NordLayer®

NordLayer research, in partnership with
NordLayer Intelligence by NordStellar

2026

A Fortune 500 credential leaks every 100 seconds

What nearly **10 million exposed logins** mean for enterprise security

Table of contents

1. The scale of the exposure

9.96 M

unique Fortune 500 **employee credentials** (email and password pairs) leaked on the dark web

99%

of records **harvested by infostealers** in 2026 were taken from web browsers

130,000

credentials leaked in roughly 147 days of 2026 alone

Every 100 seconds

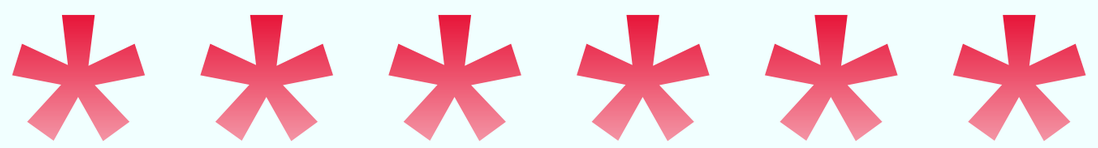
a Fortune 500 **credential appeared** on the dark web in 2026

6.6M

unique **corporate email addresses** have leaked across all available historical data

[1] 9.96 million email and password pairs came from 6.6 million distinct email addresses, so many addresses appear more than once with different passwords.

2. How we measured Fortune 500 credential exposure



The biggest companies in the United States collectively employ about **31 million people** worldwide. They hold sensitive data relating to hundreds of millions of people and operate systems classified as critical infrastructure. Despite spending billions of dollars on cybersecurity each year, large US companies have millions of employee credentials available on the dark web, where a stolen corporate login can sell for around $10.

> Credential leaks are widely reported as individual incidents, but no public research has measured the full scale of this exposure across America's 500 largest companies at once.

In partnership with NordLayer Intelligence by NordStellar, NordLayer analyzed leaked credentials tied to the domains of **Fortune 500**—an annual ranking of the 500 largest companies in the United States by total revenue, published by Fortune magazine.

The 2026 list spans **20 industries** and includes companies such as Amazon, Walmart, Apple, UnitedHealth Group, and JPMorgan Chase. Subsidiary brands, such as AWS, YouTube, or Instagram, were not included in the research.

> The companies above are named for context, not because they are more or less exposed than the other companies on the list. The research covers all 500 companies in the 2026 Fortune 500 list, and this report does not highlight any individual company's results.

We collected almost **35 million raw records** which were deduplicated down to **9.96 million** unique email and password pairs. To compare exposure by company size and by sector, each company was then matched to its industry, revenue, and employee count.

The data comes from **2 source types:**

1 Infostealer logs,

which come from individual malware infections, carry a collection date and information about the application and site the login was used on.

2 Combolists

are text files containing email and password pairs that criminals assemble from many older leaks and reshare over time, with no date attached.

Of the 34.86 million raw records tied to Fortune 500 domains, 13% are info-stealer logs, and 87% are combolists. Only the infostealer records can be placed on a timeline.

Any year-by-year figure in this report is based on the 13% of records that are infostealer log. Totals include both source types.

Combolist records carry no date, but they stay in circulation indefinitely, get reshared and resold, and are still tested against corporate logins years after the original breach. Excluding them would leave out 87% of the data and understate how many Fortune 500 addresses attackers can reach.

Not every leaked credential is a live risk. When an employee leaves and their account is properly closed, the leaked login no longer opens anything.

The risk is that offboarding is often incomplete, and dormant accounts stay active long after the person has gone. This research cannot tell which accounts are still valid, so the totals show accumulated exposure rather than a count of working logins.

3. Leaked credentials are a business problem

Just one working login can be enough to steal company data or launch a ransomware attack. But many stolen business logins never come from a work computer.

Infostealer malware is a type of malicious software that steals saved passwords and other credentials from a device. It often infiltrates personal devices like smartphones through pirated software or content, gaming files, fake ads, or phishing messages.

1 Infection

A victim downloads an infostealer without realizing it. The malware reaches the browser and copies every login saved there, including personal and work accounts in seconds.

2 Sale

Cybercriminals who operate infostealers rarely use the stolen logins themselves. Instead, they offer them for sale on the dark web, where they are sold in bulk **at low prices** on forums, marketplaces, and Telegram channels. Nearly 10 million Fortune 500 employee credentials are already available.

3 Testing

Buyers upload extensive lists of stolen credentials into automated tools that test each email-and-password combination against company login pages at once. With these tools, a single attacker can check thousands of logins without any special skill.

4 Access

When a combination works, the attacker gets into the organization's systems. The effort to reach this point is low, but the potential damage to an enterprise is enormous.

With 6.6 million corporate email addresses in circulation, large organizations should assess how many of their employees credentials are already on the dark web and what those logins can still reach.

TL;DR

Infostealers copy saved passwords from browsers and feed them into a supply chain that culminates in automated attempts to break into corporate systems. **There are already nearly 10 million stolen Fortune 500 credentials in circulation, each of which is a potential entry point.**

4. Company size does not predict exposure rate

All figures in this section come from infostealer records dated within the first 147 days of 2026. These figures illustrate the number of new credentials that appeared during that period, not the full amount of exposure a company carries. Based on all available data, including undated records from years prior, almost every company on the Fortune 500 has leaked credentials.

