LayerX | CASE STUDY

LayerX Helps KnowBe4 Protect Data, Govern Identities And Enable GenAI Without Any Friction

Introduction

KnowBe4 is the world's largest human risk management platform, used by tens of thousands of organizations around the globe. Through videos, interactive elements, phishing simulations, and email security training, KnowBe4 aims to boost awareness of digital threats and how to deal with them. It empowers organizations to manage the ongoing problem of social engineering by helping them train employees on best practices to reduce risks from phishing attacks and by making smarter security decisions every day.

To live up to their high security standards, KnowBe4's security team continuously assesses their architecture to enhance protection and eliminate any unprotected blind spots.

Through its analysis process, KnowBe4 recognized that most of its users consume GenAI tools and Web/SaaS apps via the browser, making the web browser the main point of risk for data leakage. Their existing network, application and endpoint security tools did not provide adequate coverage to protect the last mile of user activity, due to which KnowBe4 has identified the browser as a unique threat surface that requires dedicated protection. They aimed to empower employees with the freedom to use web apps and GenAI tools efficiently, while controlling data leakage and unauthorized access risks.

knowbe4

Industry
Human Risk Management Training

Size
2,300

Location
Worldwide

Challenges

- Preventing data exfiltration across websites and SaaS apps
- Allowing secure use of GenAI tools to drive employee productivity, while preventing data leakage and shadow AI risks
- Protecting against shadow identities and blocking hidden browser-based identity threats

LayerX Solution

- **Web DLP:** Visibility into browser sessions and user activity at a granular level to prevent users from uploading or pasting sensitive data to ungoverned SaaS/Web applications
- **Shadow AI and Gen AI DLP:** Blocking unauthorized GenAI apps while ensuring continued productivity by enabling the use of governed GenAI tools through continuous monitoring and preventing sensitive information exfiltration
- **Identity Protection:** Monitoring which identities are used to log in to SaaS apps, detecting shadow accounts operating outside of SSO, and enforcing identity-aware policies to ensure only approved, verified users can access and share sensitive corporate data.

Protecting from Insider Threats and Data Exfiltration on Web and SaaS Applications

Challenge: Data Exposure on Web and SaaS Applications

Web and SaaS applications are the easiest channels for insider threats and inadvertent data leakage. Practically all users have internet access from the browsers on their endpoints, meaning they can use it directly to exfiltrate data without having to connect external devices (such as USB drivers) or connect to outside networks. In most cases, it is the path of least resistance.

On these platforms, data is no longer a discrete file that traverses known channels like email. Rather, it stays embedded within real-time cloud-based applications, accessed and manipulated entirely via the browser. Traditional DLP tools are mostly file-centric and fail to protect data-in-use, leaving organizations blind and exposed to sensitive data leakage.

Employees may copy and paste sensitive data or upload files to ungoverned SaaS and Web apps using non-corporate identities. This could include risky sites like online drives, file-sharing SaaS apps, web messaging tools, etc., which are crucial for day-to-day work. Without full control and oversight, organizations are left vulnerable to data leaks, which happen unnoticed through these channels.

KnowBe4 wanted to detect and control shadow SaaS usage and ensure employees weren't exposing internal documents or customer data on sanctioned apps. They needed an easy-to-deploy solution that covered web DLP without impacting user experience.

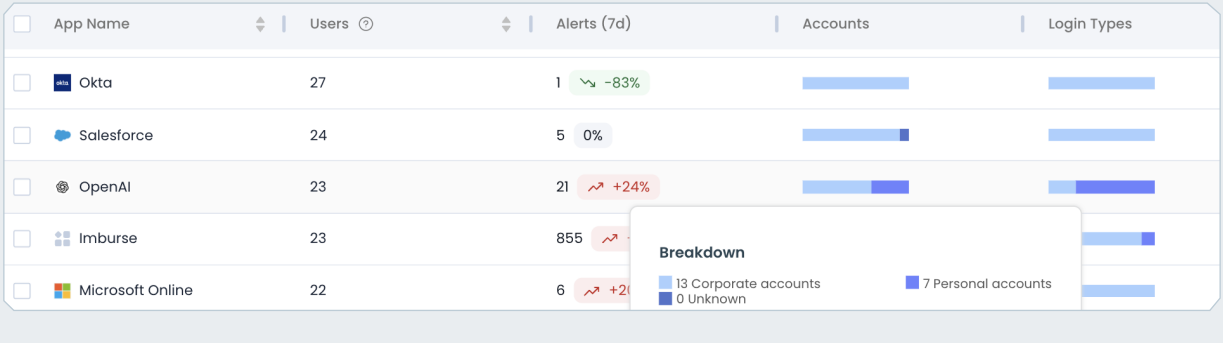
LayerX Solution: Web DLP to Prevent Data Exposure Risk

LayerX provides complete visibility into all websites and SaaS apps, identifying which tools are accessed, by whom, through which accounts (corporate or personal) and what data is going through them. It controls both file-based and file-less data transfers, such as text input, copy-paste, and file sharing, by using real-time classification and labelling to detect sensitive data shared with SaaS apps and unsanctioned services.

