REDLEIF Island

The *Enterprise Browser* in Government & Education:

Practical Use Cases for Modern Security and Productivity

How state, local, and education leaders are simplifying control, strengthening protection, and modernizing how their people work.

Introduction

Why a Browser Belongs at the Center of Security

Government and education leaders have long faced a familiar tension: every effort to modernize (e.g. to improve speed, access, or collaboration) often increases risk. Security and modernization have historically been competing goals.

Virtual desktops, VPNs (Virtual Private Networks), and complex endpoint management systems helped bridge that gap, but at a cost: complexity, expense, and friction for users.

The Enterprise Browser changes that equation.

It embeds control, visibility, and protection directly where people work (in the browser) without slowing them down. Instead of relying on layers of infrastructure or third-party gateways, the browser itself becomes the secure workspace.

Across the public sector, this shift is already underway.
State IT agencies, city governments, and higher education institutions are using the Enterprise Browser to:

- Provide secure access for contractors and hybrid staff without managing devices.
- Replace complex VDI (Virtual Desktop Infrastructure) setups with lightweight, policy-driven control.
- Protect sensitive citizen and student data inside SaaS (Software as a Service) and web applications.
- Enable safe, auditable experimentation with AI and other modern tools.

This guide outlines practical use cases, drawn from real government and education scenarios, that show how the Enterprise Browser delivers measurable value across security, compliance, and productivity. Each section includes:

- A short description of the problem.
- How the Enterprise Browser helps.
- Why it matters for different stakeholders.
- What a proof of concept (PoC) might look like.
- Metrics to track tangible results.

Use Case 1

Contractor and Vendor Access Without the Complexity

The Scenario

Government operations depend on external contributors like consultants, engineers, auditors, and seasonal workers, who all need some level of system access to do their jobs.

But every one of those users represents a challenge for IT: Issuing government-owned laptops, managing Virtual Private Networks (VPNs), or running Virtual Desktop Infrastructure (VDI) for short-term access adds cost, delays, and risk.
Even when those controls work, they're cumbersome. Devices get lost. Credentials linger. And when contracts end, access often doesn't... at least not immediately.

How the Enterprise Browser Helps

The Enterprise Browser extends secure access to contractors without the baggage of VDI or VPNs.

It applies security policies, session controls, and data protections directly at the browser layer, where most work already happens, without requiring special hardware, new agents, or complex setup.

In practice, this might look like:

- A contractor logs into a secure browser workspace from their personal device.
- Downloads, copy/paste, and screenshots are automatically restricted for sensitive systems.
- When the contract ends, access is revoked instantly. No device retrieval or manual cleanup needed.

It's the same level of control, but without the friction, cost, or delay.

Why It Matters

- **Security Leaders:** Maintain oversight of every contractor session, with visibility into actions and data flow, even on unmanaged devices.
- **IT Teams:** Cut down provisioning time from days to hours; eliminate the need to manage hardware for short-term users.
- **Executive Leadership:** Reduce operational risk exposure while showing measurable efficiency improvements.
- **End Users (Contractors):** Log in quickly, work efficiently, and stay compliant without cumbersome setup steps.

What a Proof of Concept (PoC) Might Look Like

- Identify a single department or project that regularly engages external vendors or consultants.
- Enforce session-level policies like data movement restrictions, watermarking, or clipboard controls through the Enterprise Browser.
- Compare provisioning time, audit findings, and user satisfaction against the previous cycle.

Outcomes Scorecard: Contractor & Vendor Access

Metric	Without Island	With Island	Trend
Average contractor onboarding time	37 days	1 day	🟢 ↓
Time to revoke access after contract end	87 days	< 1 day	🟢 ↓
IT support tickets related to contractor access	148 / month	9 / month	🟢 ↓
Unauthorized access attempts blocked	4	154	🟢 ↑
Access audits completed on time	32%	94%	🟢 ↑
High-risk audit findings (contractor access)	37	1	🟢 ↓
Estimated IT provisioning cost per contractor	~$180	~$95	🟢 ↓
Contractor access occurring outside approved controls	87%	2%	🟢 ↓

Use Case 2

Field and Inspection Teams - Secure Mobility Without the Headaches

The Scenario

Field teams - from building inspectors and environmental assessors to public health caseworkers - spend most of their day away from the office.

They need reliable access to agency systems, but traditional remote access tools like VPNs (Virtual Private Networks) and VDI (Virtual Desktop Infrastructure) often create more problems than they solve.

Spotty connectivity, complex logins, and slow load times make it hard to stay productive. Even worse, these tools sometimes encourage insecure workarounds, like saving files locally or emailing data to themselves to finish reports offline.

