# Defending the Cloud:
# Considerations for Enterprise Migration


## Abstract

Enterprise migration to the cloud is now entering a period of dramatic growth. During this shift to cloud infrastructure, enterprises must consider and plan for how they will protect their sensitive corporate and personnel information before, during, and after this operational transformation. This paper describes the challenge of defending an enterprise - during and after- its migration to the cloud. The challenge is two-fold: First, how to maintain a defensive posture during the actual enterprise migration and Second, how to deal with the inherent challenges of migrating/updating the personnel skills and expertise needed to defend the enterprise in the cloud.


## Introduction

Over the past five years large enterprises have started to shift their local network infrastructure toward cloud based infrastructure. While security concerns remain paramount to this migration, the cloud offers a host of advantages over traditional large and wide area networks in cost, speed, redundancy, and efficiency. The costs associated with defending the cloud architecture will far outweigh the costs of supporting existing systems and architecture. Cost savings in licensing alone will be worth the risk of abandoning client-server architecture. Additionally, enterprises of all sizes can see large reductions in IT labor costs by exploiting efficiencies and leveraging resources offered by migrating to the web-based cloud model. As the pace to migrating to the cloud continues to accelerate, the threat of penetration and compromise continues to grow, both in complexity and lethality as services are federated and consolidated. Malware and sophisticated penetration software can compromise systems and gain vast amounts of information rapidly. Network security specialist will need to develop new and more dynamic defense techniques to counter the complex threat environment.

This paper describes the challenge of defending an enterprise - during and after- its migration to the cloud. The challenge is two-fold: First, how to maintain a defensive posture during the actual enterprise migration and Second, how to deal with the inherent challenges of migrating/updating the personnel skills and expertise needed to defend the enterprise in the cloud.

## Defending the Cloud Requires a New Skill set for Traditional Local IT Staff

Cloud services shift the defensive effort from one focused primarily on network and operating systems to web technology and application development. Most network specialists are networking experts who have made the shift to security after working in an enterprise network environment. Shifting to web-based services will be a challenge for most.

Timing the change and migration of the IT team's skills can be a challenge. The best strategy to migrate skills of the current local IT team is to do so just prior to or as near as services are moved to

the cloud. While core networking skills will remain invaluable, companies will need to augment the team with developers with middleware and integration experience. New roles in the cloud call for a need to have team members that can institute secure coding standards and evaluate partner and federated partner integrations and adaptive program interfaces (APIs). Additionally, the new team must have the ability to write custom code for the cloud services supporting interconnectivity/interoperability between the new systems and legacy systems.

## Security Teams will Need to Shift from Event Based Analysis to Threat Based Analysis

Before, during , and after the migration, security teams will need to shift from event based analysis (analyzing prior attacks to define trends and threat vectors) to a dynamic threat model (using open-source intelligence data to identify trends and zero day exploits before they are used by attackers). To change the model, leaders will have to change the culture of the team and evangelize the benefits of the new model.

Client-server networks are easily exploited using malware and unsophisticated social engineering. Users visiting social networking sites can infect client machines or easily download unauthenticated applications. Event based analysis focuses on malware behavior on client machines and the mechanisms the code uses to propagate.

Web based cloud services are susceptible to a different set of vulnerabilities; cloud services require sophisticated and complex attack methods to compromise. Companies will need to train security analysts and upgrade their skillsets from the current model to threat based analysis, focusing on applications, middleware, dependencies, and identity solutions to identify vulnerabilities. Analysts will now need to understand how applications communicate and interact with the operating system, management memory, and secure coding practices rather than more traditional networking and TCP/IP.

## Federation and Affiliation Increase the Risk of System-Wide Compromise

Services will no longer be sequestered and stand alone; federations of applications will be aggregated and users will be authenticated via identity management solutions for single-sign-on access. Much like today's systems, users will sign on to the domain and identity software will manage credentialing across the cloud. Users will be able to move across the various applications with one login.

Federating services represents a significant risk to the enterprise should a compromise occur. Penetrations will not be isolated to a single service, but could potentially span a number of services. Should an identity solution be compromised, an attacker would have unrestricted access to the entire federation. Considering the risk and potential loss, companies need to vet rigorously vendors and partners to ensure their software and API's are secure, enforce strict secure coding standards, and mandate thorough testing.

