LayerX | CASE STUDY

LayerX Helps Dun & Bradstreet Gain Full Visibility and Control Over Browser-Based Risks, Protect Sensitive Data, Enable Safe AI, and Govern Identities Without Any Friction

Introduction

Dun & Bradstreet (D&B) is one of the world's most trusted sources of business data and analytics, empowering organizations to make informed decisions with accurate, real-time insights. As a global data company, protecting information assets is central to D&B's mission.

While D&B maintained a strong defense posture across endpoints, networks, and cloud environments, its security team identified an overlooked vector, the web browser, where employees now spend over 80% of their workday. From SaaS access to GenAI use, the browser had become the main workspace for their employees and a major blind spot for their security team.

Recognizing that traditional network and endpoint solutions provided little visibility into what actually happens within the browser, D&B sought a purpose-built solution to protect users, data, and identities at this critical last mile without introducing friction or disrupting workflows. They aimed to empower employees with the freedom to use web apps and GenAI tools efficiently, while controlling data leakage, risky extensions and unauthorized access risks.

After evaluating multiple solutions, LayerX emerged as the clear choice, delivering seamless deployment, deep visibility, and powerful browser-native protection without disrupting the user experience.

Closing the Visibility Gap Left by Network and Endpoint Security

Challenge: Limited Browser Visibility and Data Protection

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 SASE, DLP and endpoint solutions provided strong control over ingress and egress traffic but little insight into the browser itself. While these tools could filter URLs, categorize sites, and protect file-based uploads, they lacked visibility into what users were actually doing inside web sessions:

- Which SaaS apps they were logging into
- Whether they were using personal identities
- What extensions were being used
- What data was being copied or pasted

The result was a visibility gap around what SaaS apps employees were using, file-less data activity, browser extensions, shadow identities and more. Sensitive data could be shared or exfiltrated without detection, and identity misuse was difficult to track.
D&B wanted to gain visibility into its users' browsing sessions 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.

dun & bradstreet

Industry
Business Intelligence and Data Analytics

Size
6,000+

Location
Worldwide

Challenges

- Lack of visibility into browser activity could lead to unseen risks and silent data loss.
- Traditional SASE and endpoint tools stop short at the browser, leaving the most critical layer unprotected.
- Enabling secure AI use to drive employee productivity, while preventing data leakage.
- Eliminating threats from malicious extensions and shadow SaaS that bypass enterprise controls.
- Protecting against shadow identities while ensuring identity-aware, least-privilege access to SaaS apps.

LayerX Solution

- **Shadow AI and Gen AI DLP:** Allowing safe usage of approved AI tools and AI browsers while blocking unauthorized AI tools and sensitive data exfiltration
- **Web DLP:** Visibility into browser sessions and user activity at a granular level to prevent users from uploading or pasting sensitive data to SaaS and Web applications
- **Browser Extensions Protection:** Allowing the use of legitimate browser extensions and blocking malicious ones
- **Identity Security and Governance:** Detecting and restricting unsanctioned logins and shadow SaaS accounts, and enforcing identity-aware policies to ensure only approved, verified users can access and share sensitive corporate data