Organizations can define granular policies based on website category, data sensitivity, user identity, etc., to create tailored security policies with a range of enforcement options, ranging from monitoring only to warning users with customizable messages, to masking sensitive data, or to completely blocking their actions.

The KnowBe4 team used LayerX to bring full browsing context with identity awareness and cross-identity controls into their DLP logic. They restricted logins and activity on multi-tenant SaaS apps like file-sharing tools and online drives when accessed via unmonitored, non-corporate accounts. This ensured that sensitive corporate data could be accessed and shared only by verified corporate users.

> "LayerX unlocked visibility into previously hidden browser activity like text inputs, copy-paste and file uploads to all web apps, including both sanctioned and non-sanctioned apps. This gave us the controls to stop data leakage before it happens."
>
> Kenneth Elie, Senior Information Security Engineer at KnowBe4



Restricting Shadow AI Usage and Preventing Data Leakage to GenAI tools

Challenge: Employees Inadvertently Leaking Sensitive Data to GenAI Tools

Preventing GenAI data leakage has become an industry-wide problem. The widespread use and convenience of AI-driven tools and lack of awareness result in employees unknowingly sharing proprietary and confidential information while seeking assistance, developing code or generating content. GenAI tools transmit all data uploaded to them to external LLMs. This creates security risks as such data might be stored remotely, used for LLM training, or exposed to third-parties. This unintentional data sharing can compromise the organization's security posture and expose it to legal and compliance risks.

Traditional security measures such as SASE/SSE, Network DLP tools and employee training programs are not fully equipped to handle the unique risks posed by AI-driven tools. While they can enforce file-centric data transfer restrictions, the main issue arises when there is file-less data activity like copy/paste, text input, etc. This means that despite efforts to secure data, there was a gap in effectively monitoring and controlling how employees interact with AI tools.

While some organizations block GenAI altogether, KnowBe4 recognized the productivity advantages of GenAI tools and how they could enable businesses to operate more efficiently. KnowBe4 wanted to allow access to approved AI tools while blocking all GenAI activity from unauthorized or shadow AI apps. They also needed to monitor and control all data shared with GenAI tools. The goal was to let employees use these tools to boost productivity and innovation without risking sensitive data leakage.

Since the browser is the primary point of access for GenAI tools, it has become the main channel for both usage and risk. To gain complete control and visibility over GenAI interactions, KnowBe4 needed dedicated browser-based protections that could monitor, analyze, and enforce policies at the exact point where data is entered and shared.

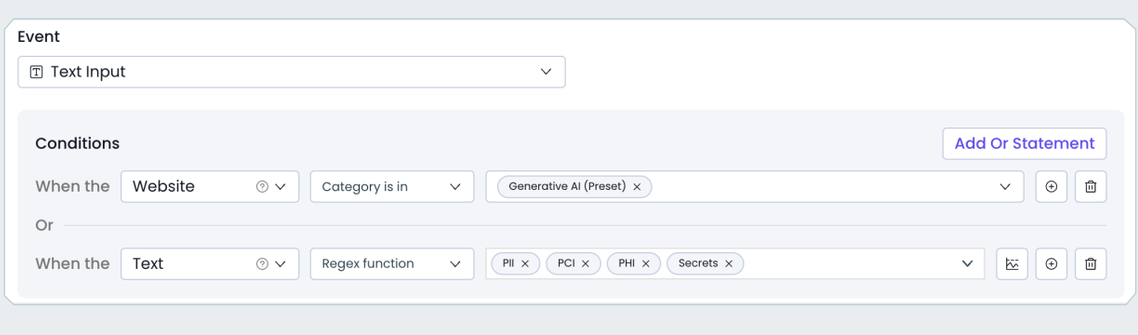
LayerX Solution: GenAI Discovery and Prevent GenAI Data Leakage

LayerX is deployed directly within the browser, giving it direct visibility and control over all GenAI activity. It monitors user actions such as browsing activity, login attempts, data input, and file uploads, identifying which tools are accessed, by whom, and through which accounts (corporate or SSO or personal). This enables organizations to detect unauthorized data sharing and enforce policies to block 'shadow' AI applications.

LayerX permits organizations to enforce last-mile controls on GenAI tools and AI-enabled SaaS applications, directly within the browser, with granular enforcement options ranging from monitoring only to warning users with customizable messages, to masking sensitive data, to completely blocking their actions. By leveraging advanced algorithms and real-time analysis, LayerX detects and prevents typing, copy/paste or sharing files with sensitive data, ensuring confidential information is not exposed. This proactive approach enables organizations to benefit from the productivity capabilities of AI while maintaining stringent data security standards.

The KnowBe4 team deployed LayerX on the browser to secure employee interaction with GenAI tools and allow them to use it without compromising security.

