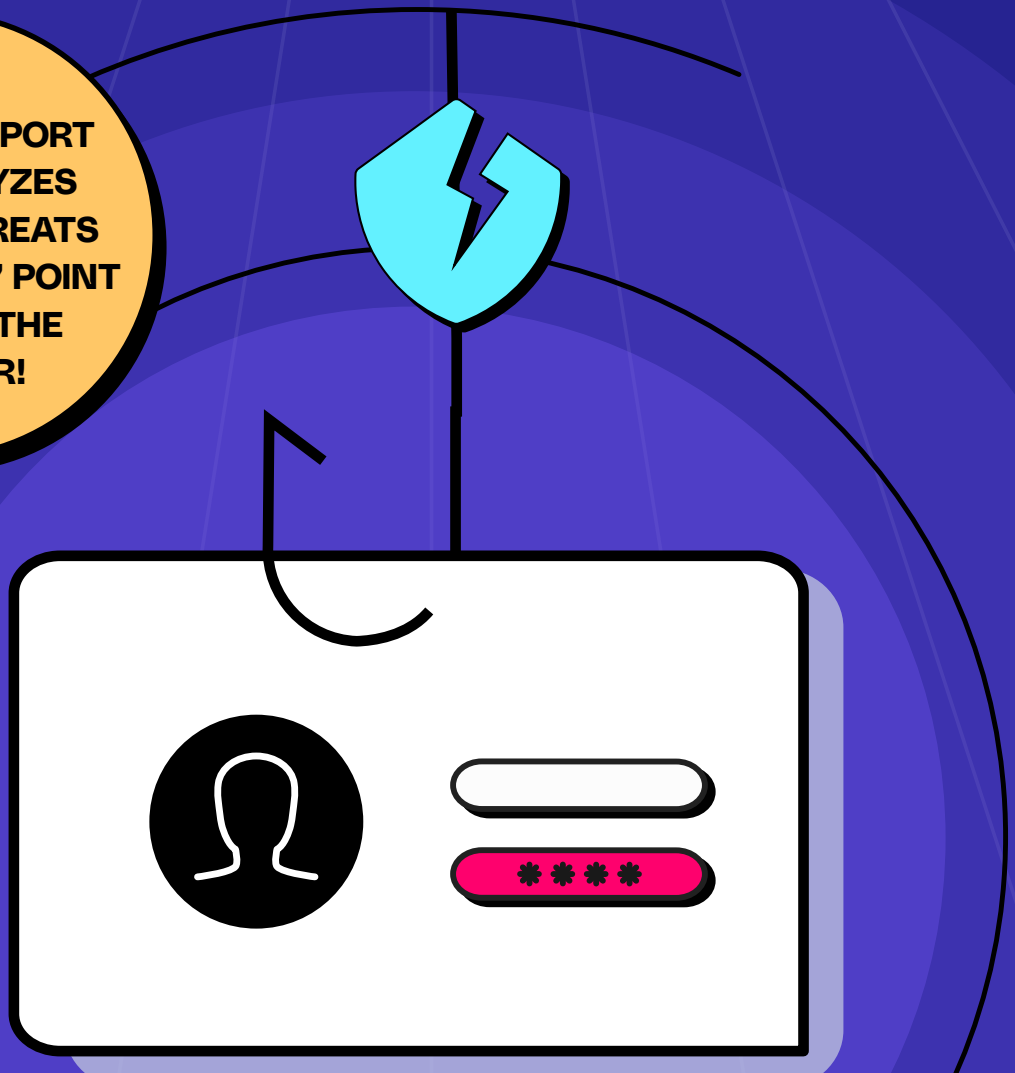
LayerX

Enterprise Identity Threat Report 2024

Understanding the Hidden Threats to Corporate Identities

THE ONLY REPORT THAT ANALYZES IDENTITY THREATS AT THE USERS' POINT OF RISK IN THE BROWSER!



Summary

The corporate identity is the new security perimeter of modern organizations.

In the world of anywhere-work, with most work being done on browser-based SaaS applications, the corporate identity is what stands between keeping organizational data safe, and having it exposed.

As a result, securing enterprise identities a key priority for security managers today.

What Makes This Report Different
(and what data you won't find anywhere else)

The uniqueness of LayerX's data is derived from where we get our data from.

LayerX is an enterprise security platform deployed directly within our customers' browsers.

That means that unlike network-layer solutions, which have visibility only to the high-level session-level data, LayerX has visibility to every user action and activity within the browser, regardless of whether that user is connected to the IdP, using a personal or corporate account, or using a sanctioned or non-sanctioned SaaS application.