How the Enterprise Browser Helps

The Enterprise Browser keeps work secure, even beyond the agency network.

Instead of relying on hardware or heavy infrastructure, the browser applies security policies directly at the session level, enforcing controls for data sharing, copy/paste, and downloads in real time.

For example:

- A building inspector logs into a secure browser workspace on a tablet before heading into the field.
- They can access inspection systems, upload photos, and submit forms without ever storing data locally.
- If they lose connectivity, session data remains encrypted, and access can be terminated remotely.

That means field staff can stay productive without compromising security, even in low-connectivity or bring-your-own-device (BYOD) environments.

Why It Matters

- **Security Leaders:** Reduce risks tied to local file storage and unmanaged field devices.
- **IT Teams:** Simplify mobile access without maintaining VPN infrastructure or troubleshooting offline issues.
- **Executive Leadership:** Improve productivity while demonstrating compliance with data protection standards.
- **End Users (Field Teams):** Get faster, more reliable access without the delays and downtime of virtual desktops.

What a Proof of Concept (PoC) Might Look Like

- Choose one regional inspection or field services unit.
- Equip 20–30 users with the Enterprise Browser for field operations.
- Configure policies for file uploads, downloads, and offline caching.
- Compare productivity, data handling, and security event data before and after deployment.

Outcomes Scorecard: Contractor & Vendor Access

Metric	Without Island	With Island	Trend
Successful secure access attempts (first try)	~1,930 / month	~2,325 / month	🟢 ↑
Field users requiring VPN or VDI to access systems	275 users	35 users	🟢 ↓
IT support tickets related to remote access	~26 / month	~9 / month	🟢 ↓
Time to regain secure access after connectivity interruption	~18 minutes	~3 minutes	🟢 ↓
Security alerts originating from field devices	~11 / month	~4 / month	🟢 ↓
Sensitive data stored locally on field devices	~9 GB	~1 GB	🟢 ↓
Compliance audit findings related to field access	2	1	🟢 ↓
Mobile access sessions occurring outside approved security controls	~2,850	~300	🟢 ↓
Secure mobile access sessions per month	~450	~3,000	🟢 ↑

Use Case 3

Protecting Sensitive Data Without Slowing Down the Mission

The Scenario

Public agencies manage enormous amounts of sensitive information: student records, health data, tax details, court documents, and more.

Every employee, contractor, and partner who touches that data increases the risk of accidental exposure or malicious misuse.

Traditional controls, like network firewalls or VPNs (Virtual Private Networks), were designed to keep intruders out, not to control what happens after someone gets in. And while Virtual Desktop Infrastructure (VDI) helps isolate data, it often introduces user friction that drives risky workarounds.

How the Enterprise Browser Helps

The Enterprise Browser protects data at the point of interaction — inside the browser session itself — where nearly all modern work occurs.

Security policies and Zero Trust controls apply dynamically based on user, device, or context:

- Sensitive fields (like SSNs or student IDs) can be automatically masked.
- Copy, paste, or download actions can be disabled for certain roles or applications.
- Session data is encrypted in real time and wiped when the browser closes.

It's granular control without the overhead of legacy isolation tools, reducing the chance of both accidental leaks and deliberate misuse.

For example:

- A caseworker views a resident's medical file but can't export or print it.
- A student records clerk can only view masked data unless additional authentication is verified.
- A finance employee logging in from an unmanaged device can still perform approved actions, but file downloads are blocked automatically.

Why It Matters

- **Security Leaders:** Enforce data-handling policies at the most vulnerable layer (the browser) to reduce insider and endpoint risk.
- **IT Teams:** Eliminate redundant DLP (Data Loss Prevention) configurations and manual audit prep.
- **Executive Leadership:** Strengthen compliance posture for mandates like HIPAA, FERPA, and CJIS while improving staff efficiency.
- **End Users (Staff & Analysts):** Work faster with fewer pop-ups, disconnected sessions, or complicated remote setups.

What a Proof of Concept (PoC) Might Look Like

- Identify a team that handles personally identifiable or regulated data (e.g., student services, public health, HR).
- Deploy the Enterprise Browser for those users and configure masking and download policies for critical systems.
- Monitor user friction, data movement, and compliance event volume over 30–60 days.
- Compare audit outcomes and user behavior with the previous reporting cycle.