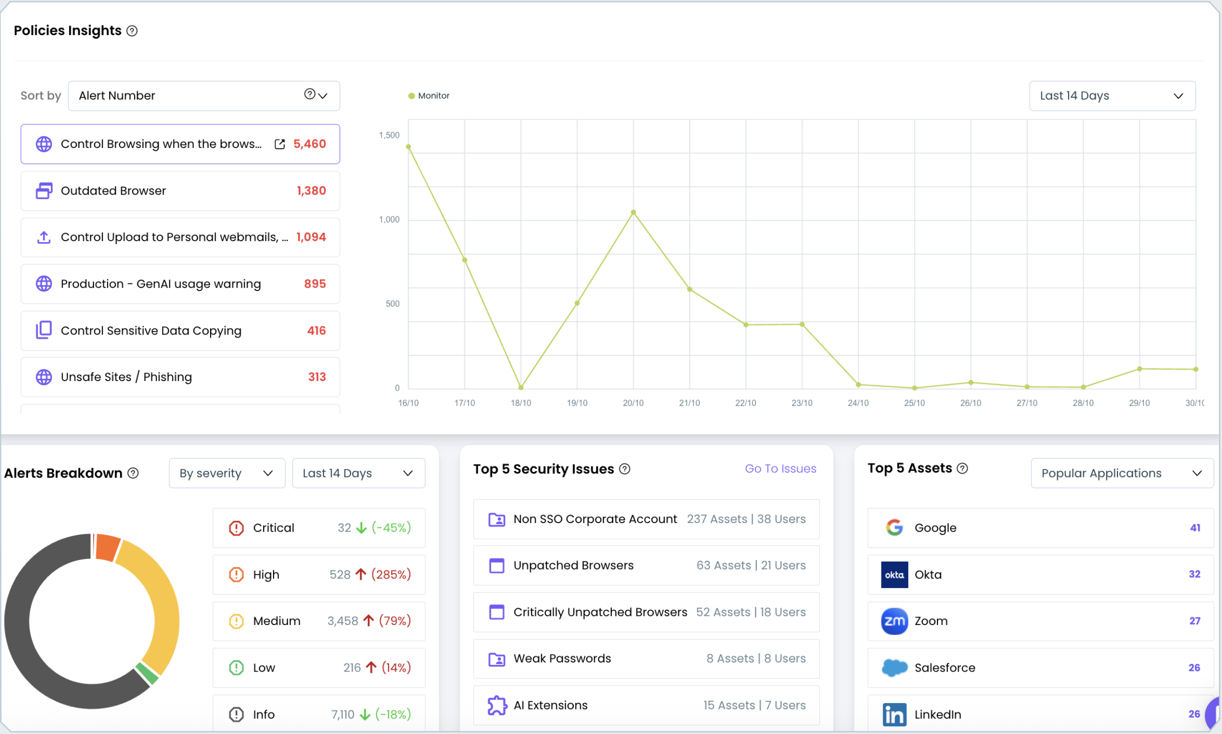
LayerX Solution: Browser-Native Control and Protection

LayerX provided D&B's security team with complete visibility into browser activity, 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.

It also provided visibility into extensions, scripts, and all user actions in the browser. From detecting risky plugins to blocking unauthorized data uploads, LayerX became D&B's **"EDR for the Browser."**

Deployed as a lightweight browser extension, LayerX required no workflow changes. It monitored activity in real-time, classified data contextually, and enforced granular 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.

> *"LayerX is essentially that EDR at the browser level that gives us visibility into what actually happens within the browser by detecting malicious extensions, blocking risky uploads, and stopping data loss before it happens."*
>
> *Jay DePaul (CISO, Dun & Bradstreet)*



Control Browsing when the brows...	5,460
Outdated Browser	1,380
Control Upload to Personal webmails, ...	1,094
Production - GenAI usage warning	895
Control Sensitive Data Copying	416
Unsafe Sites / Phishing	313

Critical	32	↓ (-45%)
High	528	↑ (285%)
Medium	3,458	↑ (79%)
Low	216	↑ (14%)
Info	7,110	↓ (-18%)

Non SSO Corporate Account	237 Assets | 38 Users
Unpatched Browsers	63 Assets | 21 Users
Critically Unpatched Browsers	52 Assets | 18 Users
Weak Passwords	8 Assets | 8 Users
AI Extensions	15 Assets | 7 Users

Google	41
Okta	32
Zoom	27
Salesforce	26
LinkedIn	26

Enabling Safe AI Usage and Preventing Data Leakage to GenAI tools

Challenge: Balancing Innovation and Risk with AI Tools and Preventing Employees from Inadvertently Leaking Sensitive Data to Them

Preventing GenAI data leakage has become an industry-wide problem. The widespread use and convenience of AI-driven tools and AI-powered browsers, and the 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 and use AI tools.

While some organizations block AI altogether, D&B recognized the productivity advantages of AI tools and how they could enable its business to operate more efficiently. D&B wanted a solution to let employees use these tools to boost innovation without risking sensitive data leakage.

