sumologic

A Sumo Logic White Paper

# The New Mindset for Building Secure Services in the Cloud

By Joan Pepin, VP Security & CISO at Sumo Logic

Cloud computing is reshaping not only the technology landscape, but the very way companies think about and execute their innovation process and practices to enable faster, differentiated and personalized customer experiences and services.

And the path to operating in the cloud securely and confidently requires a new set of rules and a different way of thinking.

No doubt this shift is gaining in acceptance, but we still find pockets of unnecessary pushback and outright fearfulness for venturing into unchartered cloud "waters" when the required mindset shift is absent or slow to take shape.

In this white paper, Joan Pepin – a recognized security expert in cloud computing – discusses 10 best practices to accelerate the mindset shift and enable practitioners to securely leverage the cloud and capitalize on this market disruption with confidence and clarity.

This paper does not attempt to cover every best practice one should employ in order to build secure and scalable systems in the cloud, but discusses some of the foundational design principles which will help provide guidance in your thinking as you design such systems.

## 1. Different Rules, Different Logic

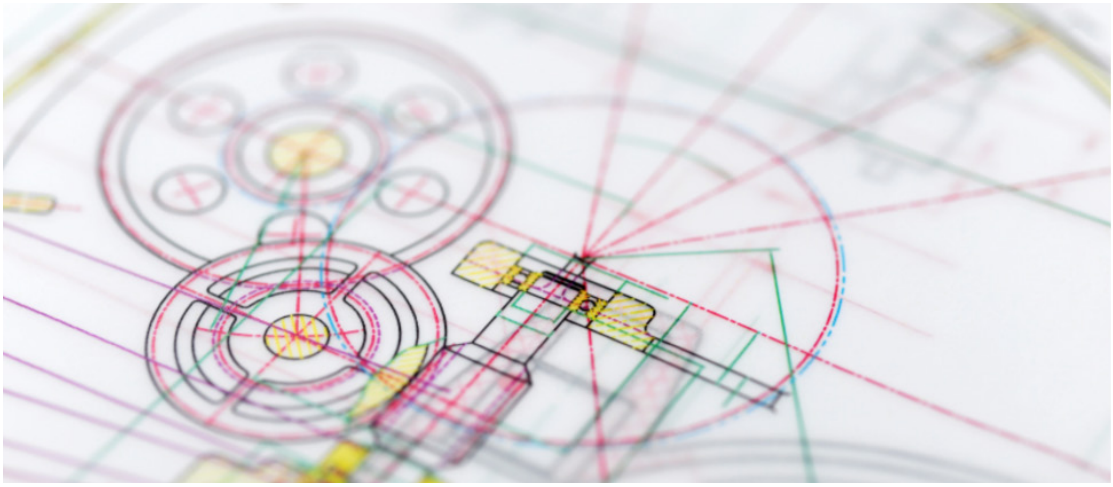
Operationally, security organizations need to change their thinking and processes from traditional data center-centric (what I'm now calling "flat Earth") models to new, more statistical models. For example, we exchange hands-on control over physical hardware with odds over a population of hardware. From a systems administration perspective, we exchange scripts and manual capacity planning and scaling with API calls, triggers, feedback loops, and the automatic provisioning and de-provisioning of spot-bid compute resources. And, of course, from a security perspective, we face the challenge of a world that is not under our complete physical control.

While many veteran security professionals react to the cloud with caution, there are two realities:

- The cloud is here to stay; and
- It gives us an extremely powerful new set of tools for securing this environment.

When properly leveraged, cloud-based IaaS offers availability benefits beyond what many enterprises - large and small - can easily achieve on their own. Additionally, by employing a combination of automation, integration with an IaaS provider's APIs, and thoughtful system design, you can achieve a level of security that is actually higher than most legacy in-house services currently provide. With a few well-placed API calls you can have an army of hardened, patched, encrypted, scalable, and disposable virtual machine resources at your disposal, ready to do your bidding, securely deliver your results and then self-destruct before returning from whence they came. Of course, doing this and leveraging it properly requires a different thought process than we may be accustomed to, but the reward can be well worth the effort and shift in thinking.