As a result, LayerX can see and cross-correlate data across corporate and non-corporate accounts, identify user activity on malicious web pages that get through existing protections, and gain visibility into browser activity that is hidden from network-layer or endpoint protections.

The report herein covers a wide range of identity risks and threats, including:

- The enterprise users most at risk for credential compromise
- Non-corporate and non-SSO 'shadow' identities
- Password and user account security, which can lead to exposure of user accounts
- Evasion techniques attackers employ to evade existing protections
- The risk of browser extensions that have access to sensitive identity data
- And much more...

Key Findings

#1

Just 2% of Users Are Your Biggest Security Risk.
These are users who have a history of identity exposure, do not use SSO-backed passwords, and have weak passwords that can be easily cracked. If cybersecurity is all about risk management, these users are the biggest risk you should worry about.

#2

Enterprises Are Blind to Most Identity Usage.
Over two-thirds of corporate login events are done without SSO. Moreover, over 40% of SaaS applications in organizational networks are accessed via personal credentials. This means security and IT teams are blind to usage of these accounts, and have little-to-no visibility and control over their activities, or where they are used.

#3

Corporate Passwords are Just as Weak as Personal Passwords.
Over 54% of corporate passwords are classified as medium-strength or below, meaning modern password-cracking tools and hardware could easily break them.

#4

Legacy Cloud Security Tools are Routinely Bypassed by 0-Hour Evasion Techniques
Attackers have adapted to the standard protection techniques of traditional cloud-based security tools, and use various evasion techniques to bypass it. Nearly 50% of malicious web pages that successfully bypass existing protections are hosted on public hosting services, and 70% scored 'medium' or lower on phishing-kit similarity scores of known malicious web pages.

#5

Browser Extensions are a Significant Threat to Users' Identity
66.6% of extensions have 'high' or 'critical' -level permissions and 40% of users have such extensions installed. 13% of extensions have access to users' cookies, meaning they could potentially use those cookies and access tokens to steal corporate identities.

The Bottom Line: Measuring Exposure

> About 2% of Users Are Your Biggest Risk; Do You Know Who They Are?

19.3%

Of corporate users, based on a random sample, appeared in public data breaches

9.3%

Of corporate users have been exposed in a public data breach *which included password exposure*

1.8%

The proportion of enterprise users who appeared in a data breach with password exposure, AND do not use SSO, AND use weak passwords

5.9

Average number of data sets in-which an exposed corporate identity appeared in

9.5

Average number of data sets in-which an exposed corporate identity appeared in, of users who appeared in data breaches that included password exposure

The Finding

About 1.8% of corporate users make up the group who are most at risk for identity compromise.

These are enterprise users who have appeared in public data breaches that *included password exposure*, do not use SSO-backed authentication for their corporate accounts, and have weak passwords that modern tools can easily crack.

Nearly one in five corporate users has appeared in a public data breach. However, not all data leaks are created equal: while most contain Personally Identifiable Information (PII) of some sorts, not all of them include account passwords (whether encrypted or not).

When looking only at incidents with password exposure, just under 10% of corporate users appeared in such a breach.

However, closer examination shows that these users tend to be much more at risk: whereas users who appeared in a data leak appeared, on average, in 5.9 different breaches, users who appeared in leaks *with passwords* appeared in 9.5 incidents.

While the data provides no explanation for this phenomenon, it does indicate that users who have had their password exposed are at a significantly higher risk.

Why It Matters

Cybersecurity is all about risk management. In today's complex environment, covering every attack vector in every instance is virtually impossible, even for the largest and best-funded organizations.

The key, therefore, is to manage risk and identify the users and factors that put your organization most at risk – and concentrate on mitigating those risk factors.

The following pages expand on the top risk identity risk factors identified by LayerX, and why they are important.

Risk Factor #1: Shadow Identities

> Organizations Have No Visibility to Most SaaS Identities

67.5%

Of login events using corporate accounts are done not using SSO

42.5%

Of logins to SaaS applications by organizational users are done using non-corporate accounts

The Finding

Single Sign-On (SSO) is one of the most effective ways of guaranteeing corporate identity security. Not only is it frequently combined with other forms of authorization and authentication, such as Multi-Factor Authentication (MFA), but it also enables organizations to see exactly where their corporate identities are being used.

The findings, however, show that SSO-backed corporate logins are not used in most connections within organizations, even ones for corporate SaaS applications.

Of logins using the corporate account, two-thirds (67.5%) are done using passwords, and not SSO-backed authentication. Moreover, nearly half (42.5%) of total logins to SaaS applications within the organizational network are done using *non-corporate* credentials, such as the user's personal email accounts.