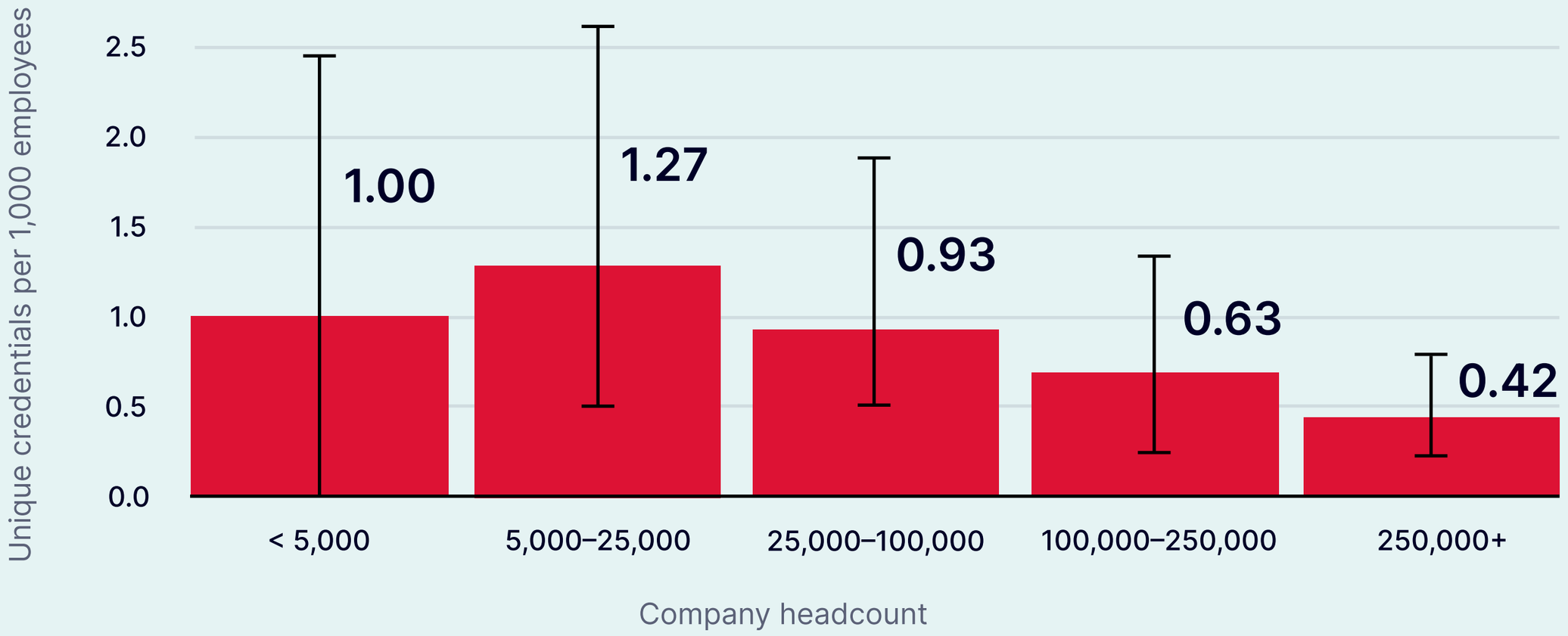
People often think that the bigger an organization is, the more frequently it is targeted by cybercriminals.

Larger organizations do have a larger attack surface, with more devices, more suppliers, more sensitive data, and more public visibility. A successful breach at a major company may also produce a larger payoff, so very large businesses attract targeted attacks from ransomware groups, state-backed actors, and other well-resourced adversaries.

However, infostealer infections are automated and opportunistic. A company's rate is determined not by its size, but by how many of its employees work on a computer with a corporate account.

Median credential leakage rate by company size

(bars = median, whiskers =25th—75th percentile)



The highest individual rates come from midsize technology companies none of which are among the largest employers on the list. What they share is a workforce in which nearly every employee holds a corporate email account and saves logins in a browser.

During this period, companies without credentials cluster in smaller bands. **There are 8 in the smallest band, 14 in the 5,000–25,000 band, 1 between 25,000 and 100,000, and none above 100,000.** This may be because a company of 3,000 people will generate few infections in 5 months, so landing at 0 is a realistic outcome.

However, a company of 300,000 will record infections almost regardless of how it is run. Across the full dataset, including undated records, almost none of the Fortune 500 companies are clean.

