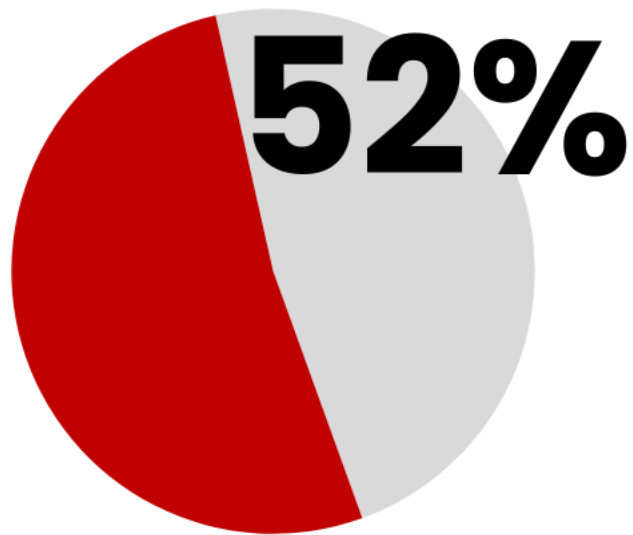




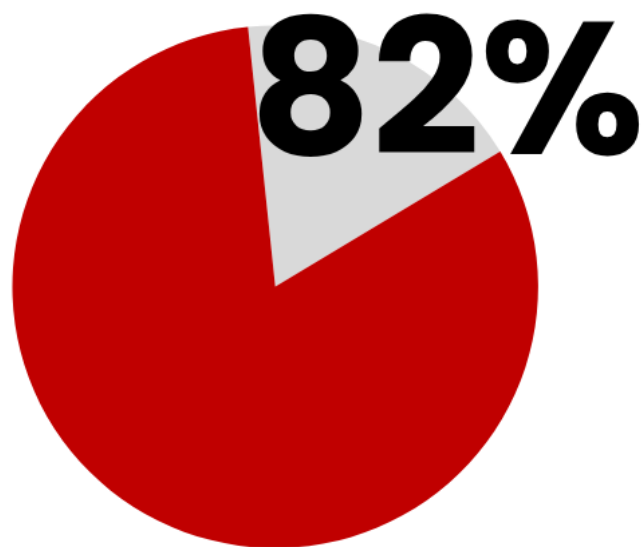
ACCESS IS THE ATTACK SURFACE.

PRACTICAL CYBERSECURITY FOR LEAN IT TEAMS

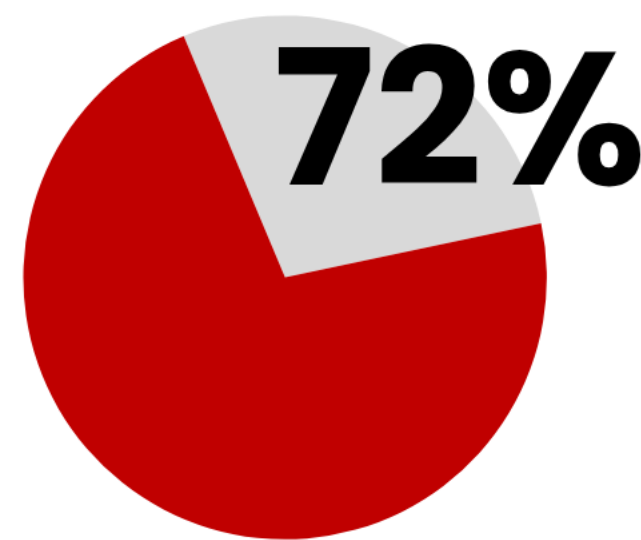
Attackers aren't breaking in...they're logging in.



of vulnerabilities observed in 2024 were related to **initial access**.



of detections in 2025 were **malware-free**.
(Up from 79% in 2024)



of organizations experienced a significant or very significant disruption to business **resulting from a breach**.

Access *is* the **attack surface**

● **Standing admin**

On by default, on every machine, forever.

● **Reused passwords**

One leak becomes several systems.

● **A VPN that grants the whole network**

One login, and you're inside like staff.

● **A drifting Microsoft 365 tenant**

Exceptions granted in March, still there in November.

None of these are exotic. They are the default state of most organizations your size — and they are what turns one compromised user into a company-wide event.



"A proactive cybersecurity policy is not just smart — it's essential"

Proactive cybersecurity means putting strategies and processes into place before a threat emerges to reduce your vulnerabilities and the risk of an attack.



