TAG

UNDERSTANDING THE WORKFORCE EDGE APPROACH FROM NUDGE SECURITY

DR. EDWARD AMOROSO,
CEO, TAG
RESEARCH PROFESSOR, NYU

nudge

TAG

UNDERSTANDING THE WORKFORCE EDGE APPROACH FROM NUDGE SECURITY

DR. EDWARD AMOROSO, CEO, TAG,
RESEARCH PROFESSOR, NYU

With so many cybersecurity vendors in business today, it is rare that our team at TAG sees an idea or concept that we believe is truly fresh in terms of how it approaches the reduction of cyber risk in enterprise. But we spent time recently with the leadership of Nudge Security, and we were impressed with their model of Workforce Edge as a way to address common deficiencies in modern enterprise cybersecurity. This report outlines what we learned.

Nudge, today, shows strength in its approach to handling risk, especially in the context of Software-as-a-Service (SaaS) and generative AI applications, which are increasingly the backbone of most companies. The Workforce Edge model is a natural extension of what they've been doing, but we like how it combines modern methods for SaaS and related risk reduction with focus on addressing perimeter weaknesses.

POROUS ENTERPRISE PERIMETER

A major conundrum in modern enterprise security is that so many security teams, including their Chief Information Security Officer (CISO), will acknowledge that the perimeter does not work – and yet, it remains the primary control for audit and for determination of whether incidents occur internally or externally, which is important for establishing materiality. For example, if data is exposed to an internal marketing team, then this is not an incident.

But when security teams are asked to define what they view as their actual perimeter, the answer has evolved from prior years. Roughly a decade ago, it was thought that the perimeter was virtual or even software defined. We saw startups emerge trying to cover this software defined perimeter (SDP), but practitioners found this also to be an enormously difficult boundary to define – and an even tougher one to police.

What we like about now about the Workforce Edge model is that it elegantly presents the perimeter in terms that we believe match up well with how security teams actually view their task. Rather than trying to identify some perimeter in terms of devices, nodes, or networks, our observation at TAG is that security teams instead have used the corporate workforce including employees, staff, third parties, and other stakeholders as the defining elements.

WORKFORCE EDGE MODEL

Let's examine the model, which serves as the basis for the Nudge platform, in a bit more detail. As we have intimated above, unlike traditional approaches that center control around networks, endpoints, or identity providers, the Workforce Edge model will focus on users and their behavioral patterns. This includes how users discover, access, and interact with SaaS and cloud services over time.

Note again that this edge model isn't defined by hardware. Rather, it's a model that is driven by human activity, with particular emphasis on SaaS applications, because – and this is key – we have seen most businesses evolve into a collection of SaaS applications adopted by business teams and individual employees. The prior concept of workers on a local area network (LAN) accessing enterprise software is mostly replaced by users choosing their own SaaS and genAI applications from pretty much anywhere, including the corporate office.

If you accept this evolution and this idea that users present the perimeter and SaaS applications serve as the base for modern business, then the Workforce Edge concept, as defined and implemented by Nudge Security, is a good choice for your environment. In such case, the path to security for you will lie in continuous, real-time visibility into the SaaS sprawl initiated by your company, teams, and people, not just devices or accounts.

FROM PERIMETER TO PEOPLE: THE CONTEXT FOR WORKFORCE EDGE

One aspect of the Workforce Edge model that we find particularly interesting is its insistence that even identity, often held up as the new perimeter, is not sufficient. As Nudge Security suggested to our team at TAG, identity platforms like Okta or Microsoft Entra provide valuable control, but their visibility is limited to pre-approved apps and federated services – and this observation resonated with us for sure.