Outcomes Scorecard: Contractor & Vendor Access

Metric	Without Island	With Island	Trend
Sensitive data interactions occurring inside approved security controls	~35%	~92%	↑
Sensitive data interactions occurring outside approved security controls	~65%	~8%	↓
Unauthorized sensitive data downloads	~11 / month	~2 / month	↓
Reported data handling incidents	6	1	↓
Policy enforcement success rate	74%	97%	↑
Compliance audit findings related to data handling	4	2	↓
Time required to complete data-handling audits	~14 days	~9 days	↓
Help desk tickets related to data access restrictions	~23 / month	~16 / month	↓
Sensitive data exports blocked by policy	~18 / month	~140 / month	↑

Use Case 4

BYOD at Scale Without Losing Control

The Scenario

In government and education, BYOD (Bring Your Own Device) isn't one thing. It shows up in a few very real patterns:

- Education: thousands of students, adjuncts, and visiting researchers logging in from personal laptops, phones, and tablets
- Government: a mix of full-time staff, seasonal workers, contractors, and partner organizations who need access without waiting on a device rollout
- Field and distributed teams: inspectors, social services, public works, emergency coordination, and other roles where work doesn't always start at a desk
- "Access is needed now" moments: someone is onboarding, covering for another team, responding after hours, or helping during a surge

Even when organizations do provide standard devices, the reality is that personal devices still touch work, especially for browser-based systems: portals, collaboration tools, dashboards, forms, case tools, learning systems, and admin platforms.

The problem isn't that BYOD exists. It's that most controls were designed around device ownership—and browser work doesn't always cooperate with that model.

How the Enterprise Browser Helps

The Enterprise Browser gives organizations a way to protect browser-based work without requiring every user to be on a fully managed endpoint.

Instead of placing all the burden on devices, you can apply protection directly to the browser session:

- Policy-based access: restrict access by role, device type, location, risk signals, or application
- Data protection inside the session: control downloads, copy/paste, printing, uploads, and file handling where needed
- Visibility and auditability: log activity inside approved browser workspaces for oversight and investigations
- Fast deprovisioning: when someone's role ends, access ends—without having to recover a device first

Hypothetical Examples (how this could play out)

- A contractor accesses a procurement portal through the Enterprise Browser where downloads are restricted by default.
- A visiting researcher or adjunct faculty member accesses approved web tools through a controlled workspace without gaining broad access to everything else.
- A field supervisor reviews and submits updates in a browser session where sensitive data can't be copied into personal apps.

Why It Matters

- Security Leaders: Reduce the risk of sensitive work spilling into unmanaged tools while improving visibility into browser-based activity.
- IT Teams: Support mixed-device realities without turning every edge case into a device provisioning project.
- Executive Leadership: Keep onboarding and access from slowing down mission delivery.
- End Users (Faculty & Students): Reduce exposure and improve accountability without forcing one-size-fits-all technology constraints.

What a Proof of Concept (PoC) Might Look Like

- Choose one BYOD-heavy workflow (contractor onboarding, adjunct access, field approvals, seasonal staffing, partner access, etc.).
- Limit scope to a few critical web applications used in that workflow.
- Start with a small policy set focused on preventing common data leakage paths (downloads, copy/paste, printing, uploads—only where appropriate).
- Run for 30–60 days and evaluate whether access becomes more controlled without creating new bottlenecks.

Outcome Scorecard: Bring Your Own Device

(Example metrics; values are placeholders.)

Metric	Without Island	With Island	Trend
Time to grant access for short-term / BYOD users	3 days	1 day	↓
Time to revoke access when access should end	2 days	< 1 day	↓
Access exception requests	~24 / month	~11 / month	↓
Help desk tickets tied to access friction	~65 / month	~38 / month	↓
Confirmed policy violations tied to web work	~14 / quarter	~9 / quarter	↓
% of browser-based work occurring in approved workspace	~52%	~81%	↑
User-reported ease of access (pulse check)	3.4 / 5	4.2 / 5	↑
Document/data exposure events tied to unmanaged tools	~6 / quarter	~2 / quarter	↓
Peak-week onboarding demand met within SLA	~78%	~92%	↑
Median time to load key web apps (p50)	~2.9 sec	~2.4 sec	↓

Use Case 5

Critical SaaS Applications - Enforcing Policy in the Cloud

The Scenario

Agencies and institutions rely on dozens... sometimes hundreds... of cloud and SaaS (Software as a Service) tools: workspace platforms, HR and finance systems, case management tools, collaboration suites, and more.

Each tool helps teams move faster, but every new app adds another layer of security and compliance risk, especially when employees use personal accounts or log in from unmonitored devices.

Legacy solutions like VPNs (Virtual Private Networks) or DLP (Data Loss Prevention) systems can't effectively govern behavior once users are already inside cloud apps. The browser becomes the control point, but without visibility or guardrails, it's also the weakest link.

