EBOOK

CALL SIGN: PAM

The State of Privileged Access Management

By: James Hauswirth
Practice Lead, PAM
GuidePoint Security

GUIDEPOINT
SECURITY

IF YOU ASK ME, PAM IS A BIT LIKE FLYING A HELICOPTER

For 16 years of my life, I served in the military—both as a national guardsman and a Black Hawk pilot. One of the most important things I learned during that time was that when you're making a decision as an aviator—especially a safety decision—communication is the most critical piece of the puzzle, followed closely by collaboration and situational awareness. Through the training I received, I learned to look at events around me from every angle and to make sure that, when necessary, I could step in to mediate hard conversations. Even in the face of intense challenges, we were taught to maintain a calm, cool, and collected demeanor, absorbing as much information as possible without letting our emotions cloud our insight.

YOU HAVE TO HAVE EMPATHY

When I think about PAM (Privileged Access Management) deployments, I see an undeniable parallel between my time as an aviator and what I do in my day-to-day as the PAM practice lead at GuidePoint. PAM is a holistic security posture that must be looked at from every angle.

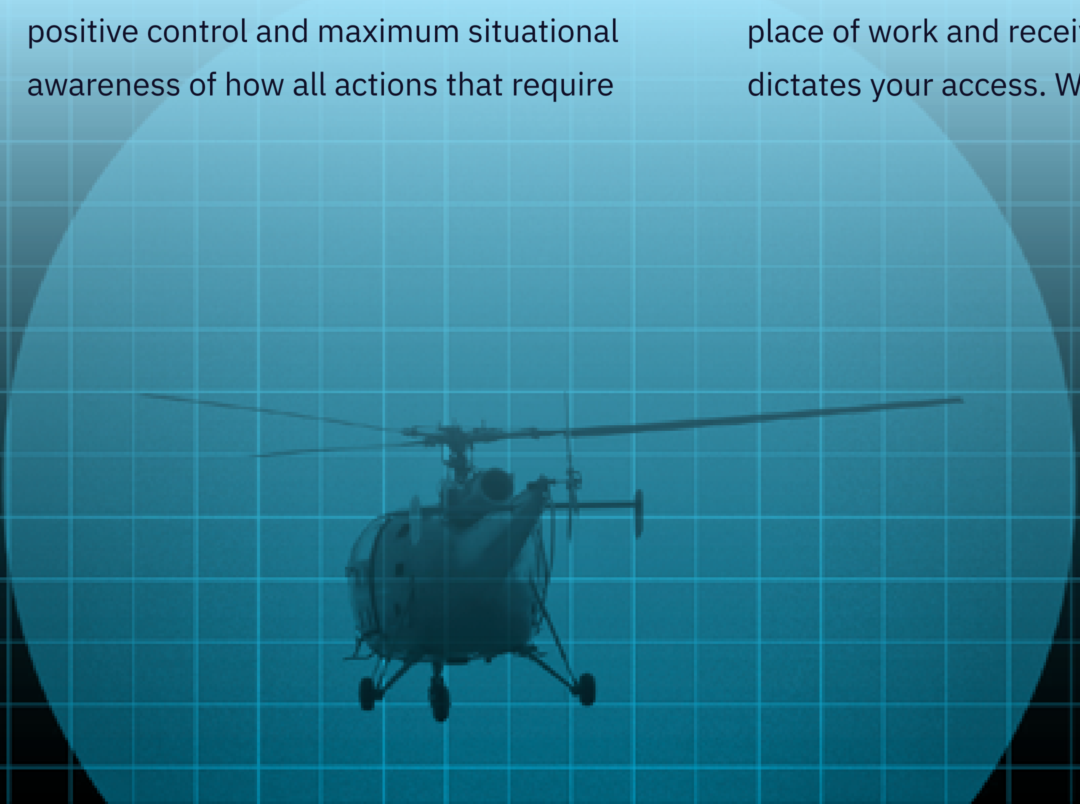
You must consider the day-to-day effect PAM has on your end users and your engineers. You have to socialize it properly with your workforce and be ready to handle the fallout when something inevitably goes awry. When things become contentious, I know how to keep my head screwed on straight and how to find the most effectual course of action—focusing on the success of the endeavor as opposed to the success of a particular individual. Because that's what security is about--protecting the organization as a whole.

SO, WHAT THE FLYING HECK IS PAM, ANYWAY?

