



# Browser Risks and Commercial Comparison Report

**Internet Explorer 11 vs Chrome 44 vs  
Microsoft Edge (Current)**

**Context: Self-Service Kiosk / CUSS 2  
Applications**

**Mike Irons  
Sales@elevationsoftware.com  
April 28, 2026**



# Table of Contents

- 1. EXECUTIVE SUMMARY..... 1**
- 2. AT A GLANCE — MASTER COMPARISON..... 1**
- 3. WINDOWS 11 AVAILABILITY AND COMPATIBILITY ..... 2**
  - 3.1 INTERNET EXPLORER 11 .....2
  - 3.2 CHROME 44.....2
  - 3.3 MICROSOFT EDGE 147 .....2
- 4. SECURITY COMPARISON ..... 2**
  - 4.1 VULNERABILITY EXPOSURE .....2
  - 4.2 TLS AND ENCRYPTION .....3
  - 4.3 KEY SECURITY FEATURES MISSING IN IE11 / CHROME 44 .....3
- 6. COMMERCIAL AND LICENSING IMPLICATIONS ON WINDOWS 11..... 4**
  - 6.1 LICENSING COST COMPARISON.....4
  - 6.2 CYBER INSURANCE IMPLICATIONS.....4
  - 6.3 WINDOWS 11 KIOSK MODE — EDGE ONLY.....4
  - 6.4 IE MODE — COMMERCIAL TERMS AND TIMELINE.....5
  - 6.5 DCS AND VENDOR SUPPORT .....5
- 7. CUSS KIOSK DEPLOYMENT SUITABILITY MATRIX..... 6**
- 8. RECOMMENDATIONS ..... 6**
  - 8.1 IMMEDIATE ACTIONS .....6
  - 8.2 CUSS 2.0 MIGRATION PATH.....6
  - 8.3 TARGET ARCHITECTURE.....7

## 1. Executive Summary

This report provides a consolidated comparison of three browser environments — Internet Explorer 11, Google Chrome 44, and Microsoft Edge (current) — evaluated against security posture, Windows 11 compatibility, compliance obligations, kiosk suitability, and commercial implications. The assessment is specifically framed in the context of self-service kiosk and CUSS (Common Use Self-Service) applications in airport environments as of April 2026.

**[CRITICAL FINDING]** Both IE11 and Chrome 44 are either unavailable or non-installable on Windows 11. Windows 11 Assigned Access kiosk mode supports Microsoft Edge ONLY. CUSS 1.x was officially discontinued on 1 January 2026. Any organisation still operating IE11 or Chrome 44-based CUSS applications must treat this as an immediate security and operational incident.

## 2. At a Glance – Master Comparison

Factor	IE11	Chrome 44	Edge 147 (Current)
Release date	October 2013	July 2015	Active — Edge 147, Apr 2026
Vendor support ended	June 2022	August 2015 (~6 weeks support)	Fully supported
Years without patches (Apr 2026)	~4 years	~10 years	0 (patches within days)
Versions behind current	N/A	103 major versions	Current
Available on Windows 11	NO — not installed	NO — cannot be installed	YES — pre-installed
Win 11 Assigned Access kiosk	<b>NO</b>	<b>NO</b>	YES — only supported browser
TLS 1.3 support	<b>NO</b>	<b>NO</b>	<b>YES</b>
TLS 1.0 / 1.1 present	YES (security risk)	YES (security risk)	NO (disabled)
NPAPI attack surface	No (ActiveX instead)	YES — last Chrome with NPAPI	NO (removed)
Known unpatched CVEs (approx.)	Hundreds	Thousands (103 versions)	0 (all patched current)
Site Isolation (Spectre)	<b>NO</b>	NO (added Chrome 67)	<b>YES</b>
SameSite cookie protection	<b>NO</b>	NO (added Chrome 51)	<b>YES</b>
Subresource Integrity	<b>NO</b>	NO (added Chrome 45)	<b>YES</b>
V8 JS sandbox	N/A	NO (added Chrome 123)	<b>YES</b>
PCI DSS v4.0	<b>FAIL</b>	<b>FAIL</b>	<b>PASS</b>
Cyber Essentials v3.3 (Apr 2026)	<b>FAIL</b>	<b>FAIL</b>	<b>PASS</b>
ISO 27001	<b>GAP</b>	<b>GAP</b>	<b>PASS</b>
CUSS 2.0 compatible	<b>NO</b>	<b>NO</b>	<b>YES</b>
IE Mode available	IS IE11	<b>NO</b>	YES (free, until 2029)
Cost on Windows 11	Not applicable	Cannot install	FREE — included with Windows 11
Overall risk rating	<b>CRITICAL</b>	<b>CRITICAL</b>	<b>LOW</b>

## 3. Windows 11 Availability and Compatibility

### 3.1 Internet Explorer 11

**[NOT AVAILABLE]** IE11 is not installed on Windows 11. It was never included. Attempting to launch IE11 redirects to Edge.