This means that organizations have no visibility to most applications and instances where their corporate credentials are being used.

Why It Matters

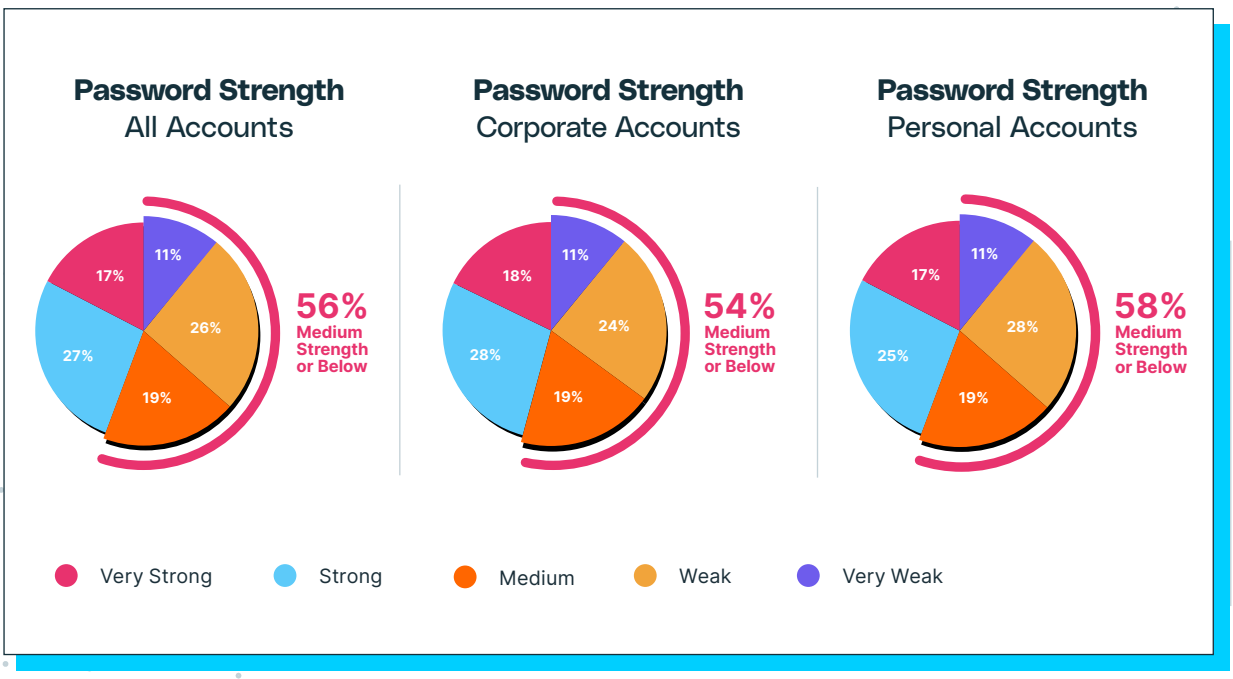
The first step to securing your identity perimeter is to identify it. But how can organizations be expected to protect exposure that they don't know about?

Shadow identities put corporate accounts at risk since they increase the risk to identities (by not being backed by SSO/MFA) while simultaneously leaving organizations blindsided since they have no idea where these identities are being used.

Therefore, eliminating shadow identities is a big first step for organizations to map out and narrow down their threat surface.

Risk Factor #2: Bad Passwords

> Corporate Passwords Are Just as Weak as Personal Ones



The Finding

You would think that corporate passwords tend to be stronger than passwords of personal accounts. If so, you would be wrong.

Over half of all passwords are categorized as medium-strength or below. While "medium" might not necessarily sound bad, such passwords can typically be broken in under 30 minutes by password-cracking software running on servers with current high-end processes.

Although there is a misconception that corporate passwords are stronger than personal ones due to password governance policies, the data shows that there isn't a significant difference between personal and organizational passwords: 58% of personal passwords are medium-strength or below, whereas 54% of corporate accounts use passwords of medium strength or under.

The internal breakdown is also remarkably similar, with 11% of passwords classified as 'very weak' and 19% of passwords assessed as 'medium' for both categories. Passwords for corporate accounts have a slight edge over personal accounts passwords when it comes to 'strong' (28% vs. 25%) and 'very strong' passwords (18% vs. 17%), but those differences are fairly minor on the whole.

Why It Matters

Passwords are the cornerstone of cyber security and the primary means of protecting most user accounts and identities.

Any password security system worth its salt (pun intended) encrypts passwords using hashes. In most cases, when passwords are exposed in a data breach, what is actually exposed are not the plaintext passwords themselves, but their encrypted hashes.