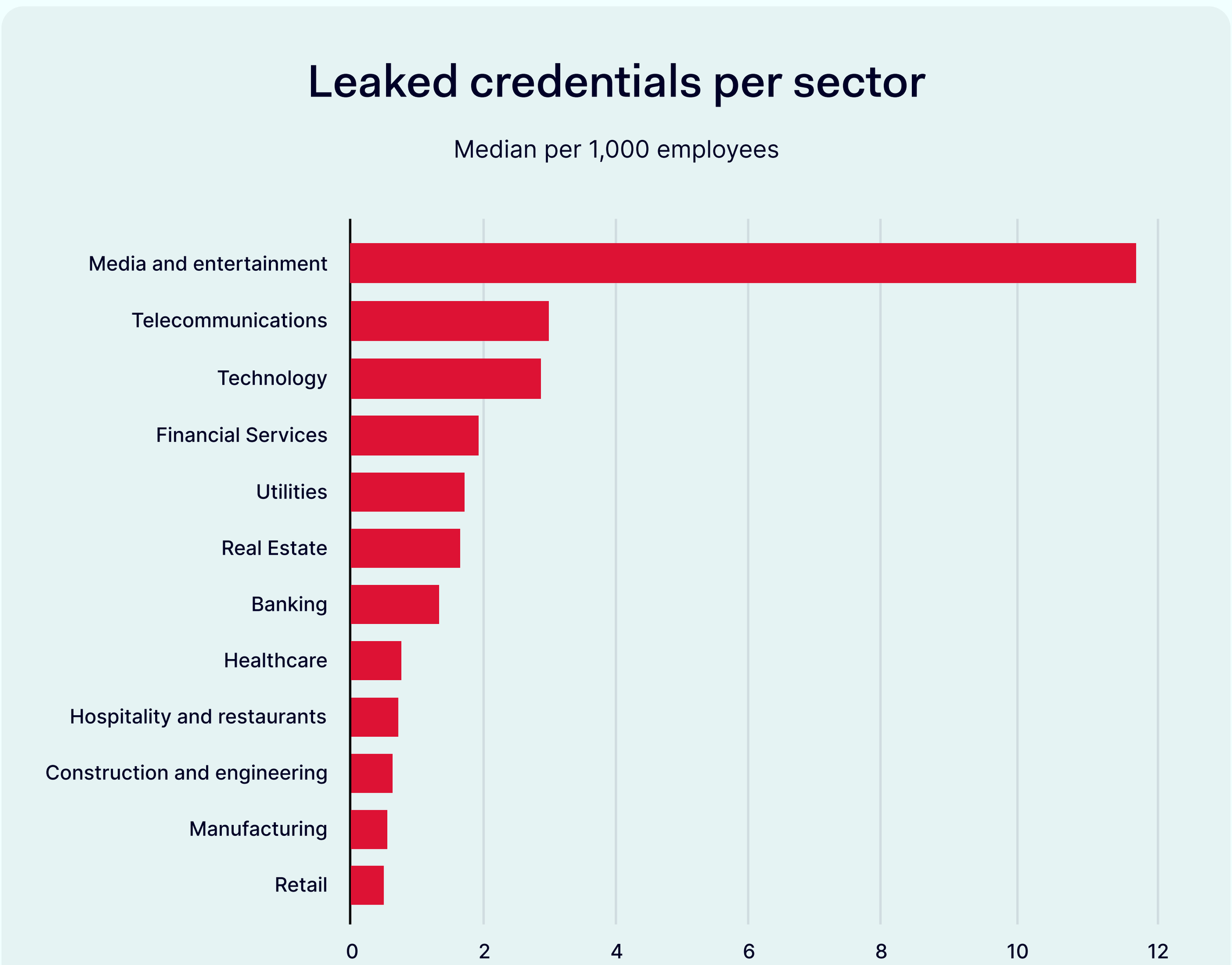
Workforce composition explains most of what the numbers show. When nearly every employee has a corporate account and a browser, rates run high. However, where much of the workforce is frontline, warehouse, or store staff who never receive a corporate email address, rates run low, because the denominator includes people who cannot be exposed this way.

TL;DR

Over 147 days of 2026, midsized technology companies had the highest per-employee rates, reaching came 42 credentials per 1,000 employees. Company size predicts how many credentials appear, but not how concentrated the exposure is. Companies that recorded no credentials during this period are small enough that few infections would be expected in 5 months.

5. Exposure rates are more indicative of desk work than industry

The research grouped the Fortune 500 companies into 20 industries and compared credentials per 1,000 employees. The median rates range from 10.59 at the top to 0.51 at the bottom, but the ranking measures workforce composition more than it measures security.



As headcount rises, the total number of credentials goes up (rank correlation +0.55) while the rate per 1,000 employees goes down (-0.20). Large companies record more credentials in total and fewer per employee.

This shapes the bottom of the ranking. The lowest rates belong to retail, hospitality, logistics, and manufacturing, where most staff work in stores, warehouses, restaurants, or on production lines. A cashier or a warehouse picker has no corporate login to lose.

The top of the ranking has the reverse profile. Media and entertainment, telecommunications, technology, and financial services are sectors where close to every employee has a corporate account, device, and browser.

Sector differences hold at every company size. Among companies with 25,000 to 100,000 employees, the median is 3.23 in technology, 0.68 in retail, and 0.54 in manufacturing. Among companies with more than 100,000 employees, the median is 1.22 for technology and 0.26 for retail. Rates fall as companies get larger in every sector, but the gap between sectors stays at 5 to 6 times.

Midsized companies show the highest individual rates. The 5,000 to 25,000 employee band has the highest median, at 1.27 per 1,000, and the widest range, with the middle 50% of companies between 0.48 and 2.60.

These companies have both a high percentage of desk workers and a small number of employees, so individual firms appear near the top of the ranking even when their sector's median is low. Insurance is an example of this. Its companies have a median headcount of 12,300 and several rank among the highest-rate firms, but the sector median is only 0.87.

Neither end of the ranking indicates security quality. The largest retailers rank near the bottom in terms of rate, yet they have more exposed credentials in absolute terms than most companies at the top. Where an organization falls on this measure indicates how concentrated its exposure is likely to be among its people, not how well it is defended.