Privileged Access Management is a security solution that safeguards organizations against cyber threats by monitoring and preventing unauthorized privileged access to critical resources. It uses people, process, and technology to provide visibility into who uses privileged accounts and the actions they take with those accounts while logged in. By limiting the number of users with access to administrative functions and providing additional layers of protection, PAM can help mitigate data breaches by threat actors.

Broadly speaking, PAM facilitates positive control and maximum situational awareness of how all actions that require privilege are governed in your environment. This can be anything from installing a new application to being a domain admin and standing up whole organizational units. Positive control allows you to be proactive about privilege management and respond quickly when issues arise—controlling the blast radius if and when a security event does occur.

While on the topic, let’s define and contextualize “positive control”—what does that mean? For starters, it is the opposite of “passive control.” Let’s use an analogy: “Positive control” is like arriving at your place of work and receiving a badge that dictates your access. When you leave at



the end of the day, you turn that badge in again. Juxtapose that against “passive control,” where you receive that same badge on the day you’re hired, and then we all hope it doesn’t get stolen, lost, etc.

Finally, PAM is one of the best ways that you can be empathetic to and supportive of the people operating in all verticals across your company. These folks are entirely responsible for keeping the lights on across the entire organization—at a highly technical and stressful level. These are the same folks who will be in charge of PAM implementation and maintain the integrity of the privilege assignments. When things go wrong, these are the people who get up in the middle of the night, step away from their kid’s soccer game, and go back to the hotel room during a family vacation to handle it. By implementing PAM correctly, we can ensure that these folks get to sleep through the night, enjoy that family vacation, watch that soccer game, and have a better work/life balance.

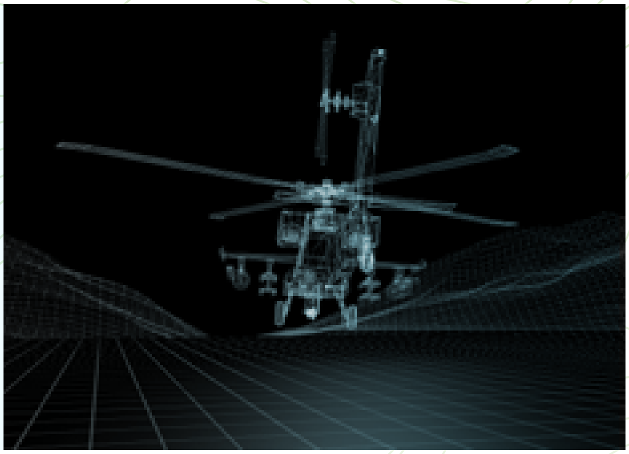
PAM IS OF THE GREATEST IMPACTORS FROM A BEHAVIORAL CHANGE PERSPECTIVE

PREFLIGHT CHECKLIST:

WHY IS PAM SO IMPORTANT?

In recent years, PAM has gone from a "nice-to-have" to a "must-have." Cyber insurance firms have begun seriously cracking down on companies that don't have it deployed across their systems. Instead of simply checking a box, organizations are now required to prove to these insurers what they have done to make privilege access management a reality. And these checks have become extremely granular: How are you maintaining positive control and situational awareness around privilege throughout your entire environment? What does your logging scheme look like? Do you have a PAM platform? Are you using credential tiering in your environment? How often are you cycling passwords within your environment? Etc. Not to mention that, without PAM, insurance premiums skyrocket.

So why the need for proof? No matter how many tools you have in an environment, human beings will always be your weakest link. PAM ensures that users have only the access they need to do their jobs, with no extra bells or whistles. Data breaches most often target admin-level accounts—accounts that always have the access necessary to exfil sensitive data or enact system changes. By providing the situational awareness needed to see what accounts are making changes when they are making the changes, PAM lets your security team shut down the access of and to a compromised account.