Nonetheless, these hashes can be broken through brute-forcing and dictionary attacks, and password-breaking software can easily be found online. This is why a strong password is essential, to prevent it from being easily broken by such techniques.

However, the prevalence of weak and medium-strength passwords – even on corporate accounts – means that most hashes can be easily broken by modern password-cracking software and hardware. If such passwords were to be exposed in a data breach, hackers would have an easy time using these passwords to access organizational resources.

This is especially true since – as we saw in the findings on previous pages – most organizational identities are protected by passwords, and not by SSO/MFA.

The implication is that organizations need to strengthen their password security rules to make sure that their organizational accounts are protected against such attacks.

Risk Factor #3: Password Re-Use

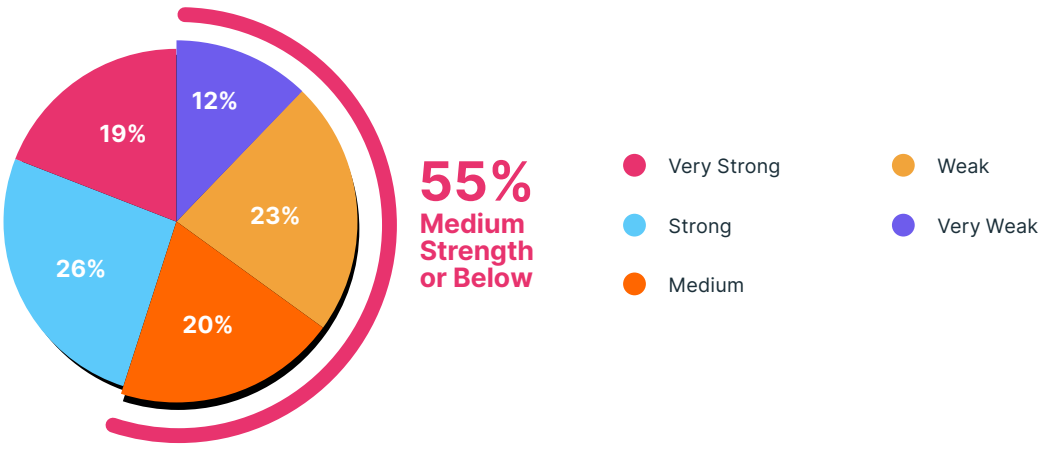
Password Re-Use is Rampant in Corporate Environments

26%
Of enterprise users re-use passwords on multiple accounts

15%
Of corporate accounts use a re-used password

55%
Of re-used passwords are medium-strength or below

Password Strength - Re-Used Passwords



The Finding

One in four enterprise users re-uses passwords across multiple personal and corporate accounts. Moreover, about one in six corporate accounts uses a password that was re-used in a different account.

Approximately 55% of re-used passwords are medium-strength or less. These findings are in line with general findings on password strength in corporate environments (see previous findings).

Why It Matters

Hackers count on password re-use to break into user accounts. When users re-use passwords on multiple accounts, if any of those accounts gets exposed, then all of the other accounts which use the same passwords are exposed, as well.

Hackers routinely employ credential-stuffing attacks where they try multiple passwords known to be associated with the same user, in the hopes that one of these passwords will be re-used in the account the are targeting. This risk is even greater in corporate environments, where re-use of passwords from less-protected personal accounts can lead to breach of the organizational network.

This is why preventing password re-use is crucial, particularly in corporate accounts.