Microsoft made a deliberate decision to exclude IE11 from Windows 11. The only mechanism for accessing IE11-rendered content on Windows 11 is IE Mode within Edge — which uses the Trident engine in a sandboxed tab within the Edge process, not as a standalone browser.

### 3.2 Chrome 44

**[CANNOT BE INSTALLED]** Chrome 44 (2015) cannot be installed on Windows 11. Google no longer provides installers for versions this old, and the installer binaries from 2015 are incompatible with the Windows 11 security architecture.

Any organisation that believes it is running Chrome 44 on Windows 11 is either: (a) running Windows 10 or older, not Windows 11; or (b) running an unofficial/modified build — which carries additional security risks beyond those documented in this report. In either case, the underlying browser remains critically vulnerable and unsupported.

### 3.3 Microsoft Edge 147

**[FULLY SUPPORTED]** Edge 147 is pre-installed on all Windows 11 editions. It is the default and recommended browser. No additional installation, licensing, or configuration is required.

- Deeply integrated with Windows 11 identity, security and management infrastructure
- Fully supported in Windows 11 Assigned Access (kiosk mode) — the only browser that is
- Receives security patches within days of Chromium upstream fixes
- Includes IE Mode for backward-compatible legacy application support at no cost

## 4. Security Comparison

### 4.1 Vulnerability Exposure

Vulnerability Category	IE11	Chrome 44	Edge 147
Unpatched RCE vulnerabilities	CRITICAL	CRITICAL	LOW
Memory corruption / use-after-free	CRITICAL	CRITICAL	LOW
TLS downgrade / weak cipher exposure	HIGH	HIGH	LOW
NPAPI / legacy plugin attack surface	N/A	CRITICAL	N/A
JavaScript engine (V8/Chakra) hardening	HIGH	CRITICAL	LOW
Sandbox / site isolation	HIGH	HIGH	LOW
Active CISA KEV catalog exposure	HIGH	CRITICAL	LOW
Cross-site / SOP bypass exposure	HIGH	HIGH	LOW
Passenger PII data-at-rest leakage risk	HIGH	HIGH	LOW

## 4.2 TLS and Encryption

Protocol	IE11	Chrome 44	Edge 147
TLS 1.0	Available (risk)	Available (risk)	Disabled
TLS 1.1	Available (risk)	Available (risk)	Disabled
TLS 1.2	Available (manual enable)	Available	Default minimum
TLS 1.3	NO	NO	YES — default
RC4 ciphers	Present	Present	Removed
HSTS preload	Limited	YES	YES — enforced
Cert Transparency	Limited	Partial	Enforced

## 4.3 Key Security Features Missing in IE11 / Chrome 44

The following protections, all standard in Edge 147, are absent from IE11 and Chrome 44:

Feature	Introduced	Impact of Absence
Site Isolation (Spectre mitigation)	Chrome 67 / Edge 67 (2018)	Prevents cross-origin memory leakage via CPU side-channel attacks. Critical for kiosks processing PII from multiple airlines.
SameSite Cookie Enforcement	Chrome 51 (2016)	Blocks CSRF attacks. Without this, session cookies for DCS/check-in flows can be stolen.
Subresource Integrity (SRI)	Chrome 45 (2015)	Ensures JavaScript loaded from CDNs has not been tampered with. Absent in Chrome 44 (removed the version after).
V8 Pointer Compression	Chrome 80 (2020)	Reduces V8 heap exploitation surface. Absent from Chrome 44's V8 4.4.x engine.
V8 Sandbox	Chrome 123 (2024)	Isolates V8 from the rest of the process. Not present in IE11 or Chrome 44.
HTTPS-First Mode	Chrome 94+ / Edge default 2024	Prevents downgrade attacks. Edge enforces this; IE11 and Chrome 44 do not.