## 2. Design. Design, Design



Creating the right security infrastructure that aligns to business risk is traditionally a matter of strict design principles and security policies distributed across a number of departments and areas of expertise. In a system designed for the cloud you have the tools to design, implement, and refine your policies, controls, and enforcement in a streamlined and centralized fashion. The tools exist to add security at the network layer (with security groups, access management, host-level firewalls, and VPNs), at the O/S layer, (with encrypted storage, strict privilege separation, and ruthlessly hardened systems), at the application layer (with the latest updates and thoroughly enforced policies) as part of your design and development cycle, rather than as part of ongoing operational maintenance.

Deploying services in the cloud gives you the freedom to design your network and security measures from the ground up, while implementing your secure designs in code, which is not subject to the same concerns you have in a physical data center or hosting facility. Legacy compromises of rogue crossover cables and obsolete equipment are laid to rest by APIs, such as those from Amazon Web Services, which allow you to design an entire network exactly the way you would like it to be implemented, complete with firewall rules, the latest security updates, and value-added IaaS tools such as identity and access management. The ability to resize your storage, memory, bandwidth and compute dynamically or

through your release-cycle to suit new designs and business needs removes the final layer of hardware management and multi-factor capacity planning inherent in large home-grown or hosted virtual machine deployments. When you need to recreate that network, or redeploy or rescale your infrastructure, there is no need to worry about legacy issues that would prevent you from making the types of sweeping changes that look so good on paper. Your paper easily becomes reality, with no need to move cables, rename hosts, or worry about maximizing the ROI on a piece of equipment that is no longer relevant

> When properly leveraged, cloud-based IaaS offers availability benefits beyond what many enterprises - large and small - can easily achieve on their own.

Cloud tools allow you to take security management to a new level by enabling you to fully automate your controls and tests. By moving systems administrators away from distributed scripts and into the hands of production-ready code–which can be rigorously reviewed, tested, and updated along with the rest of your service–you can achieve a scale and ease of management unthinkable in traditional paradigms.

In this new paradigm, you are free to design your systems with all of the security controls you could ever want but were probably never able to achieve in a flat-Earth, brick-and-mortar data-center or hosting facility. Since your entire infrastructure is transitory in nature, the best approach is to automate your deployments leveraging the cloud-based tools that allow you to make the installation, baselining, and management of things like file-integrity-checkers trivial, so that all of your virtual machines can have file-integrity software and baselines built in from the ground up. By using APIs to programmatically assign virtual machines to role-based security groups that are well-designed in advance you can scale your network to massive sizes without ever having to worry about firewall rule ordering, optimization or audit as part of your operational cycle.

Some IaaS providers allow you to build your own virtual private network of virtual machines according to your own network topology. This affords some advantages in terms of leveraging predictable host-names and allows you to employ an network-layer protections such as Intrusion Prevention Sensors (IPS) or Web Application Firewalls (WAF) that are available as virtual machine appliances or that can run as software on your platform. These additional layers of protection and convenience allow you to leverage some of the successful technologies that were designed within the data-center paradigm and still incorporate these controls into your SDLC and minimize operational cost.

With the kind of programmatic flexibility brought to bear by cloud APIs you have the ability to engineer a system with security built in at every level, and the scaling and management of those controls has never been easier.

As a result of this transformational new paradigm we have to focus on the design of our security systems and leverage the reliability and automation that cloud providers afford us to operate securely in this new environment.

### 3. Defense in Depth. Everything. All the Time.

A cloud-based service needs to be thought about holistically, as an integrated system. This system has layers, components, interfaces and interactions, which are all under your control and programmatically scaled to wherever you set the dial. Each of these factors needs to be carefully considered from a security perspective that flows from a central design.

