Integration to Innovation: Leverage GenAI for Secure Platform Evolution

A lot of agencies are currently drinking from the firehose when it comes to understanding applications for generative artificial intelligence (genAI). When it comes to security, there are two main approaches to genAI, according to Mark Mitchell, enterprise security architect at Netskope: It can be used to minimize complexity in security operations, or it can be used within a security platform itself to increase performance.

Safely Enabling GenAI

Whether it's a zero trust architecture or a secure access service edge (SASE) platform, cybersecurity boils down to the same first step: visibility. Mitchell said many agencies are stuck in the "streetlight effect," where they have certain platforms in certain areas, and can see into those very well. But areas outside of those platforms aren't built to be visible. Because of this effect, they often don't realize they're already using anywhere from 50 to 100 apps that have genAI internally. But once they achieve that visibility and discover those apps, their concern turns to the data going into them.

But there are ways to safely enable genAI.
For instance, using Netskope, an organization can serve users a pop-up warning whenever they access unauthorized genAI platforms, warning them of what the policy is, and what the appropriate use is. Mitchell said, "You can further block any upload of or posting of data into that genAI platform if it meets a particular data loss prevention policy. So if I went to try and upload a code sample, a Python code sample, into ChatGPT asking it to give me some output, you would be able to block that upload, meaning that data would never cross that security boundary into the ChatGPT boundary."

At the heart of this are zero trust principles: Only authorized users from authorized locations can access sanctioned instances of genAI, and additional data protections can be layered in on that to limit the interactions. And that requires continuous validation of not just the user, but the location, the device, the network, the security group.

> We use deep learning models to understand the behavior of those sites that would deliver phishing and ransomware and how ransomware behaves, so that we proactively can monitor those behaviors. So it's how we use it to operationalize security capabilities and make it ultimately less complex for the agency to look at risk and understand it."
>
> Mark Mitchell, enterprise security architect at Netskope

Using GenAI to Enhance Platform and Security Controls

Netskope uses genAI to enhance its own platform security controls, increasing efficacy and reducing the complexity of threat and malware detection, through its SkopeAI functionality.

"We use deep learning models to understand the behavior of those sites that would deliver phishing and ransomware and how ransomware behaves, so that we proactively can monitor those behaviors," Mitchell said. "So it's how we use it to operationalize security capabilities and make it ultimately less complex for the agency to look at risk and understand it."

That means agencies don't have to rely on less-than-real-time threat feeds or indicators of compromise. Another use for genAI, internal to the platform, is behavior analytics. Many agencies are just coming to terms with all the logs they need to capture on user behavior. GenAI and machine learning can help them understand those logs and spot anomalous behavior, without the expense of storing those logs. That means agencies can be proactive about anomalous user behavior detection, achieve a higher level of security compliance, and reduce their data storage costs. Netskope also has a data protection process Mitchell referred to as "train your own classifier." Everyone agrees that it's imperative to prevent personally identifiable information from escaping the agency's networks, and PII is clearly defined in the controlled unclassified information catalog. But what about agency intellectual property? That can be murkier, and far more complex to control.

"Using machine learning, Netskope allows you to upload artifacts, including images, both for training and what we would call a negative learning model as well, to build a data classifier right," Mitchell said. "Now, with AI and train your own classifiers (TYOC), you can teach the platform, from an AI perspective, what the intellectual property looks like."

GenAI in DevSecOps

This can also be used to help shift security left in DevSecOps processes. Using sanctioned repositories and software bills of materials, genAI can leverage what Netskope calls instance control to ensure any code being pulled, developed, or distributed uses only 100% sanctioned information.

"If there's anything that deviates from that, we're able to call that out, provide a warning, understand what the activity is, and it may never be a malicious intent or a malicious actor, just somebody who doesn't know," Mitchell said. "Education coaching is part of the interaction that we provide not just for the operators, but for the day-to-day users. And that's something that's very unique to our approach to technology."

> "Education coaching is part of the interaction that we provide not just for the operators, but for the day-to-day users. And that's something that's very unique to our approach to technology."
>
> Mark Mitchell, enterprise security architect at Netskope