5 Minutes With
www.securitymagazine.com/articles/102100-the-new-battleground-of-cybersecurity

Bio image courtesy of Maude

The New Battleground of Cybersecurity

Jordyn Alger
January 29, 2026

Cyber threats are evolving at accelerating rates, and many cyber experts have differing opinions on what the "new battleground" will be. Here, *Security* magazine talks with James Maude, Field CTO at BeyondTrust, about why he believes that new battleground is identity security.

***Security* magazine: Tell us about your background and career.**

Maude: I've always had what I would consider a hacker mindset, a curiosity to take things apart, understand them, and use that knowledge to solve problems. That mindset took me on a circuitous route into the cybersecurity industry; after being kicked out of high school for hacking computer systems, I worked a range of jobs, managing office supply companies by day and cracking Wi-Fi networks by night until I started a Digital Forensics degree which led me to the world of security research. After publishing some papers, I was offered a full-time researcher position at a local university and then later moved into industry.

I have spent the last 15 years helping to build security research teams and working strategically across product and engineering teams to help solve real world security challenges. I now focus most of my efforts on the identity security battleground which I see as vital in defending against modern cyber threats. As a side project I also run the Adventures of Alice and Bob podcast where we shine a light on the folks working tirelessly behind the scenes in cybersecurity to find out about their journey, what motivates them, and to share the stories of the events and incidents that have shaped their careers.

***Security*: Despite security awareness training and new security technologies, many organizations still face breaches related to human error. Why is this?**

Maude: As the saying goes, to err is human but to really go wrong, you need a computer. There are two main sides to the challenge of technology and human error: the supply side of building and deploying the technology itself and the end user side where the human meets the machine.

On the first, the supply side, where we have humans building software, configuring systems, and managing risk, the challenge is that the technology is increasingly complex and interconnected. This means that no one person can hold a complete mental model of the risks and how to mitigate them, so human error becomes an almost inevitable outcome. Nowhere is this challenge more evident than in the world of identity security, where we used to focus on securing a small number of highly privileged humans known as domain admins. This felt manageable as you knew who they were and what they could do. With the shifting technology landscape of cloud, SaaS, and hybrid environments, almost every identity is privileged in some way. Interconnecting systems open new paths to privilege for attackers while the humans managing it default to thinking in smaller, manageable identity silos, only looking at part of the picture as they wrestle to regain control of identities and their privileges.

In addition, on the end user side we fall into the trap of relying on the user to not click the link, not use the same password for everything, and understand the risk of all the privileges their identity holds. If we look at common modern attack chains, we can quickly see why our security training and tooling is failing. It starts with an identity being compromised that could be through a password leak, a phishing email that links to a highly realistic looking login page, or simply an attacker calling up the service desk and asking for a password reset or MFA reset. The attacker can then simply log in rather than hack in and access data and resources across a range of cloud systems. There is no exploit code to detect, no malware payload to prevent, and the only limit on the impact is the amount of privilege and access that identity holds. Relying on the human firewall or the credentials used to authenticate alone doesn't stack up against modern identity-based threats.

This, to me, is why identity is so much more than the new perimeter — it is the new battleground of cybersecurity.

***Security*: Why should AI agents be treated as privileged users and how are they reshaping the identity landscape?**

Maude: The AI genie is well and truly out of the bottle as employees race to embrace AI — whether you like it or not. For AI agents to deliver value they generally need privilege to access data, systems and resources. In this AI arms race we are seeing agents being created with little regard for the consequences of granting those privileges, sharing credentials with an agent, or granting long lived access tokens.

Imagine you hired a new intern without asking for company approval and then gave them your passwords, access to all the company's data and the ability to make changes as you. Not only that but they could use it out of hours, any time of day or night. Seems like a bad idea, right? Yet that is what we are seeing play out with AI agents in many organizations. Even where they are being used as approved tools, we often see that organizations are unaware of the volume of highly privilege Agentic AI identities being created behind the scenes, any one of which could become the source of a breach.

It's not about treating all AI Agents as privileged identities; it's about understanding the privileges of all identities — human and non-human — including AI Agents so you can understand and protect your identity security attack surface. With that understanding you can then take a least privilege approach, implement just-in-time access, and monitor for abuse.

***Security*: How can organizations cultivate a strong, modern security culture? Is it time for privilege access management to evolve beyond passwords?**

Maude: To me this is all about aligning your security teams and culture around identity. Many organizations end up with siloed teams and technology stack with one team managing IAM, another managing security, and others managing cloud, DevOps and so on. This creates gaps in visibility and control leaving them blinded to modern threats. Privileged Access Management (PAM) has already evolved far beyond looking after a small number of passwords for domain admin accounts and is a part of a broader privilege-centric identity security that is vital to secure any organization. From managing the secrets used by machine identities in CI/CD pipelines to granting just-in-time access for human identities accessing cloud resources, modern PAM is across the entire technology ecosystem. When every identity has some level of privilege, privilege-centric identity security is the deciding factor in what the impact of an identity compromise, breach, or attack is.

***Security*: Is there anything we haven't discussed that you would like to add?**

Maude: Beware of compliance complacency. Many organizations will through choice or regulation be aligned to some form of security framework. These are often mistaken as desired end states rather than the bare minimum controls that they usually are. MFA is a great example where having some form of MFA on most accounts is set as the goal post. However, not all types of MFA are equal, a fact that is often better known by attackers than those deploying it. So organizations might feel secure by using push notifications or Authenticator device code MFA, but in reality, this provides threat actors with more of an opportunity than a challenge. Adversary-in-the-Middle (AitM) toolkits like Evilginx make light work of compromising an identity with these weaker forms of MFA. Even when stronger phishing resistant forms of MFA such as FIDO2 are used, there will often be an option to roll-back to a weaker form for convenience, again opening up an attack vector for that identity.

When it comes to securing identities, think about controlling not only how you log in, but what you can do once you have logged in.

Jordyn Alger is the managing editor for *Security* magazine. Alger writes for topics such as physical security and cyber security and publishes online news stories about leaders in the security industry. She is also responsible for multimedia content and social media posts. Alger graduated in 2021 with a BA in English – Specialization in Writing from the University of Michigan. *Image courtesy of Alger*