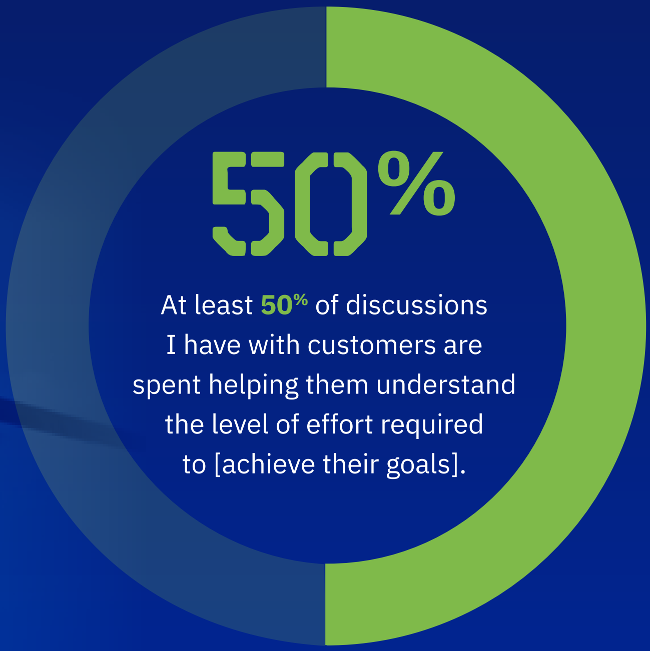


Anytime you have an environment where the HUMAN and PRIVILEGE are ONE AND THE SAME—and privilege is permissive—you lack the ability to effectively lock that down in a quick manner in response to anything. And you also lack a significant level of situational awareness around how privilege is being facilitated.

PAM HITS SOME TURBULENCE: PROBLEMS IN ADOPTION

Changes in the security landscape—like this new need to prove every fact of PAM in an organization to insurers—have drawbacks of their own. One of the major issues folks are having with deployment is that they are forced to adopt PAM in shorter timeframes than they would like or is wise. This becomes a catch-22 for many companies, as an installation of PAM that doesn't create meaningful positive change is also a mark against you by insurance agents. So, many organizations find themselves scrambling to implement PAM quickly and efficiently—something that is much easier said than done.

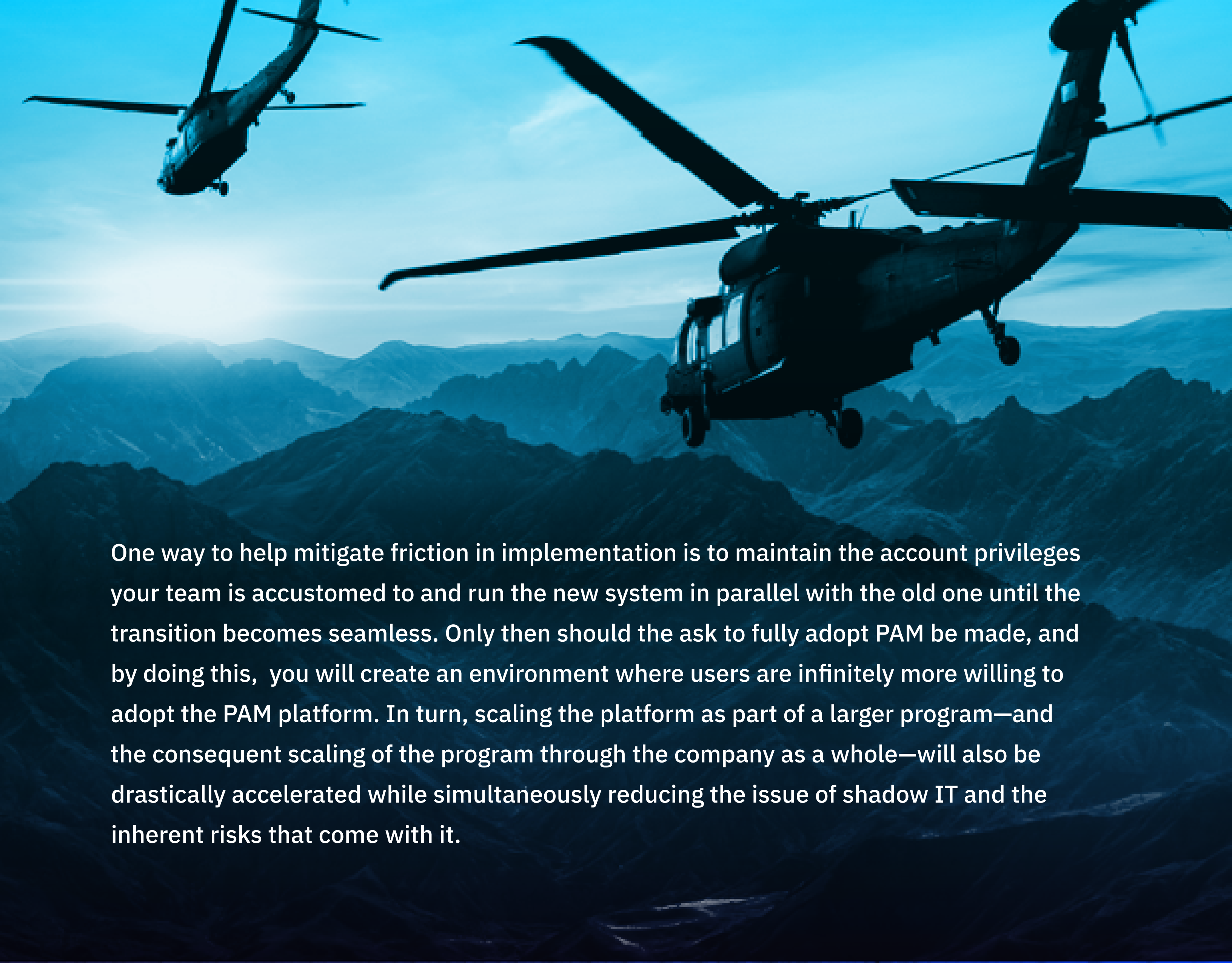
It's imperative to have realistic expectations about what your organization can accomplish during a set period of time. Too often, companies underestimate the level of effort required to effectively set up PAM and bite off much more than they can chew during the initial roadmap. To this point, a "slow-is-smooth, smooth-is-fast" approach is the most effective in these situations. Taking the time to train your teams and making sure you understand how domain admin accounts are being used—or if they're being leveraged as service accounts—is a step that shouldn't be glossed over or ignored.



