CASE STUDY

Federal integrator helps agencies secure identities

Akima, LLC, get its military, intelligence and federal civilian agency clients on a more proactive IT security stance

Key Facts

Company
Akima, LLC

Industry
IT Services for Federal Agencies

Country
United States

Employees
6,000

Website
www.akima.com

Challenges

- Migrating efficiently and securely to the cloud
- Securing user identities
- Proper delegation of user identities
- Control and manage administrators

Results

- Secured user identities
- Reduced discovery of breaches from months to days or less
- A much more proactive security stance
- Smooth transition to the cloud

How do you help an organization as far-ranging and multifaceted as a federal agency secure its user identities? it's a particularly big job when you add other unique challenges, such as a huge geography that includes 50 states and international offices; an ever changing list of employees and constituents; supporting and protecting an infrastructure that enables all business functions; and finally ensuring that your strategies meet all regulatory compliance.

Akima, LLC, has been taking on these challenges for decades. The federal contractor, headquartered in metro DC, is a subsidiary of Anchorage, Alaska-based NANA Development Corporation, delivers a host of services to U.S. Department of Defense, the intelligence community, and federal civilian agency customers across the United States and in 12 countries.

Situation: Reactive vs Proactive

Providing secure environments is always important but with clients like that, delivering rock-solid IAM solutions takes on even more significance. Security used to be all about the perimeter, not anymore.

"In today's world, it's critical to help secure user identities," said John Fair, director of business development at Akima. "Cyberattacks often ride in on user identity. And with social media, [a person has] user identities that are all over the world. Everything is on the web, including information such as your birthday to what you ate for dinner last night."

ONE IDENTITY™

> **"It used to be months before an issue was discovered, now it's within days or sooner. That's huge for our type of clients."**
>
> *John Fair, Akima, LLC*

With social engineering techniques and a less-than-vigilant user, it's not a huge leap to gain access to a network and parlay access from there to access critical resources.

Often, the biggest challenge is a lack of awareness that these homegrown risks pose, and therefore many clients are unprepared and their ability to act quickly to identify and address potential and active issues is lacking.

"They don't realize how vulnerable they are,' Fair said. "And they are in a more of reactive stance instead of proactive one. So, by the time they realize that they have been breached, it's too late."

To avoid a delay in responding – and even prevent a breach outright – is why identity governance has become so important. But many clients don't worry about it until they experience the destruction a bad actor can leave in their wake.

Another common challenge that Akima's federal clients face is a mandated move to the cloud. Often, they aren't prepared or are confident of how to truly secure the jump. Plus, they may have issues with their current on-premises identity infrastructure, which are often run on legacy technology. So when they make the move to the cloud, they compound their issues.

"With the One Identity products, we can help them with that transition to get a very secure environment," Fair said.

Solution: Enhance Identity Governance

A key benefit that Akima's clients get with One Identity solutions is a more proactive security stance. With the ability to implement solid identity governance practices, they are less susceptible from identity-born breach attempts and if a breach were to occur, the damage would be limited by capabilities, such as segmentation of access rights by role, context-aware security models, password vaulting and session-controlled access.

"One Identity products reduce the amount of time it takes for our clients to realize that something is happening on their network," Fair said. "It used to be months before an issue was discovered, now it's within days or sooner. That's huge for our type of clients."

On top of that, Akima federal clients also get better control over administrative-rights creep. "We'd find that administrators were out of control and what they [had access to as part of their daily job]," Fair said.

Traditionally, administrators would have blanket access to everything from printer administration to mission-critical resources. Privileged credentials were often shared with multiple people which provided little accountability. But with One Identity privileged access management solutions as part of the governance infrastructure, admins can be managed on a more finite level with permissions granted such that they can access only the resources they need to do their job.

"Before One Identity solutions were implemented, there wasn't a really good delegation model available for a lot of our clients."

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats.

For more information, visit **www.oneidentity.com**

CaseStudy-Akima-US-RS-32652

ONE IDENTITY™