ANALYST CONNECTION
Sponsored by: Adobe

The document is a Q&A with Maarten Van Horenbeeck, Adobe's chief security officer, discussing top security concerns, balancing AI/GenAI technologies with security, Adobe's unique security approach, and measures for protecting hybrid work environments.

Navigating AI, Hybrid Work, and Trust in a Connected World

November 2024

Questions posed by: Grace Trinidad, PhD, Research Director, Future of Work, and Holly Muscolino, Group Vice President, Workplace Solutions

Answers by: Maarten Van Horenbeeck, Chief Security Officer, Adobe

Q. What are the top security concerns that keep you up at night?

A. One of my primary concerns is the increasing integration of software systems. You may have 10 different software products that interface with each other, and the way they use each other's data and the way trust relationships are established between products are a real concern for people in my role. The more tools that are connected, the harder it becomes to monitor and secure data. IT departments may not always be fully aware of how each tool interacts, complicating security efforts.

When evaluating software vendors, I recommend focusing on three key areas:

- First, ensure the vendor adopts a security-first mindset during product development. This means recognizing that they are part of the broader supply chain and have implemented security controls to manage data sharing effectively.
- Second, look for products that are secure by default. This is crucial because after deployment, non-security staff will likely manage the product. Products should have security features enabled by default, reducing the need for extensive configurations and making it easier to control exceptions rather than reconfiguring for security from the start.
- Third, it's important to consider defense in depth, a well-established security principle. It means having multiple layers of protection, so if one control fails, there are others in place to safeguard against potential breaches.

Beyond these core principles, there are industry standards emerging around enterprise-level security features. One such standard is the minimum viable security product (MVSP), developed by multiple organizations. Although not a definitive solution, these standards provide valuable guidance on essential security features and configurations, like the requirement for single sign-on (SSO) as a baseline.

Finally, ensure that security settings are conservative by default, particularly for sharing features. This means making secure configurations the path of least resistance, while options that introduce potential risks should require more friction to be used, ensuring safer overall deployment.

Q. How is Adobe balancing AI and GenAI technologies with security?

A. I think this topic is on everyone's mind in the industry. We have two main perspectives: one is how we use generative AI (GenAI) internally at Adobe, and the other is how we integrate it into our products. I'll start with our enterprise approach. Early on, we realized that as a company developing AI technologies, it was crucial to leverage them internally as well. We formed an interdepartmental steering group that included me as chief security officer, our chief privacy officer, and leaders from various teams, which include products and technology services. Our goal was to enable employees to innovate with AI while maintaining the necessary safeguards. We developed standards and practices to make it easy for teams to not only experiment and innovate but also evaluate security risks and appropriateness if the technology is being brought to a wider audience.

For our products, we focused on our enterprise customers, particularly those with strict security requirements for their documents and data. We made several commitments, like not using customer data to train our language models and giving customers control over where the AI sources data. We wanted to make AI features transparent, verifiable, and easy to manage and/or disable, especially for those in security roles. Our ethical principles guide how we design AI.

Q. Given the prevalence of hybrid work, what security measures has Adobe taken to protect employees working from home and other remote locations?

A. As a company that supports hybrid and remote work, Adobe has implemented several key security measures to protect its employees working from home or in remote locations. Although I wasn't at Adobe during the onset of the COVID-19 pandemic, the company had already taken significant steps prior to the pandemic, which proved valuable in this transition.

One of the major initiatives was deploying an enterprise networking platform architecture. This allowed Adobe to manage employees' devices, authenticate them, and implement rules on what could be accessed remotely. Employees no longer needed to rely on a VPN — but rather accessed Adobe resources through an access proxy, ensuring that all traffic was encrypted in transit. This was crucial, as many employees were no longer working within protected office networks, but instead, they're suddenly in coffee shops everywhere. They're suddenly at home. Centralized access controls played a key role in securing this environment.

The second thing that was very important, was a shift in the way Adobe handled data sharing and how employees accessed data. Instead of relying heavily on email attachments, as has been done historically, the company moved to collaboration platforms that allowed people to share access to specific documents without having the documents sitting in everyone's mailbox.