## 5. Compliance and Regulatory Status

Framework	IE11	Chrome 44	Edge 147	Notes
PCI DSS v4.0	<b>FAIL</b>	<b>FAIL</b>	<b>PASS</b>	IE11/Chrome 44: unsupported software; TLS below minimum. Edge: fully compliant.
Cyber Essentials v3.3 (Apr 2026)	<b>FAIL</b>	<b>FAIL</b>	<b>PASS</b>	Updated April 2026: legacy systems without security updates must be isolated or removed.
ISO 27001:2022 (A.8.8)	<b>GAP</b>	<b>GAP</b>	<b>PASS</b>	Known unpatched CVEs with no remediation path = documented compliance gap.
GDPR / UK GDPR (Art. 32)	RISK	RISK	<b>PASS</b>	IE11/Chrome 44 cannot provide appropriate technical measures for PII processing.
NIS2 Directive	<b>FAIL</b>	<b>FAIL</b>	<b>PASS</b>	Essential services operators must maintain patched systems.
CUSS 2.0 (Jan 2026)	<b>FAIL</b>	<b>FAIL</b>	<b>PASS</b>	CUSS 1.x discontinued 1 Jan 2026. CUSS 2.0 requires TLS >1.2, HTML5, WebSocket.
Windows 11 kiosk certification	<b>FAIL</b>	<b>FAIL</b>	<b>PASS</b>	Only Edge supported in Windows 11 Assigned Access.

**[CUSS 2.0 NOTE]** CUSS 1.x platform support was officially discontinued by IATA/AEA on 1 January 2026. CUSS 2.0 mandates HTML5, OpenAPI, OAuth2, JSON, TLS > 1.2, and WebSocket. Neither IE11 nor Chrome 44 can satisfy these requirements. Edge 147 meets all CUSS 2.0 technical requirements.

## 6. Commercial and Licensing Implications on Windows 11

### 6.1 Licensing Cost Comparison

Cost Factor	IE11	Chrome 44	Edge 147
Browser licence cost	Not applicable (unavailable)	Cannot be installed	FREE — included with Windows 11
Enterprise management cost	Not applicable	Not applicable	FREE — managed via Intune / Group Policy
Chrome Kiosk & Signage Upgrade	N/A	N/A	\$25/device/year if using Chrome (not Edge)
IE Mode (legacy compat layer)	N/A	N/A	FREE — included in Edge through at least 2029
Windows 11 Enterprise E3	\$7/user/month	\$7/user/month	\$7/user/month (Edge included)
Windows 11 IoT Enterprise LTSC 2024	Not available	Not available	Pre-installed, 10-year support lifecycle
Cyber insurance premium impact	Likely VOID / increased	Likely VOID / increased	Standard rates
Cost of security breach (estimated)	High — no mitigation path	Critical — 10yr unpatched	Standard industry risk profile

### 6.2 Cyber Insurance Implications

**[WARNING]** Running unsupported browser software is grounds for denial of cyber insurance claims. Insurers actively audit for end-of-life systems during incident investigations.

The industry position as of 2026 is clear:

- Most cyber insurance policies require supported OS and applications with current patching as a policy condition
- A breach investigated with IE11 or Chrome 44 in scope is likely to result in a denied claim, citing failure to maintain "reasonable security standards"
- Premiums are increasing across the board; use of end-of-life systems is a primary underwriting risk factor
- Windows 10 reached end of support in October 2025 — any remaining Windows 10 devices with IE11 or Chrome 44 carry a compounded risk that further endangers insurance coverage

### 6.3 Windows 11 Kiosk Mode — Edge Only

**[CRITICAL COMMERCIAL FINDING]** Windows 11 Assigned Access (the native kiosk lockdown mode) supports Microsoft Edge ONLY. Chrome and all other third-party browsers are not supported in this mode.

This has direct commercial consequences for CUSS kiosk deployments:

- Any kiosk application that cannot run in Edge cannot use Windows 11's native kiosk security model
- Chrome-based kiosk shells on Windows 11 require Shell Launcher or custom scripts — adding configuration complexity, support cost, and security risk

- Edge-based kiosk applications benefit from native Microsoft Intune integration, Group Policy management, and zero-touch deployment through Windows Autopilot
- For operators standardising on Windows 11 IoT Enterprise LTSC (the recommended platform for CUSS 2.0 deployments), Edge is the pre-installed, supported, and certified browser

## 6.4 IE Mode – Commercial Terms and Timeline

IE Mode Factor	Detail
Cost	FREE — included with all Windows 11 editions and Microsoft Edge
Support end date	At least 2029 (1-year advance notice will be given before retirement)
Purpose	Backward compatibility for legacy IE11 applications within Edge — not a long-term solution
Supported in CUSS 2.0	No — CUSS 2.0 requires modern HTML5/WebSocket. IE Mode uses legacy Trident engine.
ActiveX support	Limited — full ActiveX controls not supported; basic integration only
NPAPI support	No — NPAPI is not present in Edge or IE Mode
Recommended use	Bridge for legacy internal applications only, while full CUSS 2.0 migration is completed
Migration deadline	Begin CUSS 2.0 migration now — IE Mode retirement expected 2029 at latest