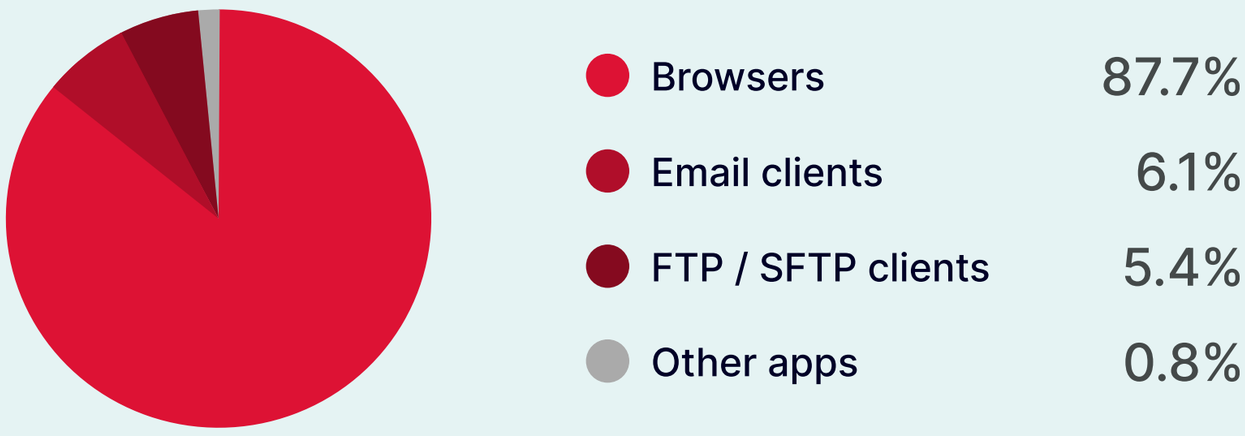
TL;DR

Media and entertainment, telecommunications, technology, and financial services industries have the highest credential rates per 1,000 employees, while retail, manufacturing, hospitality, and logistics have the lowest. This trend persists when controlling for company size, with technology companies having rates 5 to 6 times higher than retail companies in the same size band. The dividing line is the percentage of staff who work on a computer with a corporate login. Large employers have more credentials in total but fewer per employee, so a low rate reflects a large non-desk workforce rather than stronger security.

6. Why the browser is the weak point

All figures in this section come from infostealer records dated between 2023 and the first 147 days of 2026. Combolists carry no source information, so they are not included here.

Source applications



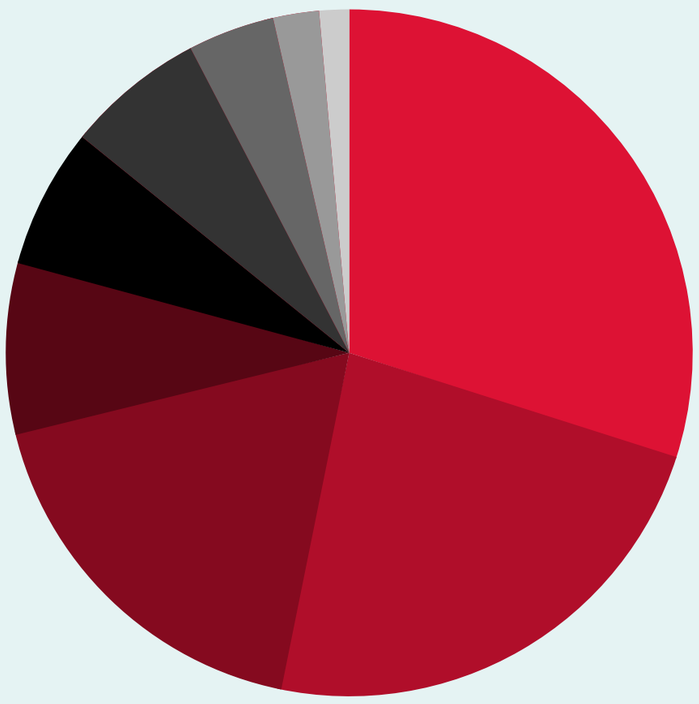
Our analysis of the infostealer logs, which record where the data was pulled from, shows that almost all of the stolen data comes from the browser.

Of the records that name a source, **87.7%** of the credentials were taken from web browsers. Email clients, such as Outlook and Thunderbird (**6.1%**), as well as FTP and SFTP clients (**5.4%**)—tools used to transfer files to and from servers—and other apps (**0.8%**) made up the rest. In 2026 alone, the browser share rose to 99%.

Browsers save logins in a set location and a known format on the device, which makes them an easy and reliable target for infostealers. On a smartphone, for example, someone who saves work and personal passwords in the phone's browser and then installs a malicious app can have every one of those saved logins copied in seconds.

Only about 20% of stolen records relate to corporate or work tools. The rest come from content and information sites, social and messaging apps, entertainment, shopping, and personal accounts. **A victim is often infected while doing something personal,** but because work and personal logins are often saved in the same browser (whether on a work laptop, a personal computer, or a smartphone), the malware copies the work accounts as well. That overlap between personal and professional browsing is one of the clearest areas where organizations can intervene, as described in detail in the recommendations later in this report.