Testing should include penetration testing, scanning, and code reviews before any product is placed in a production environment. Vendor agreements should spell out the development cycle and Service Level Agreements (SLAs) should specify response time should a penetration occur. Vendors

should also be aligned with the coding standards and be subject to code reviews. Secure coding standards should be enforced across the entire federation and vendors held accountable for failing to comply. Upgrades, patches, customizations, and new software should be treated equally and tested in the same fashion.

## Significant User Risk Reduced with Migration to the cloud

Cloud users will not require the same level of education and training as in a client-server network environment. Data and files can be controlled in a more efficient manner; users will not be able to walk away with terabytes of data as in the past. Devices will connect via the web and those stand-alone applications will be controlled via application dependencies. Simply put, the ability for users to compromise data is greatly reduced – if not eliminated – by moving to the cloud.

Social engineering, however, remains a credible threat. Users will need to be educated on social engineering techniques that are used by malicious actors to secure access and credentialing information. Much like the current acceptable use policies, users will need to sign privacy and confidentiality agreements, which include access controls and data security protocols.

## Device Proliferation Creates Added Dimension to Security

The cloud will offer device flexibility current networks and enterprises will not allow. Connecting to cloud applications from any device, anywhere, anytime will lead to an immense proliferation of the types and provenance of devices. Users will not need to rely on virtual network protocols, robust connection and proxy farms or separate application farms.

Supporting devices in a cloud environment will require stringent rules and protocols. Enterprise security teams and network architects will have to decide how many operating systems and device types will be supported by the enterprise; those users operating outside the enterprise device standards will be on their own for support.

Security teams will be required to build device profiles to outline all of the vulnerabilities by type. Since device vendors are outside the federation of services, security teams will be responsible for assessing risk and developing mitigation strategies for devices with known vulnerabilities. Enforcing data storage and application permissions by device will be necessary once security profiles are built.

Finally, since devices are made all over the world, the security team will need to evaluate all facets of the device. Security analysts will need to evaluate the firmware, software, operating systems, device drivers, and communications protocols for every device on the enterprise. Security teams will then have to build preferred vendor lists and educate users on the risks of unsupported device types.

## Identity Management Solutions will be the Key to Cloud Infrastructure

Identity management - controlling individual access and permissions - is a crucial key to cloud implementation success that can improve data security and productivity. The challenge with identity management in the cloud is the admixture by IT teams of existing local network architecture with new cloud architecture. That is, the current strategy during a cloud migration is to

integrate and aggregate existing identity solutions rather than build new ones. The issue with the current architecture is known vulnerabilities are now mixed with new vulnerabilities without remediation in some cases. The existing risk of the current solution remains and new risk is added with any new code or interface added to support multiple applications.

Security team will have the added responsibility to test and evaluate complete solutions and assess enterprise risk. Hasty transitions and integrations to the cloud could result in increased risk. For example, adding virtualization to an existing Active Directory Forest - which has known vulnerabilities and security flaws - to support a legacy application could introduce significant risk to the entire cloud.

To combat these challenges, IT teams would be wise to develop and test an interim solution to support legacy architecture and applications prior to exposing the organization to risk. Testing and evaluation of the solution should include known vulnerabilities and gaps to expose potential weaknesses in the cloud communication protocols. Testing should include a rollback plan and go/no-go decision points for production systems.

## Summary

While the benefits a cloud migration far exceed the associated costs, the movement to the cloud is not without its challenges. Security teams will have a steep learning curve to adopt new techniques, procedures, and tactics to counter the threat of malicious actors. Situational awareness and visualization tools must be enhanced to support evaluating software and code instead of merely monitoring network traffic. Solutions will be more complex and require more thorough testing and evaluation before implementation and adoption. Depending on the enterprise, this could be a considerable challenge, especially in growth industries where time to market could cost the enterprise revenue.

While users should become less of a security threat through identity management, affiliation, and federation, security teams will need to shift their focus to device management. The proliferation of the number, type, and origination of devices will only increase as the cloud continues to increase the mobility of today's employees. Although role-based control may get easier, the threats of social engineering and industrial espionage remain; employers need to focus on educating users on those topics.

Security administration will become more complex and require different analytical skills and techniques. Analysts and forensic teams will undergo significant change in methodology to support the cloud. Restructuring the security team should be a continuous process as the threat changes. Redesigning the security team will require constant attention as technology becomes more integrated and connected.