## 6.5 DCS and Vendor Support

Major aviation technology vendors have aligned their support positions:

- **DCS Vendors:** Amadeus, Sabre, and Travelport all reference Edge IE Mode as the supported compatibility path for legacy DCS integrations — not standalone IE11 or Chrome 44
- **IATA CUSS 2.0:** IATA CUSS 2.0 specification (effective January 2026) requires a modern browser engine supporting HTML5, OAuth2, OpenAPI, TLS > 1.2, and WebSocket — satisfied only by Edge or current Chrome
- **Microsoft:** Microsoft provides official documentation and support for Edge in airport/kiosk configurations through the Windows IoT Enterprise programme
- **Support Availability:** No commercial support contract is available for IE11 or Chrome 44 — any organisation operating these browsers is entirely self-supported

## 7. CUSS Kiosk Deployment Suitability Matrix

Requirement	IE11	Chrome 44	Edge 147
Runs on Windows 11	NO	NO	YES
Windows 11 Assigned Access support	NO	NO	YES
CUSS 2.0 HTML5/WebSocket compatible	NO	NO	YES
TLS 1.3 for DCS/baggage API calls	NO	NO	YES
Passport scan / biometric integration	LIMITED	LIMITED	YES
Real-time ops portal monitoring	LIMITED	NO	YES
OAuth2 / SSO for staff functions	NO	NO	YES
Proactive maintenance scheduling	NO	NO	YES
Security patches within days	NO	NO	YES
PCI DSS compliant	NO	NO	YES
Cyber insurance compatible	NO	NO	YES
Free on Windows 11	NO	NO	YES
Vendor-supported (DCS/IATA)	NO	NO	YES
IE Mode legacy fallback available	N/A	NO	YES

## 8. Recommendations

### 8.1 Immediate Actions

- Conduct a full audit of all kiosk and operational systems to identify any IE11 or Chrome 44 dependencies — and confirm whether those systems are running Windows 10 or Windows 11
- Escalate IE11 and Chrome 44 kiosk deployments to security and compliance teams as critical risk items requiring immediate remediation plans
- Isolate any Chrome 44 or IE11-based kiosks from networks carrying cardholder or passenger PII data until migration is complete
- Notify your cyber insurer of the legacy browser position and obtain written guidance on coverage implications
- If still on Windows 10, accelerate the Windows 11 migration — Windows 10 reached end of support in October 2025

### 8.2 CUSS 2.0 Migration Path

- **Option 1 — Build with Elevation SDK:** The Elevation SDK provides device abstraction, DCS integration support, OAuth2/OpenAPI wrappers, and CUSS 2.0-compliant API bindings — enabling your development team to build a modern, Edge-compatible kiosk application without starting from scratch.



- **Option 2 — Managed Build by Elevation AI:** Elevation AI can deliver a fully functional CUSS 2.0 application — check-in, bag tag printing, seat selection, passport scanning — running on Edge 147 on Windows 11 IoT Enterprise, deployed in weeks. Integrated from day one with the Elevation AI Portal for real-time monitoring, ops-centre alerting, and maintenance scheduling.
- **Interim — Edge IE Mode:** For any legacy IE11 application dependencies that cannot yet be rebuilt, deploy Edge IE Mode as a zero-cost bridge. Explicitly scope this as a temporary measure with a firm CUSS 2.0 migration deadline before IE Mode's expected 2029 retirement.

### 8.3 Target Architecture

- Platform: Windows 11 IoT Enterprise LTSC 2024 — 10-year support lifecycle, purpose-built for kiosk deployments
- Browser: Microsoft Edge 147+ — pre-installed, managed via Intune/Group Policy, Assigned Access native support
- Application: CUSS 2.0 compliant — HTML5, TLS 1.3, OAuth2, WebSocket, OpenAPI
- Monitoring: Elevation AI Portal — real-time device status, session analytics, maintenance scheduling, ops-centre alerting
- Management: Windows Autopilot + Microsoft Intune — zero-touch deployment, remote management, security policy enforcement

*Sources: Microsoft Edge Lifecycle Documentation; Microsoft Learn — IE Mode, Assigned Access, Windows 11 IoT Enterprise; IATA CUSS 2.0 Specification; IASME Cyber Essentials v3.3 (April 2026); PCI DSS v4.0; CISA Known Exploited Vulnerabilities Catalog; Google Chrome Enterprise Documentation; endoflife.date/chrome; endoflife.date/internet-explorer; NVD CVE Database.*