Where stolen credentials come from



Other (forums, niche services, tools)	26.8%
Content and information	26.2%
Corporate and work tools	19.9%
Social media and messaging	8.0%
Entertainment	7.5%
Shopping and financial services	5.0%
Infostealer-related infrastructure	3.1%
Personal accounts (email, storage, etc.)	2.7%
Unclassified or incomplete records	0.8%

This is why even strong corporate defenses can still be bypassed. The weak point is the browser on a single device the company may not even control, and one infected device can be enough to put a working corporate login up for sale.

TL;DR

87.7% of stolen credentials in the data were taken from web browsers. Because most people save both work and personal passwords in the same browser, a single infostealer infection on any device can expose corporate logins even if the company’s own network was never breached.

7. How to reduce your credential exposure

The exposure comes from a chain: infostealer infections on personal and work devices, passwords saved in browsers, password reuse across accounts, and stolen credentials that then circulate on the dark web. Each of the 5 measures below addresses a link in that chain. Read them as a checklist and mark where your organization is and isn’t covered.

1 Secure the browser

Give employees a browser that the company can manage centrally, so it can block known malicious websites and stop risky downloads before an infostealer ever lands. Consumer browsers usually cannot do this. For people working from smartphones or personal devices under a bring-your-own-device (BYOD) policy, apply the same controls through a managed enterprise browser or a work profile.

2 Improve password practices

Turn off built-in browser password managers, because they are exactly what infostealers are built to read. Make sure employees do not reuse the same password across accounts: a single leak of a reused password can then unlock many company systems at once.

Give staff a dedicated password manager instead. It stores passwords in an encrypted vault outside the browser, creates strong unique password for every account, and removes the temptation to reuse one.

3 Build employee awareness

Most infections start with a normal-looking action, such as downloading a cracked app, clicking a link in a convincing email, or installing something on a personal phone that also holds work logins. Teach staff to recognize these moments and to **keep work accounts out of personal browsers** and off unmanaged devices.

The single easiest habit to build is this: never save a work password in a personal browser. Use the company password manager instead.

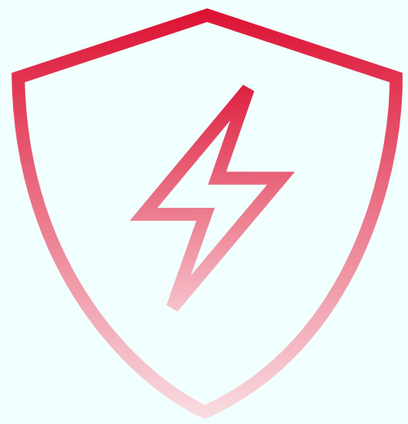
4 Monitor the dark web for your stolen logins

Dedicated monitoring tools now do this automatically, scanning leaks and alerting you when a company credential appears. This way, you can reset affected passwords, flag compromised accounts, and check for unusual activity early. **Choose a provider that watches a wide range of sources**, including infostealer logs, leaked databases, dark web forums and marketplaces, Telegram channels, and ransomware leak sites, because narrow coverage misses most of the supply.

5 Apply a zero-trust approach to access

Zero trust means the network never assumes a login is safe just because the password is correct. Every access request is checked against the person's identity, their device, and the context of the request, and each user only reaches the resources their role needs.

If a stolen password is entered, a second factor will still required.
If the login comes from an unmanaged device, access can be blocked.
Even a successful login does not open the whole network, so one leaked credential stays contained instead of turning into a full breach.



TL;DR

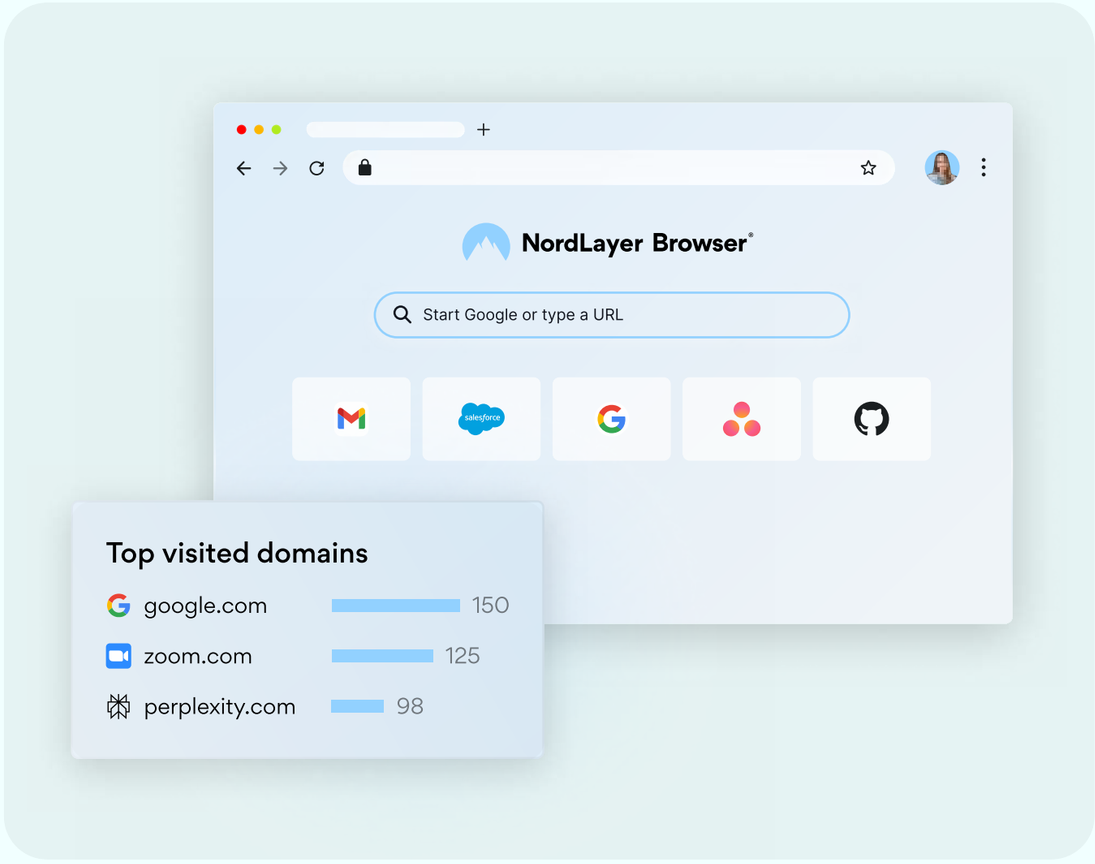
Credential exposure can be reduced at every stage of the chain: blocking infostealers before they land, removing passwords from the browser, monitoring the dark web for leaked logins, and applying zero-trust access so that a stolen password alone is never enough to get in.