Data needs to be considered in its three elemental forms: at rest, in motion, and in use. You also need to be able implement and monitor access control across all of the various virtual machines and applications

(monitoring applications, third-party applications, development resources). Interfaces and APIs need to be scrubbed as clean as possible and limited to authenticated users and systems. Keys must be stored away from locks… All of the traditional rules still apply, but can be executed in new and efficient ways.

There are a lot of details, but at the heart of it is the system, with inputs, outputs, storage, memory, and transport. Each of those must be thought of on its own, and in combination with the other components it interacts with. It is both that simple and that complicated.

Cloud IaaS providers and their partners offer a multitude of mature tools to assist with things like key-management, user management, Access/Authentication/Audit, load-balancing, caching, messaging, volume management, and much more. Leveraging these tools and interfaces can drastically reduce the engineering effort required to implement and manage your security controls.

If you properly leverage your design and automation tools, your security becomes fractal, embedded in every layer of your system as it scales and evolves.

For example, you can automatically deploy host-level firewalls, host intrusion detection systems (HIDS), and file integrity monitoring (FIM) tools to all of your servers, configured at boot-time for that server's specific function, ensuring that each service is run by the least privileged user, that only registered services are allowed to talk on registered ports, that every configuration file and binary is monitored for unauthorized changes, and that anything that falls outside of those specs generates an alert.

## 4. All Things Are Possible With Automation

Thinking of your entire infrastructure as part of your code-base changes the game in terms of what you are able to achieve. There is no longer a gap or disconnect between the operational physical layer and the software that runs on top of it. By simply changing your thinking, machine and network failures are now simply exceptions to be caught and handled by your system - automatically, unmanned. New boxes can brought online in real-time to replace or reinforce your existing fleet, new capacity can be bid on and purchased, and your infrastructure can now evolve and support your system because it is part of the system.

From a security perspective this coupling enables you to use your infrastructure to adapt automatically. For instance, a service registry can be kept which keeps the IP addresses and ports of all of the registered services in your system and your code can use your cloud provider's APIs to restrict network communication to only the IP addresses and ports which are required by the system to function. SSL/TLS services can generate new key pairs and shared secrets and securely store them on encrypted volumes every time you deploy your service. Host firewalls, host IDS, and integrity checkers can be configured based on the tags you assign to each virtual instance. All of these measures can be unit-tested and QA'd as part of your Secure Development Life Cycle (SDLC), allowing you to rapidly develop enhancements in pace with your product.

You can easily test and do rapid prototyping of security architectures using your cloud provider's management console, and then implement fully-automated, API-driven deployment methods.

### 5. Less is More

Simplicity leads to security. Simplicity of design, of interfaces, and of data-flow all help lead to a secure and scalable system.

### 6. Do the Right Thing

Keeping APIs and other interfaces simple, clean and minimal, designing in-code-reuse and centralizing configuration information will help keep your attack surface to a minimum as well as allow for easier troubleshooting and faster turnaround on any security-related items that need to be fixed. Build solid primitives, connect them in secure ways.

Every system has I/O, storage, memory and network underneath it. You build your software components on top of that stack. So think about every place that information is exchanged, transferred, or transformed in your system and make sure you are doing the right thing there:

- If this is input; sanitize it.
- If you are writing to storage or network; encrypt it.
- If it is output you are feeding back to your customer or another component; sanitize that too.
- Don't trust client-side verification; enforce everything at every layer.

### 7. Leave No Trace

You can safely use these giant blocks of anonymous pay-by-the-hour compute by leaving a minimal footprint, minimizing your attack surfaces and eliminating the chances that you'll accidentally leave sensitive data exposed.

In a cloud infrastructure, it is easy to have a zero scannable network footprint, while still maintaining robust remote access for your DevOps team. The only footprint your service needs to leave on the Internet is your service's login screen, and you can easily whitelist access -- either to the screen itself or limit the ability of certain users to log in from certain addresses.

> "Abandoning your legacy infrastructure and centralizing your security design and enforcement within your code-base will ultimately allow for greater security at lower human and capital cost.

