections*. During an event such as a DDOS attack, a provider can dynamically expand the runtime environment to include more protection. Layer 7 intrusion-detection support for DDOS protection from companies such as Radware can be virtualized to expand during a major attack and contract afterward.

The advantages of this runtime approach have led to the planning and development of security marketplaces for cloud service users. AWS has already established an impressive portfolio of security companies offering dynamic runtime protection. VMware includes support for such runtime protection as part of its native suite of cloud services. Service providers such as AT&T are also in the process of creating similar marketplace offerings for their customers.

The most important consideration in securing cloud services and infrastructure is whether the methods selected can properly mitigate relevant threats. Many readers would list compliance as the top of their priority list, especially with respect to winning customer contracts for cloud services, but compliance frameworks measure attention to management process rather than whether a target system is actually secure. Industry groups such as the Cloud Security Alliance (CSA) have done a good job advancing this notion of security versus compliance.

Determining whether a given arrangement of practical cloud security methods for some environment can sufficiently mitigate threats must include two important thresholds. First, it must be determined whether the cloud security methods provide equivalent protection to an existing perimeter, because the vast majority of practical cases will include a legacy enterprise demilitarized zone (DMZ). Second, it must be determined whether the cloud security methods adequately mitigate advanced attacks, which implies some target degree of protection higher than existing cloud solutions.

The possible solutions for threat protection are either below the state of the practice (solution A in Figure 9), above the state of the practice but below target protection levels (solution B in Figure 9), or above target protection levels, but below perfect (solution C in Figure 9). Although accurate threat assessment requires a detailed investigation of local assets, possible threat vectors, and the consequences

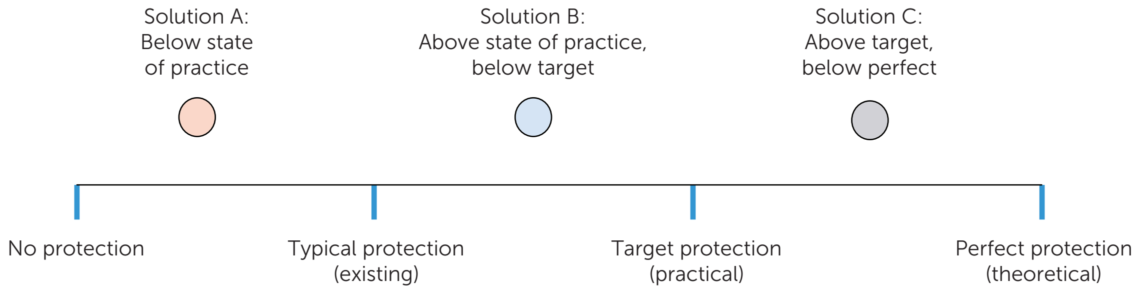
Solution A:
Below state of practice
Solution B:
Above state of practice, below target
Solution C:
Above target, below perfect
No protection
Typical protection (existing)
Target protection (practical)
Perfect protection (theoretical)

FIGURE 9. Security protection effectiveness. Today, solutions for threat protection range from below the state of the practice (solution A), above the state of the practice but below target protection levels (solution B), or above target protection levels, but below perfect (solution C).

of an attack, we can argue that by combining the practical methods for securing the cloud described here into a cohesive security architecture, cloud providers and users can achieve approaches consistent with solution C.

Specifically, by arranging our cloud methods into broad equivalence classes, motivated by the original Orange Book security criteria,[5] a hierarchy emerges. Readers can create classes as they see fit for their environment, but here's one possible approach:

- *Cloud security solution A implementation (below the state of the practice)*—utilize a public, private, or hybrid cloud with no additional protections beyond perimeters and gateways.
- *Cloud security solution B implementation (above the state of the practice, but below target)*—utilize a public, private, or hybrid cloud with full integration of perimeter protections into the cloud infrastructure, encryption of stored data, and session containers for client access to critical data and applications.
- *Cloud security solution C implementation (above target, but below perfect)*—utilize a public, private, or hybrid cloud with full integration of perimeter protections into the cloud infrastructure, encryption of stored data, session containers for client access to critical data and applications, proxy access capabilities for authentication and monitoring, and dynamic runtime protection for all cloud objects based on a threat assessment.

For organizations that currently protect their data using an enterprise perimeter with presumed trust for insiders, the cloud security solution C approach would provide a higher degree of protection for their data in public, private, or hybrid clouds because it addresses insider threats and APTs without dependence on any perimeter. In this scenario, the migration of data, applications, and systems to the cloud, even in critical environments such as financial services, should be immediately adopted to promote both IT and cybersecurity objectives.

## References

1. "Cloud Computing in the Finance Industry," panel discussion, New York Technology Council, 27 Mar. 2014; https://www.nytech.org/events/Cloud_Finance.
2. E. Amoroso, "From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud," *IEEE Security and Privacy*, vol. 11, no. 1, 2013, pp. 23–31.
3. Gartner, "IT Glossary," 2013; www.gartner.com/it-glossary/cloud-access-security-brokers-casbs.
4. US Dept. of Defense, "National Industrial Security Program Operating Manual," DOD 5220.22-M, Nat'l Industrial Security Program, 28 Feb. 2006.
5. US Dept. of Defense, "Trusted Computer System Evaluation Criteria (TCSEC)," DOD 5200.28-STD (popularly known as the Orange Book), 15 Aug. 1983 (updated 21 Mar. 1988).

**EDWARD G. AMOROSO** *is the senior vice president and chief security officer at AT&T, where his primary responsibilities lie in the real-time protection of AT&T's vast enterprise, network, and computing infrastructure, including its emerging Long-Term Evolution (LTE) mobile network and cloud services. He also manages AT&T's intellectual property and patent development group. Amoroso has a PhD in computer science from the Stevens Institute of Technology, where he also serves as an adjunct professor of computer science. He was awarded the AT&T Labs Technology Medal and is an AT&T fellow. Contact him at eamoroso@att.com.*