8. How to cover each risk

No single product removes every source of credential exposure, because the risks appear at different stages: malware landing on a device, weak or reused passwords, credentials already for sale, and stolen logins being used to get in. Each stage needs a different type of control. The NordLayer platform runs most of them as one connected set.

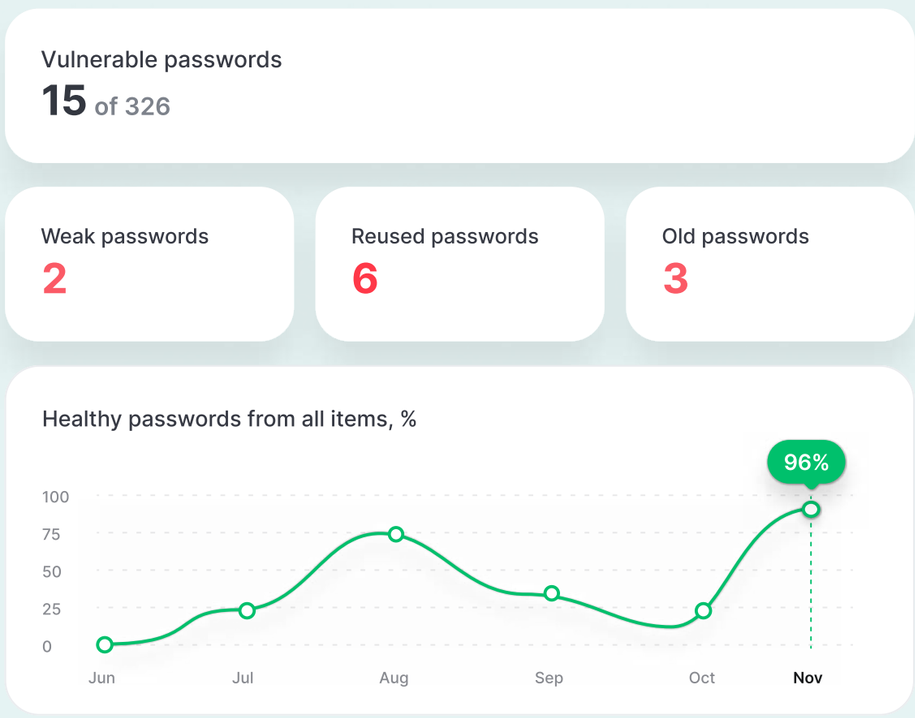
Stop infections early

With the **NordLayer Browser**, infostealers are blocked before they can reach employees. Malicious and deceptive sites, unsafe downloads and uploads, and unapproved apps are blocked centrally, and administrators can set different rules per team. Because **these controls can extendto contractors and staff using personal devices**, the company stops depending on each person's judgment about pages it cannot see and one of the most serious entry points for credential theft becomes far harder to trigger.