If your front-end web application needs to accept connections from anyone in the world so be it. But it's more likely your load balancer does, in which case your web application front-ends should only talk to the external load-balancers -- hence nothing can connect directly to your infrastructure from the Internet. As part of your IaaS software design, you know what needs to talk to what and on what port and under what circumstances, and you should only allow that. Everything else is bit-bucketed and alerted on. In a software-driven cloud architecture, there is no longer any excuse for doing it any other way.

## 8. Encrypt It All

At rest, in motion, and in use; any data that is ephemeral can be kept on encrypted ephemeral storage and the keys can simply be kept in memory. When the instance dies, the key dies with it.

Longer-lived data should be stored away from the keys that secure it. If the data is particularly sensitive, in addition to keeping it encrypted, you can program your system to securely wipe the data at the end of its retention period using any of the various best practice protocols for secure data deletion before spinning down the disk and giving it back to the pool. Tools are readily available for installation on your virtual machines, which make this secure data deletion simple and easily automated.

Ephemeral -- anything shorted lived or transitory -- is a powerful concept once you embrace it. Secure and encrypt everything you care about, the rest of your virtual machine fleet can be rebooted, terminated, or sacrificed.

## 9. Continuous Compliance

Continuous compliance goes beyond passing annual audits. Controls required under key regulations including PCI DSS, HIPAA-HITECH, SSAE 16 SOC 2 Type 2, ISO 27001, CSA Star, and NIST 800-53 should not be treat as one-time implementation. Conversely, we must ensure that the controls are in place and operate effectively at all times and if an exception occurs it must be identified real-time and remediated per incident response policy. Furthermore, fully implemented continuous compliance means monitoring and responding in a timely fashion to changes given the relevant compliance frameworks. Compliance ceases to be 'check-box compliance' and equals security only when controls are in place and operate effectively at all times, not merely at the time of an audit.

Areas of continuous compliance:

1. Asset inventory - AWS provides tools that make asset management in the cloud transparent and accurate. Knowing what production assets are available at all times despite of dynamic nature of the cloud allows adequate protection of all assets.
2. Change management - Running FIM on all servers ensures that all changes follow defined change management process with all required testing and approvals, are implemented only by authorized individuals and only during the deployment window.
3. Access management - Monitoring user accounts across key production systems ensures that only authorized individuals have access, provisioning follows approval process and de-provisioning is timely.
4. Vulnerability management - Internal and external scans, code reviews, and penetration testing are imperative to ensure that all vulnerabilities are identified, evaluated, and addressed according to incident response policy.
5. Logging key security events - Logging key security events across production systems allows us to identify and respond to risks timely.

Benefits of continuous compliance:

1. Ease of audit evidence gathering and report generation
2. Resource optimizations; controls and supporting evidence overlaps across various compliance frameworks
3. Real time identification of exceptions and remediation
4. Agile reaction to changes in regulatory standards
5. Continuous improvement

> "Cloud computing is reshaping not only the technology landscape, but the very way companies think about and execute their innovation process and practices to enable faster, differentiated and personalized customer experiences and services.

## 10. It's Easier Than You Think

Abandoning your legacy infrastructure and centralizing your security design and enforcement within your code-base will ultimately allow for greater security at lower human and capital cost.

## About the Author

Joan brings over 17 years of experience to her role as Sumo Logic's VP of Security and CISO. Her career has spanned a wide variety of industries such as healthcare, manufacturing, defense, ISPs and MSSPs. Her experience includes technical, operational, and management aspects of security, allowing her to bring highly technical research expertise to her current interests in security policy management, marketing, strategy and thought leadership. Prior to Sumo Logic, Joan spent nine years with the Guardent/ Verisign/ Secureworks organization where she invented several core technologies and established key initiatives around policy management, security metrics and incident response. She holds a patent for developing methodology to assess whether a communication contains an attack.



305 Main Street
Redwood City, CA 94063
www.sumologic.com