The third effort was to collaborate with other organizations and share security intelligence. Everyone was seeing the same types of security issues, and our connections and relationships with other organizations allowed us to react effectively to those threat trends. Adobe's engagement with threat intelligence networks, such as the IT Information Sharing and Analysis Center (IT-ISAC) is one good example, but our one-on-one collaborations with other companies are really important — we're all in the same boat, learning about each other's challenges.

Q. What makes Adobe's approach to security different from other companies?

A. The way Adobe works as a company and the amount of people we have across the world contributing to our products makes it incredibly important that we, as a security team, take a people-centric approach to security and actually represent the people we serve, whether they're our customers or the people inside the business. Adobe also adheres to a stance of broad responsibility, identifying risks before they become risks to the customer, and finally, a defense-in-depth strategy, building adaptable defenses into our products.

Even before I worked for Adobe, I appreciated Adobe's strong presence in the security community, investing in and funding organizations that work to bring new talent in, partnering with organizations like BlackGirlsHack and Women in CyberSecurity. Security has become much more specialized today, and it is no longer as easy for people to break into the field. We're only going to be successful if we can actually get that talent into our organizations. We also continually seek different perspectives, which is why Adobe's Bug Bounty Program is critically important. The people that participate in these Bug Bounties all have different perspectives and look for things we may not even be thinking of. This collaborative approach strengthens our defense against evolving threats and speeds identification of security weaknesses in our products. We also prioritize diverse, real-world security experience and enable our security engineers to learn from the people that use our products. We partner with an NGO in Switzerland called the CyberPeace Institute, which partners nonprofit organizations with cybersecurity questions with commercial companies like Adobe to provide pro bono cybersecurity support and advisement. Because of this partnership, our security engineers develop an outside experience and a different view of how customers actually use these types of technologies.

In addition, at Adobe, we take a broader responsibility approach. We focus on the impact our products have in the world and how we can ensure customers use them as safely as possible. For example, we have rolled out technologies like passkeys, which offer a simple way to use multifactor authentication, and we proactively lock credentials of users we know have been compromised. If we learn about a third-party breach and discover someone has reused their password from that breach with our products, we validate the data and take action to protect those users.

Last, Adobe also focuses on defense in depth. We thoroughly test security vulnerabilities and spend a lot of time addressing them. However, since some vulnerabilities might not be found in time, we roll out features like protected mode or sandboxing in our products to safeguard users while they interact with them. We're always thinking ahead, trying to solve potential issues before they become bigger problems.

Q. Adobe publishes product security testing reports to the public. Could you share more on that?

A. Adobe has taken a unique approach to security testing that differs slightly from standard industry practices. Most companies rely on third-party penetration testing, which is a great practice, and we do the same. These external reports are crucial for helping companies do business with each other by showcasing their security testing results. However, we decided to enhance this by also including the results of our internal security testing and Bug Bounty Programs in the reports we share with customers.

We made this change about a year ago to give our customers a fuller view of the testing our products undergo. Sometimes, customers are surprised by the number of findings in our reports compared with other companies. The reason for this is our inclusion of internal testing results, which offers a more comprehensive look at the security of our products.

This approach has helped us build greater trust with our customers. To me, trust is built on transparency — letting others see how and why you do things, and consistently maintaining that reliability. This approach is not only about our customers but also about learning from our vendors. We believe that by sharing security practices, we can collectively raise the bar, improving security across the entire ecosystem. By engaging in meaningful conversations with vendors, we all learn and grow, evolving toward higher security maturity together.

About the Analysts

Grace Trinidad, *Research Director, Future of Trust*

Grace Trinidad is Research Director in IDC's Security & Trust research practice responsible for the Future of Trust research program. In this role she provides strategic guidance and research support on approaches to trust that include risk, security, compliance, privacy, ethics, and social responsibility.

Holly Muscolino, *Group Vice President, Workplace Solutions*

Holly Muscolino is the Group Vice President, Workplace Solutions, responsible for research related to innovation and transformation in content solutions, including intelligent document processing, esignature, imaging and printing and other content workflow services. Ms. Muscolino's core coverage also includes work transformation, technology & digital skills research, and the role of technology in driving the Future of Work.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

IDC Custom Solutions