> “Most employees now use AI to some level, but shadow AI tools were a growing blind spot. LayerX gave us the ability to identify unauthorized GenAI use, block it, and focus employee access on approved tools only.”
>
> Kenneth Elie, Senior Information Security Engineer at KnowBe4



Protecting Shadow Identities and Blocking Hidden Identity Threats

Challenge: Employees Access SaaS Apps With Unauthorized Identities

As SaaS usage explodes across organizations, users frequently use unsanctioned SaaS applications, which are not known or monitored by the organization. Access to such “shadow” SaaS apps is often done using personal accounts or non-federated corporate accounts. This means that these identities are not authenticated against the organization's IAM systems, and security teams are blind to their existence. These "shadow identities" make it impossible to track what data is being accessed or shared, and by whom. The problem is amplified in multi-tenant SaaS apps where a single user might log-in through multiple accounts, blurring the lines between corporate and personal usage.

This results in fragmented identity governance, reduced visibility, and a complete lack of control over access policies and data flows. Security teams are left guessing which users are accessing which accounts, whether corporate data is being shared outside approved boundaries, or if malicious insiders are exploiting unmanaged accounts to exfiltrate sensitive information.

KnowBe4 wanted to shine a light on this blind spot and ensure that SaaS access and activity were governed not just at the app level, but at the user identity level. They needed to detect unmanaged SaaS identities in use across their environment, block unauthorized access, and ensure that only approved, SSO-backed identities could interact with sensitive data.

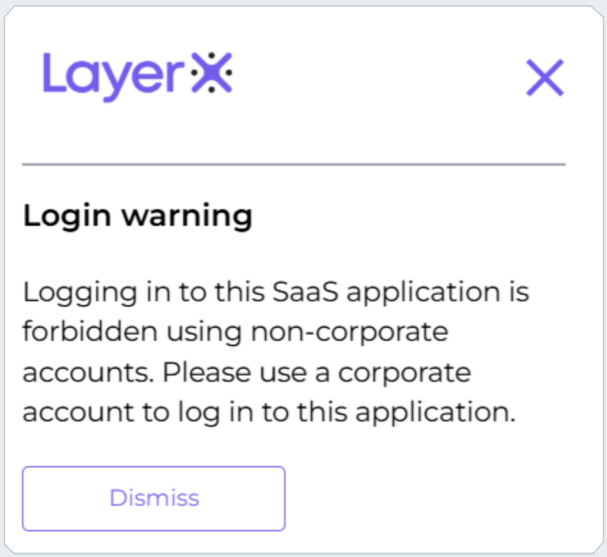
LayerX Solution: Discover Shadow SaaS Identities and Apply Identity Governance

LayerX provides granular identity-aware visibility and control over every SaaS login and session at the browser layer. It tracks which user is logging into which SaaS application, through which identity (SSO, corporate, personal, or shared), and what actions they’re taking. This unique vantage point enables full monitoring of shadow identities that operate outside SSO or IAM controls.

Using LayerX, KnowBe4 was able to discover unmanaged SaaS accounts being used in the browser, whether they were personal accounts, ex-employees, or duplicate identities, and enforce granular policies to restrict or block their usage. It provides full visibility and enforcement of browser-based identity governance, including password strength, password re-use, account sharing, non-SSO corporate accounts, OAuth permissions and more.

LayerX ensures that only verified corporate identities can access SaaS apps and perform activities such as uploading files, generating or viewing documents, or sharing external links. In addition, LayerX blocks personal account logins and enforces identity consistency across sessions, creating a secure, identity-governed SaaS environment with minimal friction to end users.

> “Before LayerX, shadow identities were a hidden threat we couldn’t control. Now, we have identity-aware visibility at the browser level that helps us catch unauthorized logins the moment they happen.”
>
> Kenneth Elie, Senior Information Security Engineer at KnowBe4



Conclusion:
Productivity-Driven Security, Powered by Browser-Native Protection

LayerX equips KnowBe4 with a powerful, user-first security layer that aligns with their strategic priorities: securing the browser while preserving productivity. By offering deep visibility into user activity, identity context, and data interactions within SaaS and GenAI tools, LayerX enables KnowBe4 to prevent insider threats, block shadow identities, and eliminate data leakage without restricting access to the tools employees rely on.

With LayerX, KnowBe4's security team could define and enforce granular policies without changing user behavior or impacting experience. Whether it's safeguarding against GenAI misuse, governing shadow SaaS identities, or controlling data exfiltration in real-time, LayerX ensures that the browser becomes an enabler of secure innovation. Its lightweight deployment, identity-aware protection, and file-less DLP capabilities make it an ideal solution for fast-moving, cloud-native teams who need both flexibility and control.

> "We were looking for a lightweight, comprehensive solution that could tackle GenAI risks, shadow SaaS, and identity threats. LayerX delivered on all fronts and has become a critical layer in our modern security stack."
>
> Kenneth Elie, Senior Information Security Engineer at KnowBe4

One Platform for ALL Browsing Risks and Web-Borne Threats