Everyone already agrees on the fix.

This isn't a knowledge problem, and it hasn't been for over twenty years.





Global frameworks. Same essential controls.

Microsoft – Use Non-Administrator Accounts for Regular Sign-in

1. As a security best practice, use your local (non-admin) account to login
2. Use “run as administrator” for elevated privileges
3. Avoid logging in as Administrator unless entirely necessary

CIS Control 4: Secure Configuration of Enterprise Assets and Software

4.7 Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: **disabling default accounts or making them unusable.**

4.9 **Configure trusted DNS servers** on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

CIS Control 5: Account Management

5.1 Establish and maintain an **inventory of all accounts** managed in the enterprise. The inventory must include both **user and administrator accounts**...

5.2 **Use unique passwords for all enterprise assets.**

5.4 **Restrict administrator privileges**

CIS Control 6: Access Control Management

6.7 Centralize Access Control

6.7 Define and Maintain **Role-Based Access Control**

CIS Control 9: Email and Web Browser Protections

9.2 **Use DNS filtering services on all end-user devices**, including remote and on-premises assets, to block access to known malicious domains

The Essential Eight – Australia

Restrict administrative privileges
Application Control

UK Cyber Essentials

User Access Control: Control who can access your data and services and what level of access they have

NIST Framework

Recommends the **principle of least privilege**, access and **credential policies**, and limited access in the “Protect” section.

Recommends that networks and network services are monitored to find potentially adverse events – NIST recently published SP 800-81r3: **Secure Domain Name System (DNS) Deployment Guide** final version (March 2026)

HIPAA Compliance

164.308(a)(4)(ii)(B)

Rights and/or privileges should be granted to authorized users based on a set of access rules that the covered entity is required to implement as part of § 164.308(a)(4), the Information Access Management standard under the Administrative Safeguards section of the Rule.

PCI Compliance

Objective “Implement **strong access control** measures”
Sections 7.1, 7.2, 7.3, 8.1, 8.2, 8.3, 8.7

FFIEC (Federal Financial Institutions Examination Council)

Authentication and **Access Controls**

Those controls were written by enterprise security

WHO DESIGNED THEM

- A dedicated security team
- A security budget line of its own
- Consultants available on retainer
- People whose only job is this
- Months of runway for a rollout

vs

WHO HAS TO OPERATE THEM

- Three people, sometimes one
- No security department at all
- The same people who fix the printer
- No consultants, no runway
- And everything still must keep running

Same controls. Completely different operating conditions. Almost nobody has designed for the second column — so lean teams inherit security they cannot run.