Risk Factor #4: Shared Accounts

Organizational Users Routinely Share Corporate Accounts

2.68%

Of all logins on corporate accounts are shared

45%

Of all logins on shared accounts are on corporate accounts

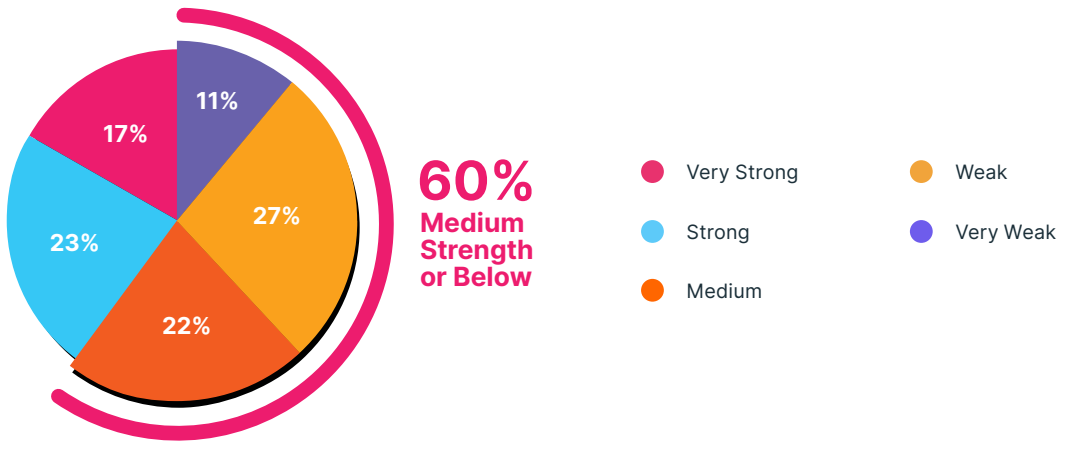
2.2

Average number of shared accounts per user

13.27

Average number of shared accounts for the top 5% of 'heaviest' account-sharing users

Password Strength – Shared Accounts



The Finding

Account sharing is frequently practiced in corporate environments. The data shows that 2.68% of corporate accounts are shared among multiple users. While this number may not seem high of itself, in an organization with 1,000 active users, it means they have nearly 30 shared accounts.

Moreover, corporate accounts account for nearly half of *all* shared accounts, showing that this is hardly a practice limited to personal accounts.

Corporate users have, on average, access to 2.2 shared accounts, and the top 5% of the 'heaviest' account-sharing users have – on average – more than 13 shared accounts.

The passwords used to secure shared accounts seem to be even weaker than average, with 60% of shared account passwords classified as medium-strength or below, compared to an average of 54% of all corporate accounts that have such passwords.

Why It Matters

Shared accounts are a major source of risk for organizations. Sharing a corporate account among several users typically leads to lower security controls for that account:

- By definition, shared accounts are not backed in SSO/MFA, since not all users will have access to those. So these are typically turned off for shared account
- Shared account passwords tend to be weaker, to make it easier for multiple users to remember them. This makes them more vulnerable.
- With shared accounts it is very difficult to establish accountability and understand which user did what action, creating security blind spots.

Account sharing is also forbidden by numerous compliance standards, meaning that organizations that don't restrict account sharing are exposing themselves both to security and compliance violations.

Risk Factor #5: Failing to Stop Attacks from the Outside

Attackers Have Learned to Bypass Traditional Phishing Protections

49.6%

Of successful malicious web pages are hosted on legitimate public hosting providers

54%

Of successful malicious web pages had ‘low’ top-level domain (TLD) risk

82%

Of successful malicious pages had ‘high’ reputation risk

70%

Of successful malicious pages had ‘low’ or ‘medium’ phishing-kit similarity

The Finding

Phishing and credential compromise continue to be the leading causes for data breaches today. According to the IBM *Cost of Data Breach Report* 2024, these attack vectors are responsible for 31% of all data breaches, and lead to an average cost of over $4.7 million per incident.

Traditionally, organizations have relied on Secure Web Gateways (SWG) and Cyber Threat Intelligence (CTI) services for protection against malicious attacks by filtering known malicious attacks and attack sources. Such tools are still the foundation of many Security Service Edge (SSE) offerings.

The data, however, shows the increasing ineffectiveness of these tools against modern attackers, who have learned to circumvent these defenses.

One key approach used by attackers is to ‘piggyback’ on-top of known, legitimate hosting services. Since SWG and CTI solutions typically assess risk by evaluating the reputation of the top-level-domain (TLD) of the URL, using public hosting services virtually assures that the page will pass inspection by SWGs. Indeed, the data shows that almost 50% of malicious web pages that pass traditional defenses were hosted on public hosting providers, and over 54% had ‘low’ TLD risk.

Another approach by hackers is to use pre-packaged phishing-kits, but to implement slight changes to them. As a result, they will not be recognized by legacy protections, and allowed to go through.

LayerX data shows that 70% of successful malicious URLs scored a ‘low’ or ‘medium’ on phishing-kit similarity scores. However, of these, only 2.6% scored a ‘low’ on phishing-kit similarity, meaning that only a very small percentage was new and not based on an existing page template. The vast majority of (67.5% of total) were rated as a ‘medium,’ meaning that the changes made were relatively minor, but enough to get by. More alarming is the fact that 27.4% of post-inspected pages scored ‘high’ on phishing-kit similarity, meaning that defenses were either outdated or not using these metrics at all.