As an illustration, what happens when a developer signs up for a generative AI service with their work email? Similarly, what happens when a salesperson quickly tests a new CRM platform before submitting a procurement request? These common situations, often invisible to security teams, represent the true expansion front of organizational risk. They are spontaneous, user-driven, and often short-lived—but they can create vulnerabilities, including:

- **Unsanctioned shadow SaaS**
- **Accidental data exposure**
- **Persistent tokens and API keys**
- **Insider risk from unsupervised app adoption**

The Workforce Edge is therefore defined less by where traffic originates, and more by why and how the traffic was initiated in the first place. This represents to our team at TAG a useful and fundamentally different means for implementing security in the enterprise.

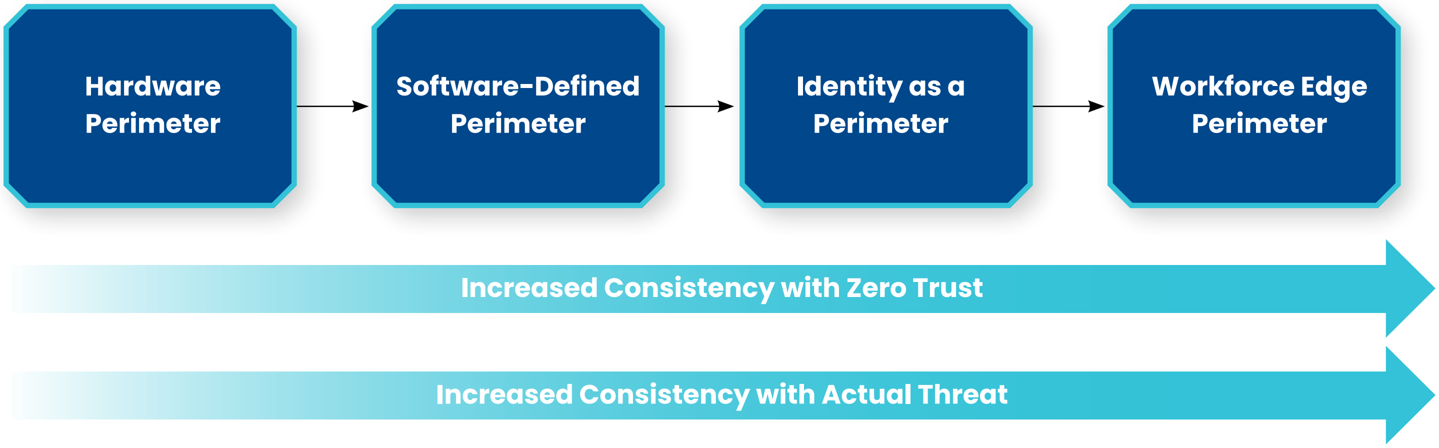
Hardware Perimeter
Software-Defined Perimeter
Identity as a Perimeter
Workforce Edge Perimeter
Increased Consistency with Zero Trust
Increased Consistency with Actual Threat

Figure 1. Evolution of the Perimeter Model

NUDGE SECURITY'S PLATFORM

To operationalize this conceptual perimeter, Nudge Security has built a platform that begins with SaaS discovery. This is not done through logs or firewall data, but through cloud-based email telemetry and behavioral analytics. The method relies on passive signals such as OAuth consent grants, welcome emails, password reset requests, and other email artifacts to reconstruct a map of every SaaS service a user touches, no matter how obscure or unapproved.

This approach stands out for two reasons. First, it doesn't require endpoint agents, browser plugins, or network-based integrations. It's infrastructure-agnostic, which makes it viable even in decentralized environments. Second, it is based on the Workforce Edge, capturing risk where it starts: with user-driven intent. Note that this method of using behavior to drive insight is common in enterprise such as with Customer Relationship Management (CRM) tools.