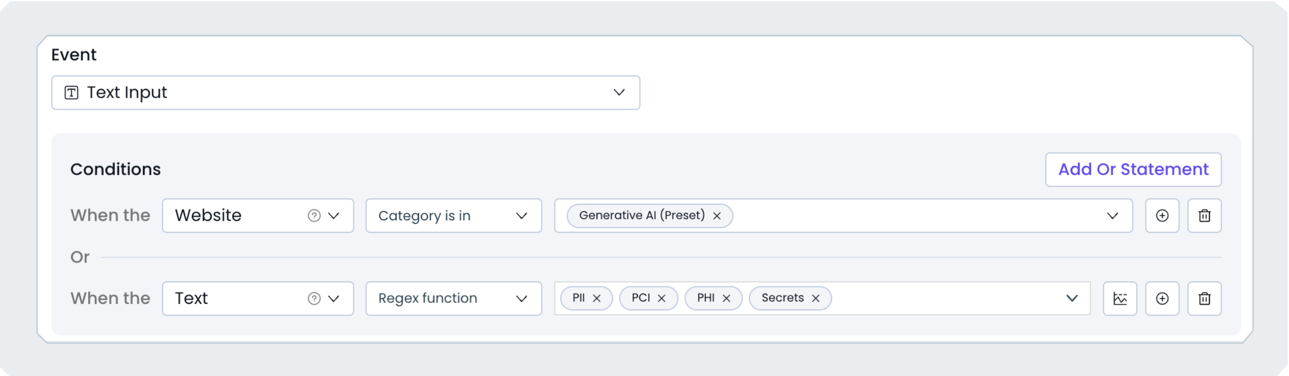
Since the browser is the primary point of access for AI tools, it has become the main channel for both usage and risk. To gain complete control and visibility over AI interactions, D&B needed dedicated browser-based protections that could monitor, analyze, and enforce policies at the exact point where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

LayerX Solution: AI Discovery, Usage Control, and Preventing GenAI Data Leakage

LayerX is deployed directly within the browser, giving it direct visibility and control over all AI 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 unsanctioned 'shadow' AI applications and redirect users to sanctioned ones.

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



Event

Text Input

Conditions

When the Website | Category is in | Generative AI (Preset)

Or

When the Text | Regex function | PII | PCI | PHI | Secrets

Protecting Against Malicious Browser Extensions

Challenge : Allowing Browser Extensions While Blocking the Malicious Ones

Browser extensions have become both powerful and dangerous, often requesting broad permissions that expose organizations to risk. They have also become a key component in attackers' toolkits. Attackers use social engineering or silent sideloading to install malicious extensions that gain full access to browser data, cookies, etc. Once installed, malicious extensions have direct access to all the browser's data and activities, making it possible for the attacker to exfiltrate them at will.

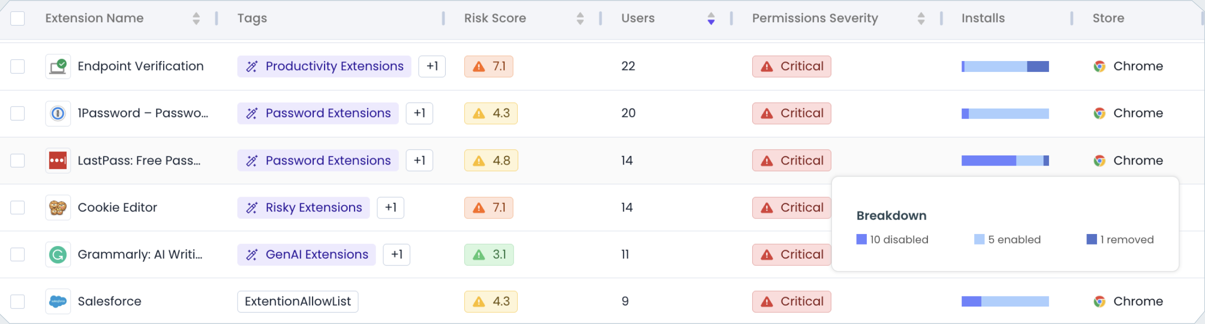
Existing tools offer little visibility into extension activity and rely on manual blocklists, making it difficult to detect threats in real-time. For D&B, detecting and managing these extensions whitelists at scale had been historically difficult and resource-intensive. As an “open” organization that is attuned to its employees, D&B did not want to block all extensions. This is why D&B was looking for automated processes that allowed safe, productivity-boosting extensions, while blocking malicious ones.