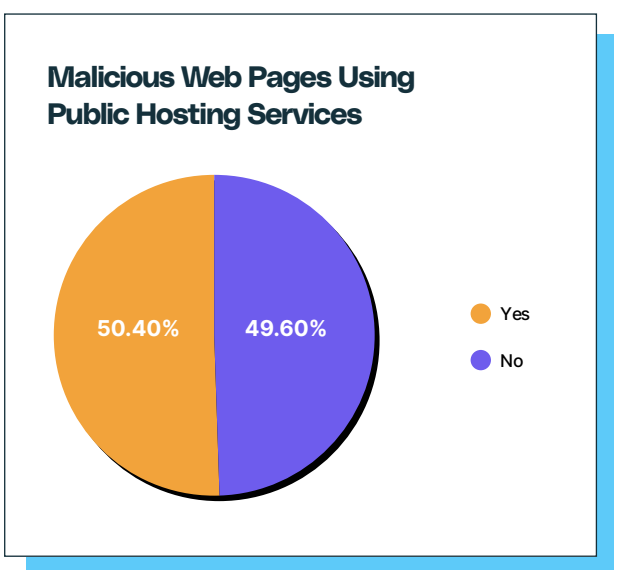
Finally, the data shows that 82% of pages that passed inspected by legacy security tools had ‘high’ reputation risk. This is a very alarming finding indicating that existing web protections are overly-reliant on filtering pages according to the top level domain, and do not adequately filter malicious websites.

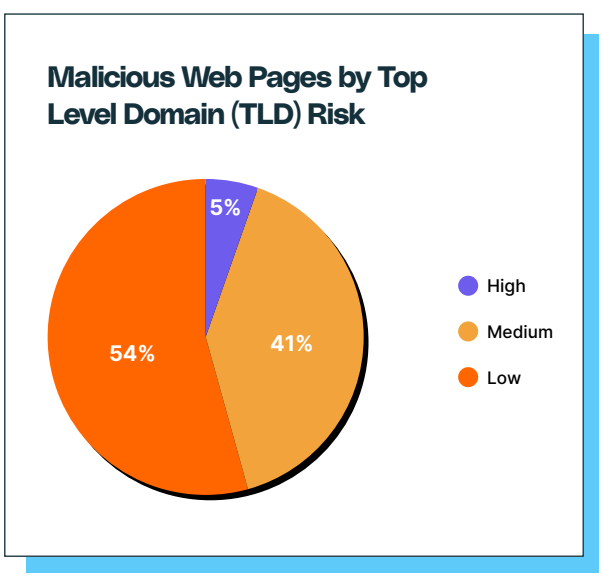
Why It Matters

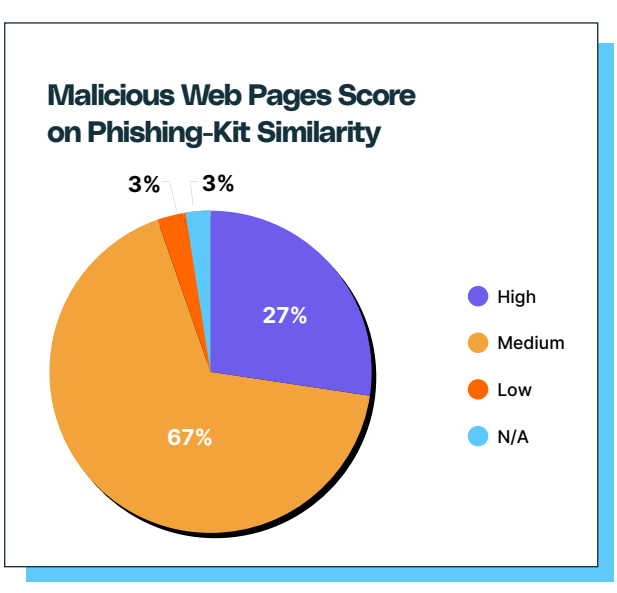
Many organizations and security professionals regard safe browsing as a solved risk. With multiple guardrails deployed on the network, endpoint, and provided by commercial browsers, many practitioners believe that they are covered.

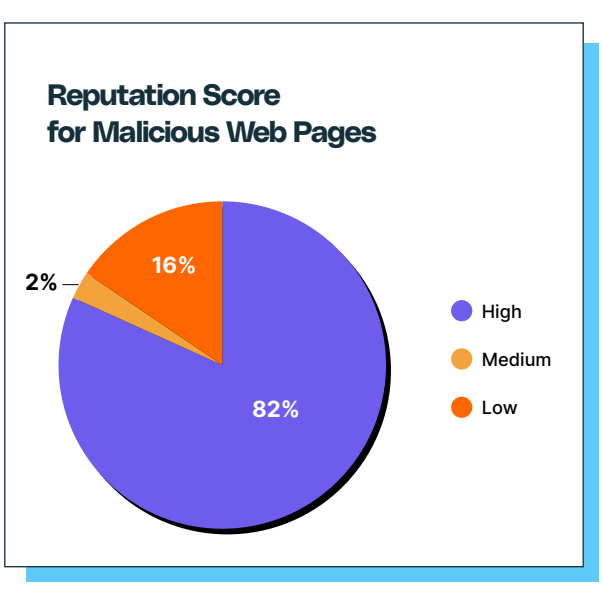
Legacy web protections primarily on lists of known bad URLs and signatures of malicious web pages. However, as the data shows, a new generation of web attackers has learned to adapt to traditional security techniques and employ a multitude of evasion techniques to circumvent them.