How the Enterprise Browser Helps

The Enterprise Browser places policy enforcement directly at the point of access — in the browser session — where users interact with SaaS data.

It enables:

- Dynamic controls: Block or allow copy/paste, downloads, or screenshots depending on user identity and context.
- Session-level encryption: Secure data flow without needing endpoint agents or custom app integrations.
- Visibility: Full audit trail of user actions across every approved SaaS app.

For example:

- A financial officer accesses budget documents in Google Drive but cannot download or print them from a personal laptop.
- An HR specialist can review records in Workday but is prevented from saving screenshots.
- A public information officer can post to an official social media account through approved browser sessions without exposing credentials on a personal machine.

Why It Matters

- **Security Leaders:** Gain visibility across all SaaS tools without deploying agents or rewriting policies in every platform.
- **IT Teams:** Centralize access control, reducing manual app-level configurations and shadow IT.
- **Executive Leadership:** Demonstrate improved cloud governance while supporting digital-first initiatives.
- **End Users (Staff & Analysts):** Work confidently in familiar SaaS tools with fewer security interruptions.

What a Proof of Concept (PoC) Might Look Like

- Choose 2–3 high-risk or high-use SaaS apps
- Enable Enterprise Browser access for departments using those apps daily.
- Configure role-based policies for data movement and session control.
- Track data handling events, help desk tickets, and policy enforcement rates for 60 days.

Outcomes Scorecard: Contractor & Vendor Access

(Based on a 1,000 user organization)

Metric	Without Island	With Island	Trend
SaaS access sessions occurring inside enforced browser controls	~40%	~93%	🟢↑
SaaS access sessions occurring outside approved security controls	~60%	~7%	🟢↓
Unmanaged device logins to SaaS applications	~28 /month	~6 month	🟢↓
SaaS data leakage alerts	~9 /month	~2 /month	🟢↓
Policy enforcement success rate (SaaS access)	~81%	~96%	🟢↑
Help desk tickets related to SaaS access issues	~32 /month	~18 /month	🟢↓
Shadow SaaS applications detected	~14	~5	🟢↓
Compliance audit findings related to SaaS usage	3	1	🟢↓
SaaS data export attempts blocked by policy	~120 /month	~300 /month	🟢↑

Use Case 6

Generative AI and Web-Based Tools - Controlling the New Risk Frontier

The Scenario

AI tools like ChatGPT, Copilot, and Gemini are rapidly becoming part of daily workflows, even inside agencies and universities that never officially approved them.

Employees use them to summarize reports, write code, or draft communications, often by pasting in sensitive or proprietary information.

The result? Massive efficiency gains paired with massive new risks.

Unlike traditional apps, AI tools learn from input data. If that data includes confidential or regulated information (i.e. student records, criminal justice data, or internal policy documents) it may leave the agency's control permanently.
Blocking access entirely isn't sustainable. But allowing ungoverned access is equally dangerous.

How the Enterprise Browser Helps

The Enterprise Browser lets agencies and institutions enable AI tools safely, by defining how users can interact with them.

It provides:

- Context-aware policy enforcement: Limit data copy/paste or upload functions within AI sites.
- Granular visibility: Log every AI-related action for auditing and investigation.
- Role-based access: Allow certain departments or approved users to experiment safely while protecting critical data.
- Custom allow/deny lists: Specify which AI tools are sanctioned and which are off-limits.

For example:

- A communications officer can use ChatGPT to draft public FAQs but cannot paste internal memos or attachments.
- A professor can explore AI research tools in a sandboxed browser environment with no outbound data risk.

An agency policy team can use Copilot to draft internal documents with all prompts logged for transparency and auditability.

Why It Matters

- **Security Leaders:** Enforce real-time controls on AI interactions before data leaves the browser.
- **IT Teams:** Avoid risky shadow AI usage by providing a sanctioned, monitored alternative.
- **Executive Leadership:** Support innovation responsibly while maintaining compliance with privacy laws and data handling mandates.
- **End Users (Analysts, Researchers, Staff):** Explore AI safely without fear of policy violations or data exposure.

What a Proof of Concept (PoC) Might Look Like

- Identify teams already experimenting with AI tools (communications, IT, academic departments).
- Enable the Enterprise Browser for those users and apply contextual policies on data movement and upload functions.
- Track AI site usage volume, blocked actions, and audit log completeness for 45–60 days.
- Compare AI-related incidents before and after implementation.