Here's what happens instead

TWO WAYS IT FAILS

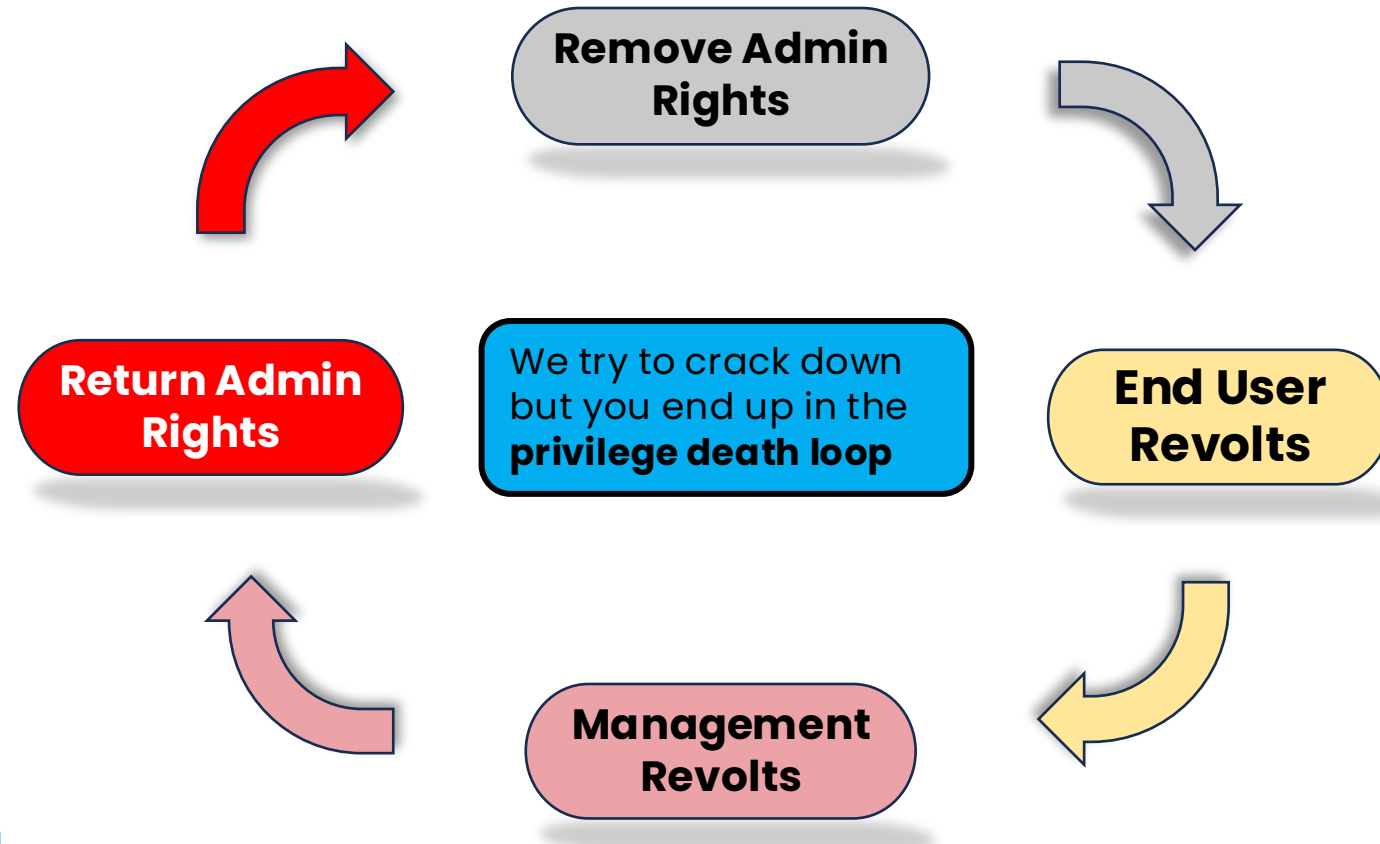
Option one: enforce it yourself.

You remove admin rights with no elevation path, become the approval desk for every install, and hand the rights back within a month.

Option two: buy an enterprise platform.

Months of implementation, a consultant, and a platform you never fully deploy.

**"Removing privilege is easy.
Giving it back is the hard part."**



"Too hard to use, too difficult to implement"

1

Replaced an enterprise PAM platform

A manufacturing organization moved off an enterprise PAM platform after finding it too hard for technicians to administer day to day.

2

Evaluated, then walked away

An IT provider trialled several enterprise PAM platforms and described them as too hard to use and too difficult to implement.

3

Had to rebuild machines to remove it

One team's previous privileged-access tool was so entangled that dozens of machines had to be wiped and rebuilt just to get rid of it.

A security control you had to wipe machines to remove was never a security control. It was a liability with a licence.



**A security control you had to
wipe machines to remove was
never a security control.
It was a liability with a license.**





Two things make this even more urgent.

WHY NOW?

1

If you have access, **AI has access**

➤ **The agent inherits every right you hold**

Something acting on a user's behalf holds exactly what that user holds — and uses it across more systems than a person could touch in a day.