The implication for organizations is that they have to move beyond the traditional approach to web security, to a more adaptive and sophisticated approach that is not as reliant on known bad actors, and can block such attacks in real-time.









Risk Factor #6: The Unknown Threat Within

Malicious Browser Extensions Can Steal Corporate Identities

66.6%
Of extensions installed in organizational networks have ‘High’ or ‘Critical’ risk permissions

40.2%
Of organizational users have extensions installed on their computers that have ‘High’ or ‘Critical’ risk permissions

13%
Of browser extensions installed in corporate environments had access to users’ cookies

5.6%
Of corporate users installed browser extensions that could access their cookies

4%
Of browser extensions installed in corporate environments had access to users’ identity

7.73%
Of corporate users installed browser extensions that could access their identity

The Finding

Browser extensions are ubiquitous among web browser users today. The Chrome Extensions store has over 250,000 extensions, and leading extensions have over 10 million downloads each.

However, LayerX data shows that two-thirds of extensions installed on the browsers of corporate users have ‘high’ or ‘critical’ risk permission scores and over 40% of corporate users installed browser extensions with ‘high’ or ‘critical’ risk permissions. Worse still, ‘critical’ -level permissions make-up the majority of these finds both among extensions (44%) and users (26%).

Looking at individual permissions, the data shows that 13% of browser extensions installed in corporate environments have access to users’ cookies, and 4% of extensions have access to users’ identities.

On the user side, nearly 8% of enterprise users installed browser extensions that access their identities, and almost 6% of corporate users have extensions that access their browser cookies.

Why It Matters

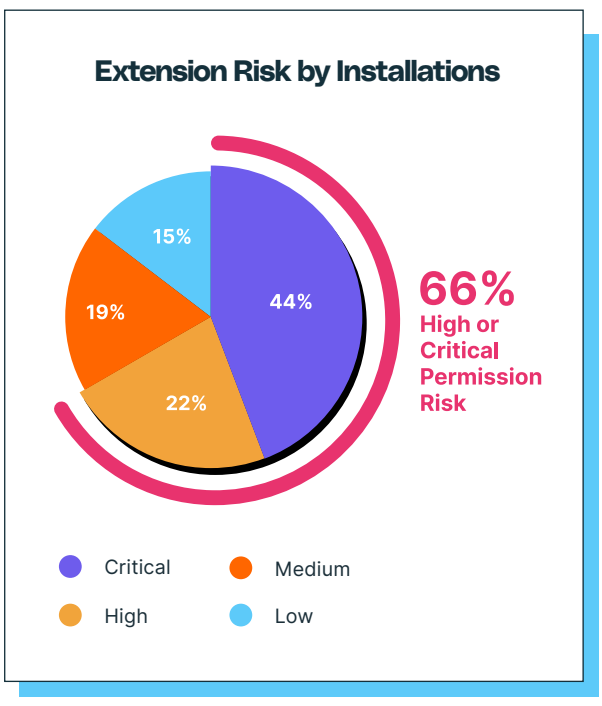
Browser extensions are the biggest organizational security threat that CISOs don’t know about.

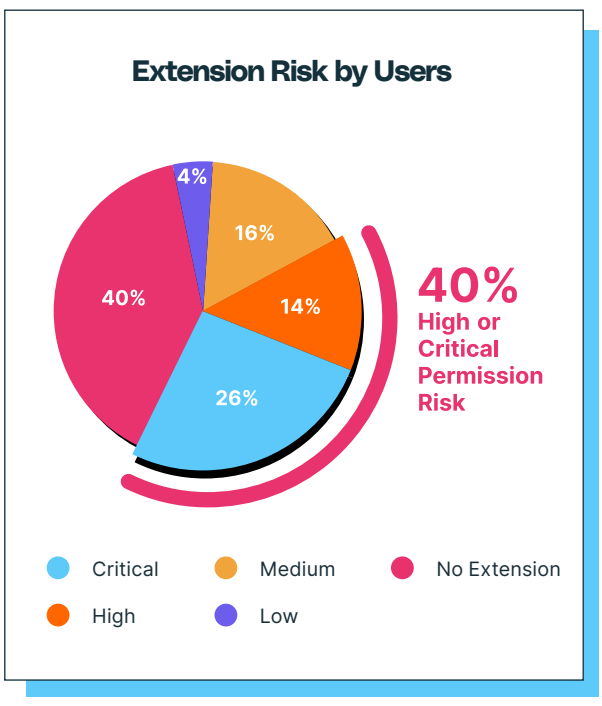
While most browser extensions are perfectly benign and help users fix their spelling or find discount coupons, they are also routinely granted extensive access permissions to key data such as cookies, identities, passwords and browsing information.