LayerX Solution: Automated Detection, Risk Scoring and Disablement of Malicious Extensions

LayerX has full visibility into all the extensions that reside on the browser. It identifies risky browser extensions using a comprehensive risk scoring approach that combines risk factors such as permission scope and extension reputation.

The D&B team used this capability to manage employee use of browser extensions across the organization. They configured policies that alerted whenever an extension with high permissions was being installed and disabled any extension that LayerX flagged as critical risk.
Once the policy was configured, LayerX automatically applied it to all the existing extensions, making it very easy for D&B to gain visibility and manage them.

> *“Downloading browser extensions is very common across our organization, but being able to defend against those that are introducing risk has been a historical challenge. Something that an endpoint detection didn't defend against, but with LayerX, managing risky and over-permissioned extensions was a breeze”*
>
> *Jay DePaul (CISO, Dun & Bradstreet)*



□	Extension Name	Tags	Risk Score	Users	Permissions Severity	Installs	Store
□	Endpoint Verification	Productivity Extensions +1	⚠ 7.1	22	⚠ Critical		Chrome
□	1Password – Passwo...	Password Extensions +1	⚠ 4.3	20	⚠ Critical		Chrome
□	LastPass: Free Pass...	Password Extensions +1	⚠ 4.8	14	⚠ Critical		Chrome
□	Cookie Editor	Risky Extensions +1	⚠ 7.1	14	⚠ Critical		
□	Grammarly: AI Writi...	GenAI Extensions +1	⚠ 3.1	11	⚠ Critical		
□	Salesforce	ExtentionAllowList	⚠ 4.3	9	⚠ Critical		Chrome

Breakdown
10 disabled 5 enabled 1 removed

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, which expose D&B’s data and identities to threats invisible to traditional tools. 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.

D&B 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 identities in use across their environment, block unauthorized access, and ensure that only approved, SSO-backed identities could interact with sensitive data.

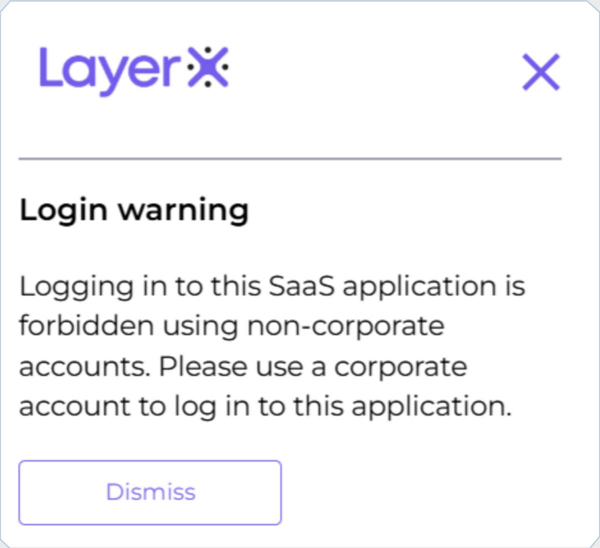
LayerX Solution: Discover Shadow SaaS Identities and Apply Identity Governance

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, D&B was able to discover unmanaged SaaS accounts being used in the browser, whether they were personal accounts or non-federated 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, tracking which identities employees used across SaaS was nearly impossible. Now, we can detect personal logins instantly and enforce identity consistency across all sessions, ensuring data stays within approved boundaries.”*
>
> *Jay DePaul (CISO, Dun & Bradstreet)*



Login warning

Logging in to this SaaS application is forbidden using non-corporate accounts. Please use a corporate account to log in to this application.

Conclusion:
D&B Fortifies its Last Line of Defense with Increased Visibility, Less Disruption, and More Productivity