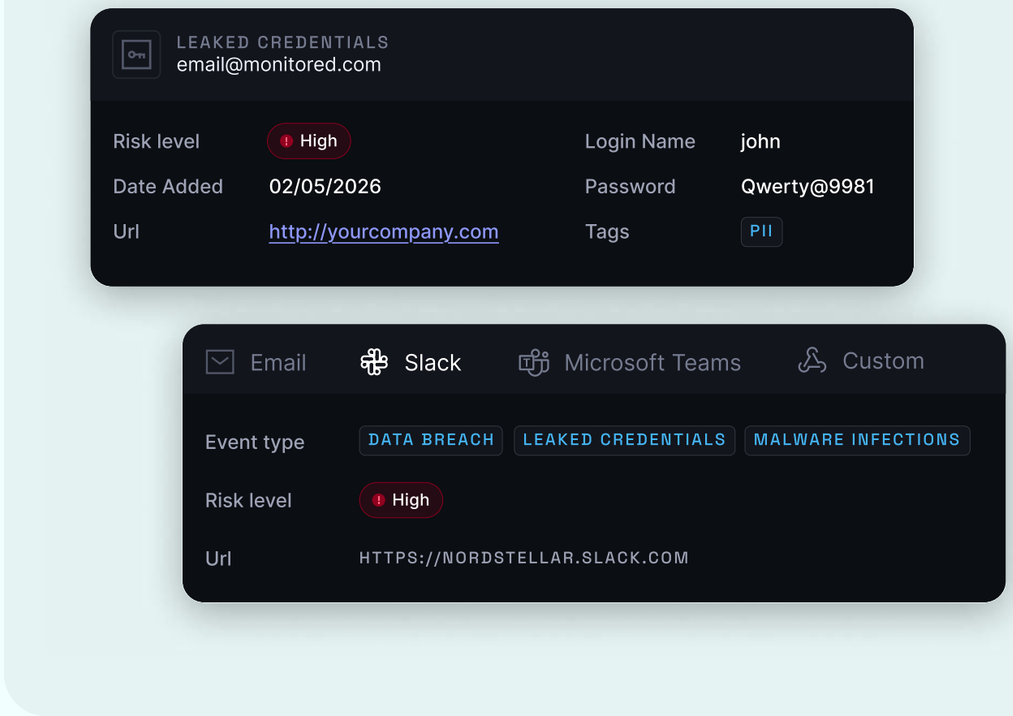
Solve the browser password problem

NordPass takes work passwords out of the browser (the exact place infostealers target) and keeps them in an encrypted company vault instead. **Weak, old, and reused passwords are surfaced automatically, and a breach scanner checks company emails, domains, and passwords against known leaks.** Shared access can be granted or revoked without ever sending passwords through email or spreadsheets. This eliminates the two habits behind most exposure: saving passwords in the browser and reusing them, stop being an option.



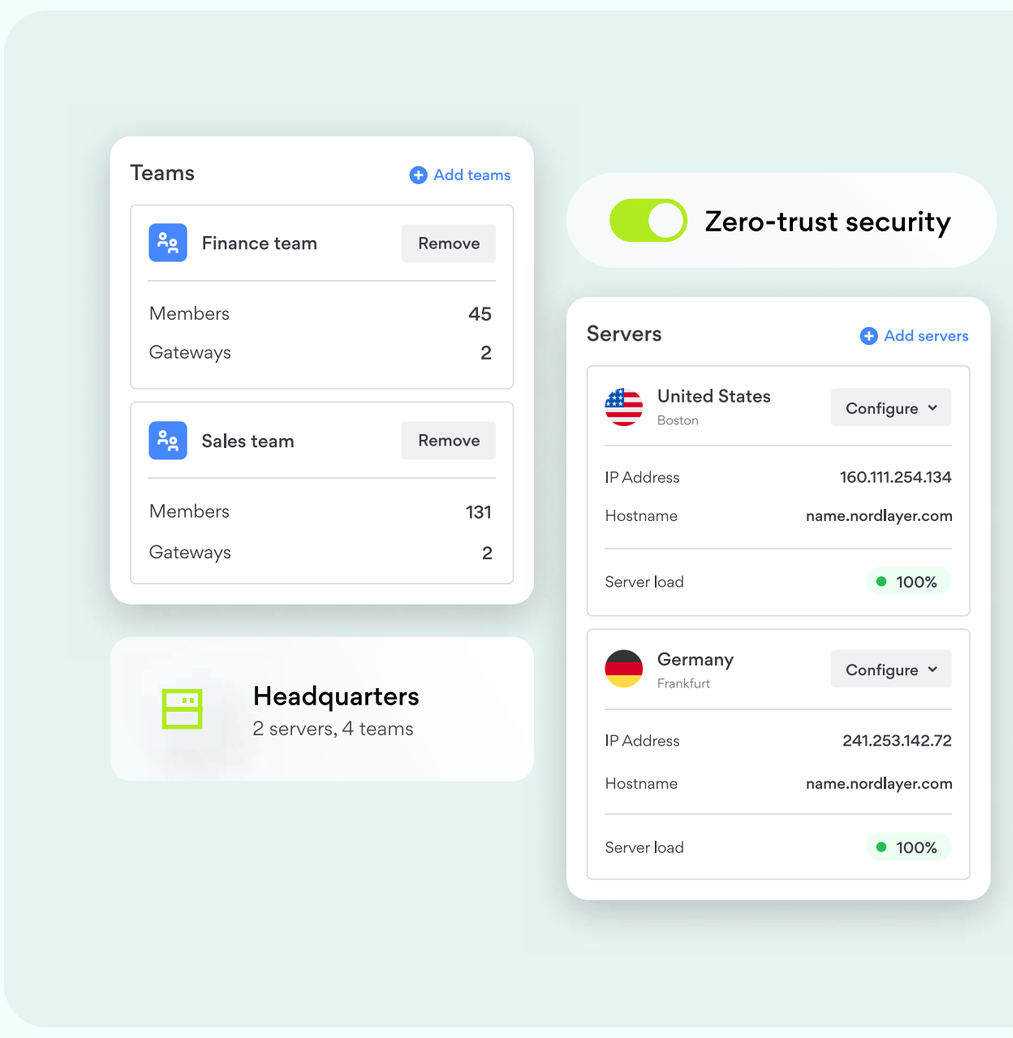
See exposure before attackers act

NordStellar gives security teams sight of credentials that have already leaked. It searches infostealer logs, leaked databases, dark web forums and marketplaces, Telegram channels, and ransomware blogs for company domains and employee emails, then alerts the team through email, Slack, or Microsoft Teams. Each alert can include the source, timestamp, and screenshots, so teams can confirm the exposure, reset affected passwords, and investigate account activity. **With NordLayer Intelligence, companies learn about a leak before an attacker can use it.**