➤ **It doesn't hesitate, and it doesn't get tired**

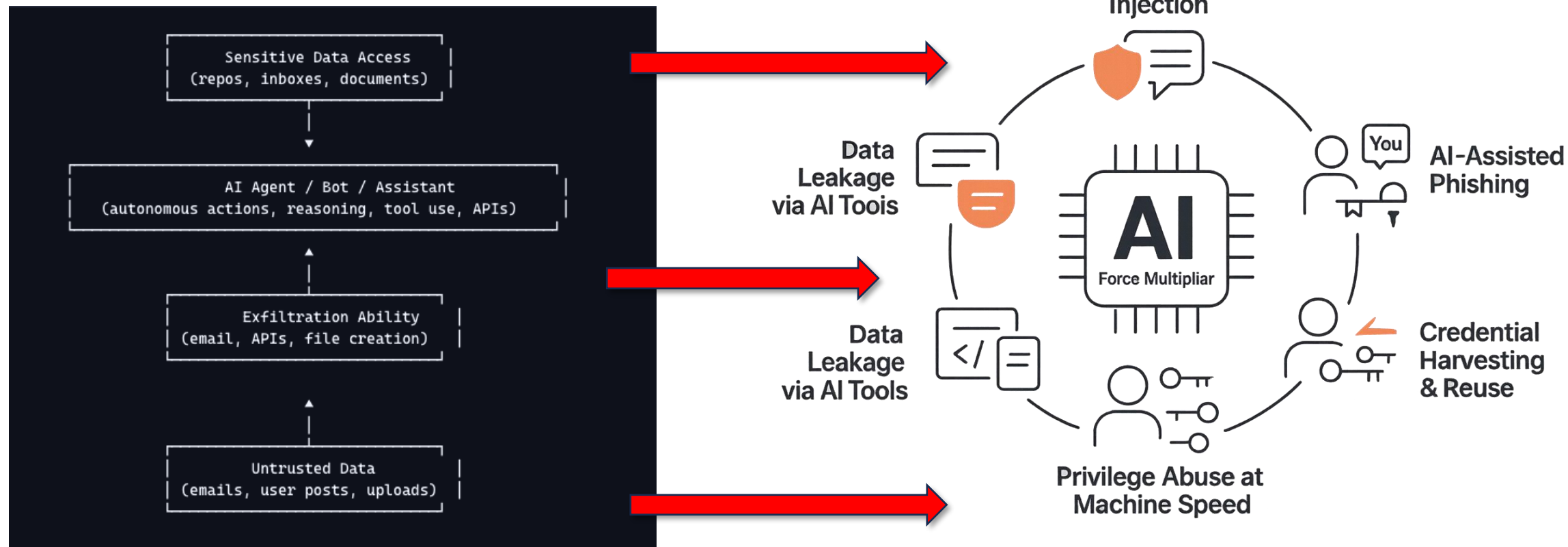
The pause before doing something that feels wrong has quietly prevented more incidents than any product. An agent is built not to pause.

➤ **So partial coverage stopped being partial risk**

A control you deployed to 60% of the estate used to be a slow leak. At machine speed, the other 40% is the whole surface.

An AI agent is not a new identity. It is your identity, running without a lunch break.

AI attack vectors



Your endpoints' AI governance is only as strong as their identity and access management and foundational security.

2

It isn't enough to control access. **Prove it.**

➤ **INTERNAL AUDITS** ➤ **CYBER INSURANCE** ➤ **REGULATORS** ➤ **ACQUIRERS**

This is what actually creates urgency

Not the threat alone. Our data shows privileged access gaps are widely recognized and consistently deprioritized — until one of these four groups asks.

So a control that works but produces no evidence is only half a control.

"We removed admin rights" is an assertion, while an exportable log of every elevation is **proof.**



What does the right implementation look like?

Five tests that hold everyone accountable.

Five tests for security that survives week three

01 **Live in hours, not months**

If it needs a project plan and a consultant, it will be half-deployed forever.

02 **Runs without a middle-man**

If every exception needs a human decision, the human becomes the bottleneck and the control gets switched off.

03 **Manageable from anywhere**

The approval that has to happen at a desk is the approval that does not happen.

04 **Produces automatic evidence**

If proving it works is a separate project, you will not have proof when you are asked.

05 **Priced so it survives a budget cycle**

A control removed at renewal was a rental, not a posture.

Most tools chase the breach. Fundamentals stop it at the door.



Most tools chase the breach. Fundamentals stop it at the door.



Almost every attack starts with a lookup

THE PROBLEM

Phishing pages, malware downloads and command-and-control callbacks all begin with a DNS query. Without filtering, that query succeeds — and without logging, you cannot answer where a machine called out to.

WHAT CLOSES IT

Destination filtering can block malicious or unwanted connections before they are made. Policies can follow devices on and off the network, with query activity available for investigation.

AGAINST THE FIVE TESTS

- 1 Live in hours
- 2 No approvals, no human in the loop
- 4 Query logs are the evidence

Stolen credentials shouldn't equal network access

THE PROBLEM

A legacy VPN is one tunnel into everything. Once a credential works, the attacker is inside the network exactly the way your staff are — and remote work means that tunnel is open from anywhere.

WHAT CLOSES IT

Zero Trust Network Access (ZTNA) continuously evaluates the user, device, and access request before allowing access to a specific resource.

AGAINST THE FIVE TESTS

- 1 Live in about 30 minutes
- 3 No hardware to be on-site for
- 5 Per-user pricing, no refresh cycle

One key, copied everywhere, under the mat

THE PROBLEM

Passwords live in spreadsheets, browser profiles, sticky notes and chat threads. The same one gets reused across systems, so one leak becomes several — and when someone leaves, nobody can list what they knew.