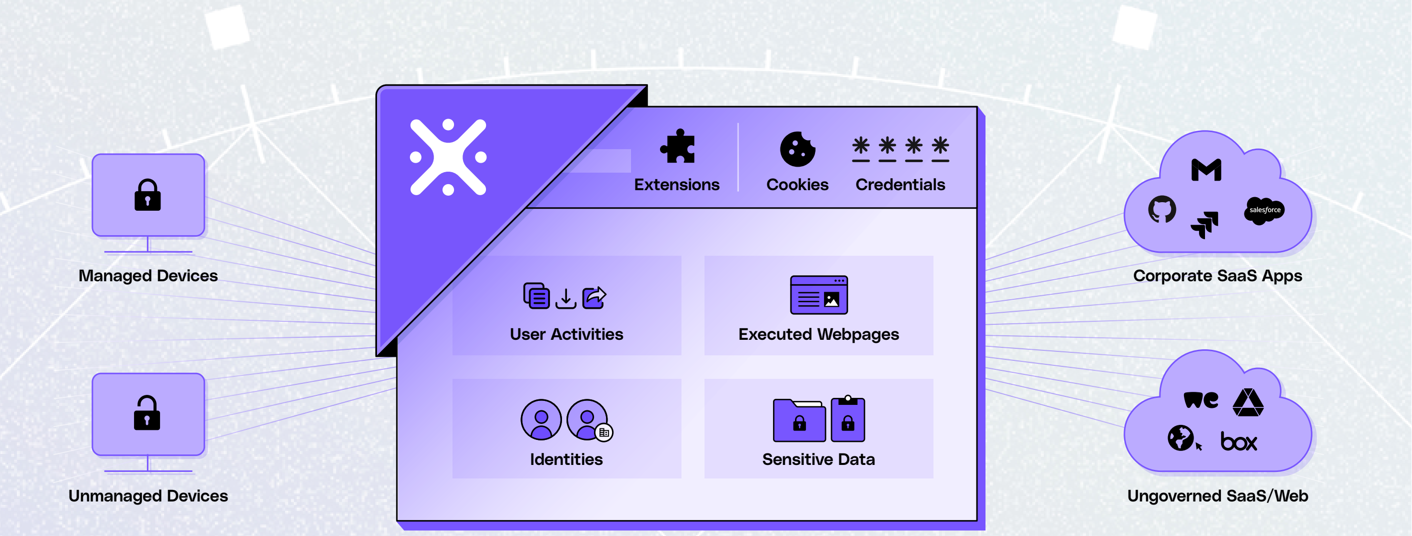
LayerX has become a critical pillar of D&B's security stack, complementing their SASE and endpoint defenses with real-time visibility and control over browser activity, the modern workspace where business happens.

With LayerX, D&B can:

- Protect sensitive data from file-less exfiltration
- Enable safe and productive GenAI exploration
- Govern identity use across SaaS and AI apps
- Defend against malicious extensions and scripts

By embedding browser-native protection into its defense-in-depth strategy, D&B has strengthened its ability to protect data, identities, and innovation without compromising user experience or productivity. 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.

> *"What stood out with LayerX was its ability to strengthen security without slowing anyone down. It protects our data, identities, and AI usage while keeping the employee experience frictionless and management overhead minimal."*
>
> *Jay DePaul (CISO, Dun & Bradstreet)*



One Platform for ALL Browsing Risks and Web-Borne Threats

LayerX

The All-in-One AI & Browser Security Platform

LayerX agentless AI & browser security platform protects enterprises against the most critical AI, SaaS, web and data leakage risks across any browser, application, device and identity, with no impact on user experience

Integrates with All Commercial, AI and Enterprise Browsers

The LayerX Security Platform

Delivered as an Enterprise Browser Extension, LayerX offers the most comprehensive visibility and enforcement capabilities over AI and Browsing risks, including:

AI Usage Security

GenAI DLP
Prevent leakage of sensitive data on AI tools

AI Browsers Protection
Protect AI browsers against attack and exploitation

Shadow AI Discovery
Discover and enforce security guardrails on all AI apps

AI Access Control
Restrict user access to unsanctioned AI tools or accounts

AI Misuse Prevention
Protect against prompt injection, compliance violations, and more

AI Response Validation
Ensure AI response validity and data security

Enterprise Browser Security

Web/SaaS DLP & Insider Threat
Prevent data leakage across all web channels

Browser Extension Management
Detect and block risky browser extensions on any browser

Shadow SaaS & SaaS Security
Discover 'shadow' SaaS and enforce Saas security controls

Safe Browsing
Protect all browsing activity against web exploits

SaaS Identity Protection
Discover and secure corporate and personal SaaS identities

AI Browsers Protection
Protect AI browsers against attack and exploitation

https://layerxsecurity.com | info@layerxsecurity.com