Outcome Scorecard: AI and Web-Based Tools

(Based on a 1,000 user organization)

Metric	Without Island	With Island	Trend
AI tool sessions occurring inside enforced browser controls	~0%	~95%	🟢↑
AI tool sessions occurring outside approved security controls	~100%	~5%	🟢↓
Unapproved AI tool usage events	~28 / month	~9 / month	🟢↓
Sensitive data submissions to AI tools	~7 / month	0	🟢↓
Approved AI tool sessions per month	0	~1,200	🟢↑
Policy enforcement success rate (AI interactions)	~80%	~98%	🟢↑
AI-related incident reports	5	1	🟢↓
Time to respond to AI-related data incidents	~4 days	~1 day	🟢↓
AI interactions logged and auditable	~70%	~99%	🟢↑

Use Case 7

Offboarding and Insider Risk - Closing the Last Mile of Control

The Scenario

Every public agency, university, or district eventually faces the same risk: the moment an employee or contractor leaves, access must end immediately.

But “immediately” rarely happens.

Credentials linger in forgotten systems. Shared passwords remain active. Files are stored on unmanaged devices. And when turnover is high — whether due to elections, contract cycles, or academic calendars — even small gaps in the process create major exposure.

Traditional controls like directory deprovisioning and VPN (Virtual Private Network) access removal are necessary but incomplete. Once someone has data saved locally or cached in a browser, control is lost.

How the Enterprise Browser Helps

The Enterprise Browser extends control to the user’s last session; the true last mile of data protection.

By embedding security and visibility directly into the browsing layer, it ensures:

- Instant deprovisioning: Access is revoked as soon as credentials are disabled — no hardware retrieval or agent removal needed.
- Session lockdown: Active sessions terminate automatically, preventing last-minute data grabs.
- Data control: Copy/paste, download, and print functions can be disabled or dynamically adjusted by user status.
- Comprehensive logging: Every action, including attempts to export data, is recorded for audit and investigation.

For example:

- A departing IT contractor loses access mid-session the moment their directory account is deactivated.
- A retiring department head’s browser session automatically wipes stored credentials and history.
- A student worker’s temporary access to a shared portal expires on schedule, with no follow-up tickets required.

Why It Matters

- **Security Leaders:** Reduce insider threat vectors by controlling access at the session level.
- **IT Teams:** Simplify offboarding. No need to chase devices, revoke VPNs, or manually wipe data.
- **Executive Leadership:** Strengthen trust and compliance posture with demonstrable control over access and auditability.
- **End Users (Managers, HR, Admins):** Gain peace of mind that access ends exactly when employment does, not days or weeks later.

What a Proof of Concept (PoC) Might Look Like

- Select one department with high turnover or contractor churn.
- Enable Enterprise Browser sessions for all staff and third-party users.
- Test automated session termination tied to directory deactivation.
- Track offboarding speed, access incidents, and audit log completion for 45 days.

Outcome Scorecard: Offboarding and Insider Risk

(Based on a 1,000 user organization)

Metric	Without Island	With Island	Trend
User sessions occurring inside enforced browser controls	~45%	~95%	🟢 ↑
User sessions occurring outside approved security controls	~55%	~5%	🟢 ↓
Average time to revoke access after separation	~3 days	~1 hour	🟢 ↓
Residual active accounts detected post-departure	~12 / year	~2 / year	🟢 ↓
Active user sessions terminated automatically upon deactivation	~40%	~98%	🟢 ↑
Unauthorized data export attempts during offboarding window	~4 / year	0	🟢 ↓
Policy enforcement success rate (departing users)	~76%	~97%	🟢 ↑
Help desk tickets related to offboarding access issues	~18 / month	~7 / month	🟢 ↓
Security audit findings related to access termination	5	1	🟢 ↓

A Practical Path Forward

Bringing Control Closer to the Work

Every security strategy in government and education shares one goal: to protect mission-critical systems without making it harder for people to do their jobs.

The Enterprise Browser delivers on that goal by bringing security closer to the user - not by adding more infrastructure, but by embedding intelligence into the browser itself.

Across the use cases in this guide, several themes emerge:

- Simplicity: Replace complex, multi-layered access models with policy control at the session level.
- Visibility: Gain real-time insight into what users do with data without installing agents or gateways.
- Consistency: Create a uniform security posture across departments, devices, and user types.
- Speed: Shorten onboarding, offboarding, and audit cycles while improving user experience.

In a world where modernization and security rarely advance together, the Enterprise Browser offers something rare: a way to achieve both.

For agencies and institutions ready to explore what this looks like in practice, the next step doesn't have to be large-scale.

Start small. Run a controlled Proof of Concept. Measure real outcomes.

In many cases, meaningful change starts not with new infrastructure, but with considering where work actually gets done. Today, that's increasingly happening in *the browser*.

Explore how *Island* is supporting the public sector.

REDLEIF Island

2026