Contain a login that still gets through

Some stolen passwords will always slip past the earlier controls, and this is where zero-trust access limits the damage. **NordLayer's zero-trust network access checks each request against identity, device, and context,** then hands the user only what their role requires. When a password is valid but possibly stolen, multi-factor authentication adds another check. Should an account still be compromised, segmentation and traffic controls keep the attacker boxed in, while session logs give the team a clear record to act on. A leaked password might pass the first login screen, but it does not hand over the network.



NordLayer®

NordLayer Browser®

NordPass®

NordStellar®

What makes **NordLayer, NordPass**, and **NordStellar** work well as one set is that **they share management and coverage across the whole chain,** from the device on which malware lands to the marketplace in which credentials are sold.

For administrators, that means fewer disconnected tools to run, consistent policy across browsers, passwords, access, and monitoring, and a single view of where exposure is being created and caught.

9. Conclusion

Credential theft runs as a steady supply chain. Of all available records, **9.96 million email and password pairs** belonging to Fortune 500 companies are in circulation. Within the first 147 days of 2026 alone, an expired credential appeared approximately every 100 seconds.

Exposure rates vary widely across the Fortune 500, but the variation is related to workforce composition rather than security posture. Companies where nearly every employee works at a computer with a corporate account have the highest exposure rates. Companies with large frontline workforces show the lowest rates, while often carrying more exposed credentials in absolute terms. However, neither position says anything about how well a company is defended.

What separates outcomes is where the chain gets broken. Infections can start on devices that companies often don’t control. Passwords can be taken from browsers. Reuse can spread a single leak across systems. Stolen credentials can circulate for years after the breach that produced them. Keeping malware off devices, moving passwords out of the browser, monitoring for leaks, and limiting what any single login reaches each cut a different link in the chain.

> Some exposure is unavoidable at this scale, but whether it turns into a breach is not.

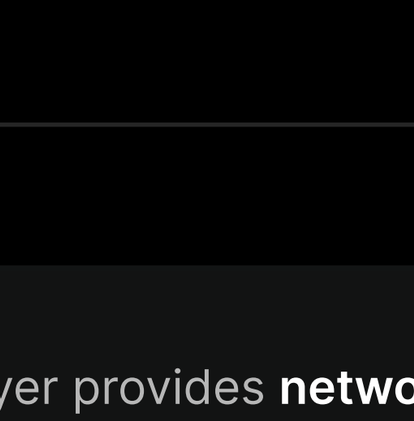
10. Methodology

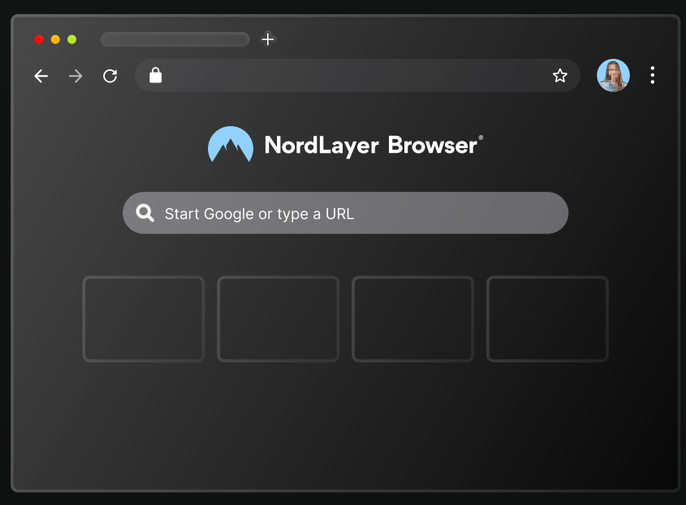
NordLayer and NordLayer Intelligence by NordStellar analyzed leaked credentials and identified those tied to domains belonging to Fortune 500 companies, covering 3,692 corporate domains. Subsidiary brands were not included. The research began with 34.86 million raw records, which were deduplicated to 9.96 million unique email and password pairs, counted once per company. Each company was matched to its industry, revenue, and headcount.

The leaked sets are made up of combolists and infostealer logs; however, only the infostealer logs carry a collection date. About 130,000 of those dated records fall within roughly 147 days of 2026, which works out to about 1 new credential every 100 seconds. Per-employee exposure was calculated by dividing a company’s unique leaked emails by its headcount, then scaled to a rate per 1,000 staff and grouped by company size and by industry for comparison.

NordLayer®

NordLayer provides **network security, threat detection,** and **response for businesses that need strong protection**. It is part of Nord Security, home to products including the VPN service NordVPN.





NordLayer **integrates with existing networks and technology**, and in March 2026 it launched the **enterprise browser** NordLayer Browser.

For more information, visit nordlayer.com