However, malicious browser extensions can exploit these permissions to steal users’ cookies, session tokens, identities and browser data, in order to steal their identities and data.

This risk is compounded in corporate environments, where exposure of corporate credentials of one user can lead to a breach that affects the entire organization.

These findings indicate that browser extensions are a significant point of risk in corporate environments, and merit dedicated protection to make sure they are not exploited.





Summary

Would you buy a car whose breaks work only 40% of the time?

Enterprise security teams have long recognized identity compromise as one of the key risks to protect against.

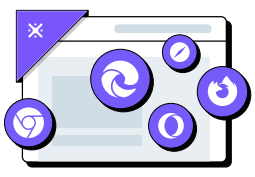
To that end, organizations deploy a myriad of security measures designed to protect corporate identities, ranging from anti-phishing protections to Identity and Access Management (IAM) solutions to enforcing governance on their Identity Provider (IdP) solution.

> The challenge, however, is that many users completely circumvent these protections by using shadow identities in the form of corporate identities not backed by SSO or altogether forgoing corporate identity protections by using their own personal accounts.

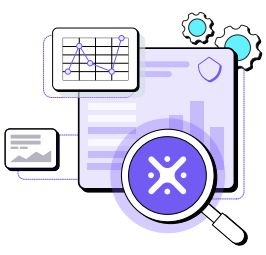
Moreover, we also see the limits of existing protections in the form of high percentages of malicious web pages that get through traditional web and email security gateways, and the high prevalence of risky browser extensions installed within users' browsers, which are not covered by existing protections.

These findings call for a new approach to identity security that enforces security governance and control at the last mile – where users are using their identities and where they are most at risk.

How LayerX Helps Address Identity Security

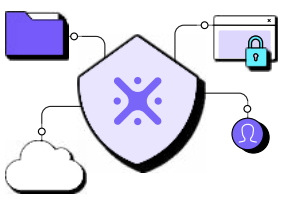


LayerX Enterprise Browser Extension natively integrates with any browser, turning it into the most secure and manageable workspace.

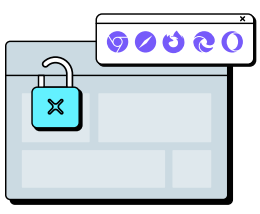


LayerX is the first solution that rises up to the challenge of securing the most targeted and exposed attack surface today - the browser, without impacting the user experience. LayerX delivers comprehensive protection for all browser-based threats with continuous monitoring, risk analysis, and real-time enforcement on any event and user activity in the browsing session.

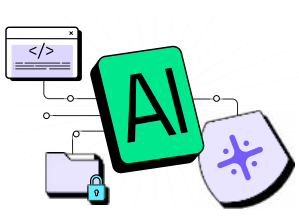
Enterprises leverage these capabilities to secure their devices, identities, data, and SaaS apps from identity threats and risks that traditional endpoint and network solutions can’t protect against.



These include blocking data leakage over the web, SaaS apps and GenAI tools, prevention of credential theft from phishing, enforcement of secure access to SaaS resources by the internal or external workforce to mitigate the risk of account takeover, discovery and disablement of malicious browser extensions, Shadow SaaS, and more.



The LayerX enterprise-designed architecture enables seamless scalability as it doesn’t require agents or proxies and natively integrates with any browser. As a browser extension, LayerX delivers 100% coverage to any browser session, with no blind spots to its threat prevention, DLP, and secure access capabilities. In a similar manner, it ensures full visibility into every installed browser extension and into user activities.



LayerX risk applies its analysis and enforcement to every event within the browsing session, such as web page components and user activities, providing granular enforcement that disables malicious activity without obstructing user experience. This AI-based analysis takes place autonomously on the edge device with zero impact on network speed and no dependency on connectivity to a management server. Additionally, as part of the browser, LayerX extension is resilient to malware-based tampering or user modification.

The ease of deployment and wide protection coverage make LayerX the ultimate choice to secure the browser and all the resources it accesses.