

cloud
accelerators

can you have
your cloud and
be secure too?

you can



“We host security services in a private cloud environment. You get cloud elasticity and agility, without the risks of public cloud.”

Jonathan Freeman
Founder, Mycroft Inc.



agility
made possible™



move applications from one data center to another with no reconfiguration.

About Mycroft Inc.

- Founded in 1987
- Provides application security and identity management services for enterprises and managed service providers
- Headquarters in St. Louis and NYC with service centers in the UK, Ireland and India
- 200+ employees, with a wide array for Fortune 500 and mid-sized enterprise customers

For more information, visit mycroftinc.com



Jonathan Freeman
Founder & Chief Information Officer

Career Highlights

- Founded Mycroft Inc. in 1987
- Pioneer in the development & deployment of Security as a Service & enterprise private cloud solutions
- Background in advanced computing & distributed architectures, designing large-scale, multi-processor systems for corporations
- Personal interests: spending time with his 2 children, amateur car racing & motorcycles



Elizabeth Butwin-Mann
Chief Information Security Officer

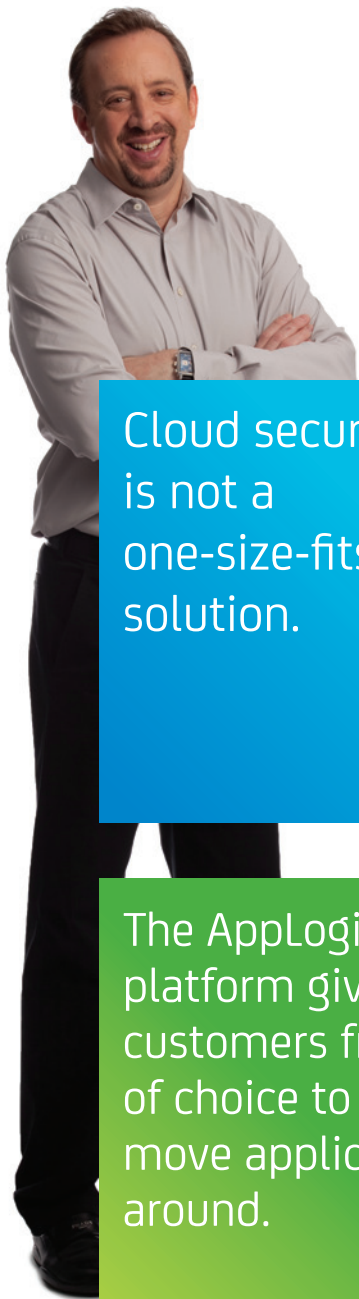
Career Highlights

- With Mycroft Inc. since 1994
- Responsible for shaping & driving the company's growth initiatives
- Previous work experience at financial services firms, implementing business-driven technology & spearheading turnaround efforts
- Personal interests: movies, art, wine & spending time in & around Manhattan with her 2 daughters

What types of cloud-based services do you offer?

Mycroft Inc. services address security concerns around identity, access control, fine-grained entitlements, logging and auditing. We host services in a private cloud environment to provide cloud-like elasticity and agility, without the risks of deploying in a public cloud. Depending on what our customers prefer, we provide a fully dedicated set of resources (at the customer's site or ours), a shared, logically-bound set of resources or a multi-tenant deployment.

Mycroft offers cloud-based services to both enterprises and managed service providers. We've also found that the cloud-based solution has opened up a new market opportunity for us, specifically the mid-size enterprise. That size organization tends to have difficulty providing all the hardware, software and implementation skills needed to provide a robust identity management solution, and yet, they're subject to the same regulatory requirements and security concerns as very large companies. We can deliver these companies a pre-built starting point and manage and operate the environment for them, exactly as their business requirements dictate.



Cloud security is not a one-size-fits-all solution.

The AppLogic platform gives our customers freedom of choice to easily move applications around.



To learn more about Mycroft Inc., visit mycroftinc.com

Who bears the responsibility for cloud security—the customer or the service provider?

I like to say that cloud is not an excuse to abandon all of your security policies. It's not an excuse to say, "It's not my responsibility anymore, it's somebody else's." At the end of the day, security is a shared responsibility between the consumer and the service providers involved. From Mycroft's perspective, I may say, "It's Mycroft's responsibility to manage the security of your environment for you." But, customers still have a responsibility to understand what policies they have set and implemented, and what requirements they have established for your business and for your relationship with Mycroft.

If there is a third-party managing the environment in which the implementation is physically hosted, then they become another party sharing the responsibility. But again, the customer is responsible for the decisions they make about the hosting environment—do they need a SAS 70 or a SSAE 16 data center? Do they need lock and key on their rack? Customers need to be savvy consumers and know what questions to ask when they are deciding upon a hosting provider. They need to understand, for instance, where the data will physically reside, whether data will co-mingle with anyone else's data and whether their identity data is at risk.

How does your cloud-based approach to security management enable you to reduce implementation costs?

We have decades of experience in identity management and application security and deep knowledge of the CA Technologies identity and access management products, which we consider best-in-class. We've deployed these security products in our Mycroft Managed Elastic Accelerated Delivery (MEAD) environment (which is built on the CA AppLogic® cloud platform) Mycroft's MEAD platform provides pre-configured templates for common security, identity and GRC use cases.

Identity management solutions work best when they are deeply integrated with other applications and business policy. This integration work can be time-consuming. Our customers are able to realize between a 30-40% savings in implementation costs from deploying any of the CA security products on top of the CA AppLogic environment. Once we figure out how to enable a given application component to communicate with another component and build it into our Mycroft MEAD model, we never have to do the manual configuration again. We don't have to spend as much time getting the products to be operational and can focus instead on defining the necessary security policies and business processes.



To learn more from cloud service providers working with CA Technologies, visit ca.com/cloudaccelerators

What issues are your customers struggling with on the journey to cloud?

We learned very early on that virtualization has a lot of merit, but it also has a lot of overhead. Our customers want to pick and choose where they want their workloads to be deployed. Some data centers may cost more to execute on, some applications may require a higher degree of security, and due to the dynamic nature of the business, many of our customers want to shift loads from data center to data center. Doing this in a traditional virtualization model involves a lot of reconfiguration, because you not only need to move the servers, but also the wires, the routers, the switches, and so on.

What the Mycroft MEAD cloud platform allows us to do is encapsulate not just the server infrastructure, but the entire physical infrastructure supporting an application and all of the necessary interconnection points. Customers essentially have an encapsulated version of an application environment that is configured once and can be deployed quickly and easily, as many times as needed. It can be moved around from one data center to another, without requiring any reconfiguration. The CA AppLogic platform is the only product we've found that allows us to do that. It gives our customers freedom of choice.

What do you tell customers who are concerned about cloud security?

We talk to our customers about the hybrid approach to cloud computing. There are functions customers can put in the public cloud today that don't violate any security protocols or procedures—things like development and testing environments. There are solutions that allow customers to marry the ability to offload some of their capacity to public, private or managed service clouds. I think that's the real benefit right now—it's not a one-size-fits-all solution.

The key to being able to deploy successfully is to have an environment that allows you to deploy in any cloud architecture (public, private in a managed service environment or private cloud in your environment) without having to manually reconfigure the application.