At least **50%** of discussions I have with customers are spent helping them understand the level of effort required to [achieve their goals].

The pursuit of a quick and effective implementation calls back to something I talked about earlier in this piece: you must have empathy when adopting PAM. We've established that the folks implementing security changes already have high-pressure/high-impact jobs. So understanding how to make the switch to PAM easier on them is imperative for a successful deployment. Even if you remove all the security controls, just functionally moving your infrastructure from an on-prem data center posture into the cloud is a complex endeavor; it takes an immense amount of work. Mainly because this work isn't just "set-it and forget-it." It is a continuous effort that must be scaled out over months, watching the program mature and tweaking things where they need to be changed. Without empathy (i.e., establishing a strong on-ramp for your users, making sure the team feels like they have a voice in the program's construction, a stake in its success, and a hand in configuration), you don't stand a chance.

Another piece of the implementation that is positively influenced by an empathetic approach is the team's trust in the process. By doing your due diligence during onboarding to ensure that your team is invested, engaged, and has visibility into the work being done, the ask that they trust the vendor-side engineering team to connect all the necessary pieces, match passwords, secrets, and account privileges is less daunting. An engaged team is also more likely to provide immediate feedback when something goes wrong, which allows fixes to be put into place before reaching a point of catastrophic failure.



One way to help mitigate friction in implementation is to maintain the account privileges your team is accustomed to and run the new system in parallel with the old one until the transition becomes seamless. Only then should the ask to fully adopt PAM be made, and by doing this, you will create an environment where users are infinitely more willing to adopt the PAM platform. In turn, scaling the platform as part of a larger program—and the consequent scaling of the program through the company as a whole—will also be drastically accelerated while simultaneously reducing the issue of shadow IT and the inherent risks that come with it.

In my experience, the fastest way to botch a PAM deployment is to not have **EMPATHY FOR THE PEOPLE YOU'RE ASKING TO ADOPT IT** —and frankly, that goes for any other security discipline too.