Once SaaS usage is discovered, Nudge Security's platform does something unusual: It initiates dialogues with users, prompting them with "nudges" that are neither punitive nor overly technical. These nudges might ask security-related questions directly to the user. Typical example questions might be the following:

- **"Did you intend to create an account with X?"**
- **"Does this app contain customer or sensitive data?"**
- **"Is this for personal or company use?"**
- **"Are you aware of our company policy regarding this type of SaaS application?"**

This form of micro-engagement allows security teams to blend security policy with behavioral science. The platform tracks responses, enabling analysts to triage activity based not just on technical risk, but on user context and intent. This framework contrasts with traditional SaaS security tools, which often rely on rigid control gates such as blocking access or revoking privileges without nuanced understanding.

WORKFORCE EDGE VS. SSPM: WHAT'S THE DIFFERENCE?

As industry analysts, we have noticed that many observers, including enterprise buyers, might confuse Nudge Security's offering with the broader category of SaaS Security Posture Management (SSPM) platforms. While Nudge Security certainly does reduce SaaS risk, as we've explained above, the reality is that the comparison of Nudge Security to SSPM platforms shows many differences upon closer inspection.

SSPM tools typically focus on post-integration hygiene. They ensure that sanctioned SaaS services like Salesforce, Slack, or Google Workspace are configured securely, comply with internal policies, and remain free of misconfigurations. These tools are essential for posture management, but they do not detect SaaS usage that hasn't yet been integrated with IAM platforms or CASBs.

Nudge Security addresses this blind spot directly. Its premise is that risk is introduced before integration, not after. By identifying and cataloging SaaS usage at the moment of user engagement and before access control policies are applied, Nudge is effectively shifting security left, not in code, but in behavior. This is perhaps the most compelling aspect of the Workforce Edge model: it expands the security lifecycle to include the pre-adoption phase.

BEHAVIORAL RISK AT THE EDGE

The Workforce Edge model does come with challenges. Chief among them is scale, not in terms of infrastructure, but in the psychology of enterprise users. Engaging users repeatedly through nudges can backfire if not carefully tuned. Nudge Security seems to be aware of this and is investing in user interface (UX) research to ensure that its prompts are perceived as helpful, versus being annoying.

Another challenge is cultural. Some CISOs may view soft prompts as insufficient in cases of malicious or negligent behavior. But this is precisely where Nudge's model becomes complementary rather than competitive: it doesn't replace enforcement but rather informs it. By adding behavioral telemetry and context before jumping to enforcement, security teams can make better decisions.

There are also opportunities to apply this behavioral dataset toward insider risk mitigation, AI tool governance, and data egress monitoring, each of which represents a hot-button area in today's security posture conversations. As more SaaS services embed LLMs or generate autonomous data flows, the need to monitor why users are adopting tools (not just what tools are adopted) will become essential.

TAG VIEW: WHAT NUDGE GETS RIGHT

From a TAG analyst perspective, we see the Workforce Edge model as an overdue reframing of the modern enterprise security challenge. That is, just as early network security focused on ports and protocols, today's security must center around humans-as-edges. Nudge Security's framing is useful not only for its product implications, but for how it shifts our industry's collective thinking in cybersecurity strategy.

The model also aligns well with the evolution of zero trust principles, which increasingly emphasize context-aware decisions and decentralized visibility. Traditional security telemetry, which was focused on endpoints or IPs, has always missed the nuance of human-driven SaaS sprawl. We believe that Nudge's Workforce Edge model captures this nuance without requiring disruptive architectural changes.

The company's ability to remain vendor-agnostic, integrating easily with Okta, Google, Microsoft, and others, also positions it well to serve multi-cloud enterprises with fragmented IAM and SaaS procurement. No buyer of Nudge Security will need to make major changes to its deployed architecture. We view this as a nice feature and something that allows for easy deployment and support.

CONCLUDING NOTE

Readers who would like more information on this model or any other aspect of cybersecurity should feel free to reach out to TAG. Our Research-as-a-Service (RaaS) customers can request assistance through their RaaS portal accounts. Additionally, we strongly encourage readers to reach out directly to Nudge for more guidance on their fine platform, including a demo. We expect that the time will be well-spent. We look forward to hearing from you.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence,.

The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.