WHAT CLOSSES IT

An encrypted vault with secure sharing, enforced MFA and role-based access. Zero-knowledge architecture, so credentials are unreadable even to the platform. Unique credentials become the default rather than the ambition.

AGAINST THE FIVE TESTS

- 1 Live in hours
- 2 Sharing stops needing you
- 4 Access records for the auditor

The control that breaks the privilege death loop

THE PROBLEM

Standing local admin is the easiest privilege escalation in most environments, and the reason one compromised endpoint becomes a company-wide incident. Removing it without an elevation path is what starts the death loop.

WHAT CLOSSES IT

Remove standing admin, then grant elevation just-in-time and just-enough, per application, approved from any device. Rules answer the predictable requests automatically. Blocklisting stops the native binaries attackers abuse. Every elevation is logged.

AGAINST THE FIVE TESTS

- 1 Hours, and audit mode first
- 2 Rules handle the routine, not you
- 3 Approve from a phone
- 4 Least-privilege audit evidence

The panel that governs every other lock

THE PROBLEM

Microsoft 365 holds the identities everything else trusts, and its configuration drifts constantly. Weak conditional access, MFA gaps, and global admin accounts nobody has revisited in two years. Nobody misconfigures a tenant on purpose — it accumulates.

WHAT CLOSES IT

Security baselines with drift detection, MFA and conditional access enforcement, risky sign-in alerts, Secure Score tracking, and one-click remediation across your system.

Every application or AI agent connected to the tenant operates within the permissions and configuration you've established. So configuration drift doesn't just affect IT, it can affect everything you've connected to the environment.

AGAINST THE FIVE TESTS

- 1 Live in about 30 minutes
- 2 Drift is caught, not hunted
- 4 Secure Score as a trend line

How attackers actually win

Cyber Kill Chain



Cyber Kill Chain



Most tools chase the breach. Fundamentals stop it at the door.

Cyber Kill Chain





Three months where this shows up.

The time you got back. The attack that stopped. The audit that passed.



The audit that passed

INSURANCE

One organization adopted privileged access management because its cyber insurance was blocked without proof of controlled admin rights.

Another held its renewal rate flat in a year when the wider market saw double-digit increases.

WHAT YOU CAN HAND OVER

- Who elevated what, when, and who approved it
- Every DNS query, exportable
- Access records and role assignments
- Tenant posture as a trend, not a snapshot

MAPPED TO WHAT YOU'RE ASKED ABOUT

CIS 4, 5, 6, 9

NIST CSF Protect

PCI DSS 7 & 8

HIPAA 164.308(a)(4)

Cyber Essentials

Essential Eight

"We removed admin rights" is an assertion. An exportable log of every elevation is proof. Only one of those survives an audit.

Cybersecurity in hours, not months

With a script, not a consulting bill.

FIRST 30 DAYS

Watch, don't enforce

- Deploy PAM in audit mode — see who elevates and how often
- Turn on DNS filtering and start logging queries
- Inventory your Microsoft 365 admin accounts

DAYS 30–60

Close the easy questions

- Roll out the vault and enforce MFA
- Build approval rules from what audit mode showed you
- Fix the conditional access gaps you found

DAYS 60–90

Remove standing privilege

- Switch PAM from audit to live enforcement
- Replace the VPN with always-on ZTNA
- Set a review cadence so drift doesn't creep back

Audit mode first is the whole trick. Nothing breaks on day one, and your rules come from real behavior.

The attack that **stopped**

1

A credential-scraping attempt on a medical practice

A two-person IT team supporting a medical practice with more than 750 endpoints and 23 servers. Their biggest exposure was standing admin access. By removing those permanent privileges, they closed the path attackers could exploit — without forcing the practice into the costly rebuild others in the same position have faced.

2

Ransomware, then a rethink

One provider replaced a complex application-allowlisting approach with **least privilege** after a ransomware incident — because the control they had was too heavy to actually run.

Prevention is invisible by nature. The only way to make it visible is to tell the story of the incident that didn't happen.

The time you **got back**

50 → 10

hours a month spent on access requests, as one IT provider

60%+

drop in access-related tickets — and zero tickets caused by the tool itself

4,000+

printer admin tickets a year eliminated at one organization

- A 6am on-site visit every three months across 70 machines — gone.
- An hour of driving to the office to approve a printer install — gone.
- Manually entering credentials on 20–30 machines every Monday — gone.

From CyberFOX customer case studies..





**Attackers aren't breaking in.
They're logging in.**

CyberFOX stops them at the gate.