PAM: CLEARED FOR LANDING

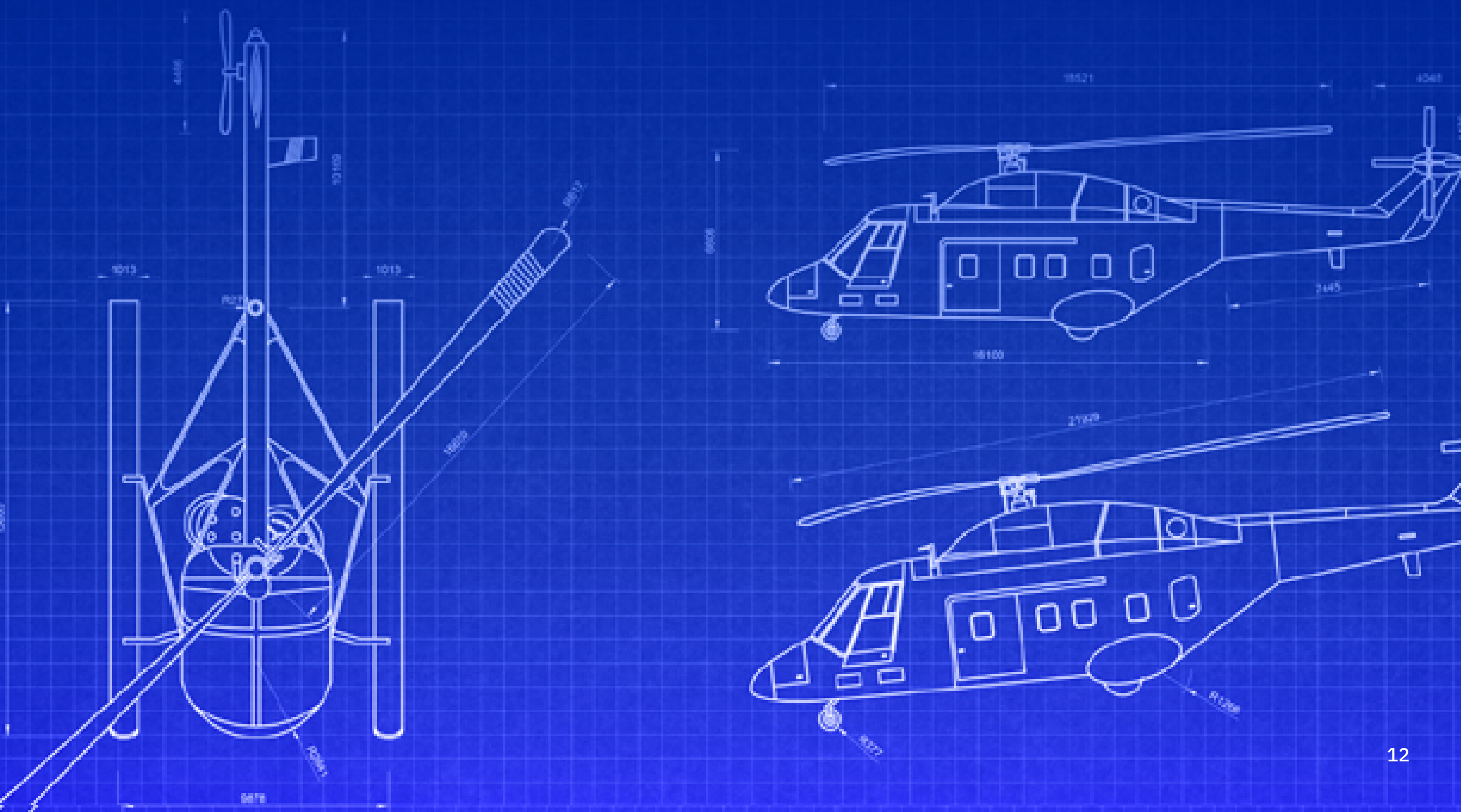
At this point, it is no longer “if” you’re going to adopt PAM but “when.” The most efficient thing you can do as a security leader to ensure the least risk of disruption is to be involved. By being hands-on from the get-go, you move from sitting in a reactive posture to a proactive one—choosing when and where you engage with the system rather than the system making a choice for you at 2:00 AM on a Saturday.

You must work holistically and inclusively, with empathy. Don’t be afraid to ask for demonstrations and to maintain an open mind. PAM platforms are exceptionally advanced, and there are a lot of things that they are capable of. Advocate for yourself and work with the organization that is helping you—we need you to tell us what you need so we can configure it for you. The faster you do this, the faster you get involved (volunteering as a stakeholder/ an early adopter, etc.) the easier the whole process becomes for your team and for your company as a whole. In this way, the platform can be built from the ground up with your needs and concerns front and center in the construction and configuration process.

BIOGRAPHY

JAMES HAUSWIRTH

James Hauswirth, a native of Corpus Christi, Texas, is a highly accomplished IT security practitioner with extensive experience in the military and technology sectors. He excelled in sports during high school and pursued a career in information technology, earning a Master's degree in cybersecurity management from Purdue University. James served in the Iowa Army National Guard for 16 years operating in multiple roles, ultimately retiring as a Chief Warrant Officer 2, UH-60M Blackhawk pilot. He is an authority in Privileged Access Management (PAM) and brings a servant leadership approach to his customers and colleagues. James values spending time with his wife and four children, as well as engaging in activities like reading, gaming and exploring the open road on his once beloved motorcycle.



GUIDEPOINT

SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132
07.2023