



دراسة تأثير أمان واجهة برمجة التطبيقات لعام 2024

الحكومة

تتزايد حوادث واجهات برمجة التطبيقات. تعرف على كيفية تعامل الحكومة مع هذه المشكلة الأمنية الكبيرة — وما يمكن لمؤسستك فعله للحفاظ على سلامتها.

أبلغت **86.1%** من المؤسسات الحكومية عن تعرضها لحادث أمني متعلق بواجهات برمجة التطبيقات في عام 2024 — وذلك يُعد زيادة كبيرة على نسبة 76.8% في عام 2023

717,500 دولار هو متوسط التكلفة المالية لخرق أمان واجهة برمجة التطبيقات للمؤسسات الحكومية في الولايات المتحدة، وهو ما يتجاوز متوسط الصناعة بأكملها البالغ 591,404 دولارات

تحتفظ **66.9%** من الهيئات الحكومية بجدول واجهات برمجة التطبيقات، ومع ذلك، فإن 18.5% منها فقط لديها رؤية كاملة لواجهات برمجة التطبيقات التي تتعامل مع البيانات الحساسة، ما يعرض المعلومات المهمة للخطر

أهم 3 تأثيرات

1. زيادة التوتر والضغط على فرق الأمان
2. الإضرار بسعة الفريق لدى القادة ومجالس الإدارة
3. توقيف الغرامات التنظيمية لعدم الامتثال

المصدر:

دراسة تأثير أمان واجهة برمجة التطبيقات لعام 2024

بالنسبة إلى الهيئات الحكومية، تكون تكاليف هجمات واجهات برمجة التطبيقات باهظة، ويشمل ذلك التأثيرات المالية والبشرية. إن فقدان الثقة على مستوى القيادة بسبب الخروقات قد يعني زيادة التدقيق، والاضطرابات التشغيلية، والمزيد من العمل للفريق التي تعاني بالفعل من ضغط شديد وتكافح من أجل تلبية متطلبات الامتثال.

تتعرض الحكومات حول العالم لضغوط متزايدة لتأمين الخدمات الرقمية في عصر يعتمد على واجهات برمجة التطبيقات بشكل أساسي. في عام 2024، أبلغت 86.1% من مؤسسات القطاع العام عن وقوع حادث أمني يتعلق بواجهة برمجة التطبيقات — وذلك يُعد قفزة حادة من 76.8% في العام السابق. تضع هذه الزيادة القطاع العام فوق متوسط الصناعة بأكملها البالغ 84%، ما يسلط الضوء على حجم التحدي المتزايد. بدءًا من تلبية متطلبات **اللائحة العامة لحماية البيانات (GDPR)** إلى فرض إقامة البيانات عبر أنظمة السحابة المتعددة ومواجهة التهديدات الأمنية السيادية، تواجه الهيئات حاجة عالمية إلى رؤية أكبر وحوكمة أقوى ومرونة مدمجة.

التكلفة الحقيقية لحوادث أمان واجهة برمجة التطبيقات الحكومية

تعتمد الهيئات الحكومية بشكل متزايد على واجهات برمجة التطبيقات لتمكين الخدمات الرقمية وتسهيل مشاركة البيانات بين الهيئات وتحديث البنية التحتية. لكن هذا الاتجاه أدى إلى ظهور مجموعة من الثغرات الأمنية الجديدة التي تحرص الجهات التخريبية على استغلالها. لقد أدت آليات المصادقة الضعيفة وتكوينات واجهة برمجة التطبيقات الخطأ وعدم الوعي الكافي بمؤشرات المخاطر الحرجة إلى جعل الحكومة عرضة بشكل خاص لحادث خروقات أمان واجهة برمجة التطبيقات. تمتد عواقب هذه الحوادث إلى ما هو أبعد من سرقة البيانات حيث تشكل مخاطر على استمرارية التشغيل والامتثال التنظيمي وثقة الجمهور.

كيف نعرف ذلك؟ أجرت شركة Akamai استطلاع رأي لأكثر من 1,200 متخصص في تكنولوجيا المعلومات والأمن — من كبار مسؤولي أمن المعلومات إلى موظفي أمن التطبيقات — للتعرف على تجاربهم مع التهديدات المرتبطة بواجهات برمجة التطبيقات.

هنا، قمنا بتصنيف النتائج التي توصلنا إليها من المشاركين في الاستطلاع من الجهات الحكومية، الذين قالوا إن أبرز تداعيات حوادث أمان واجهة برمجة التطبيقات لديهم كانت كما يأتي:

- "زيادة التوتر و/أو الضغط على الفريق/القسم" (28.5%)
- "الإضرار بسعة قسمنا لدى كبار القادة و/أو مجلس الإدارة" (27.2%)
- "توقيف غرامات من الجهات التنظيمية" (25.2%)

من السهل فهم هذه العواقب الممتشابهة، نظرًا إلى أن الأقران قد حددوا تكلفة معالجة حوادث واجهة برمجة التطبيقات بنحو 717,500 دولار أمريكي — أي أعلى بنسبة 21.3% من المتوسط في كل الصناعات الثماني التي شملها الاستطلاع.

تابع القراءة للحصول على رؤى خاصة بالمجال من **دراسة تأثير أمان واجهة برمجة التطبيقات لعام 2024**.

مع زيادة الهجمات، أصبح مستوى الرؤية مصدر قلق متزايدًا

عندما طُلب ذكر أهم أسباب حوادث أمان واجهة برمجة التطبيقات، حدد الأقران ثغرتين رئيسيتين:

- نقص ضوابط مصادقة واجهة برمجة التطبيقات (25.2%)
- الأدوات التقليدية المستخدمة لتأمين واجهات برمجة التطبيقات (25.2%)

على الرغم من الأدلة المتزايدة على عواقب تهديدات واجهة برمجة التطبيقات — من تكاليف المعالجة المرتفعة إلى فقدان الثقة — فإن النتائج التي توصلنا إليها تشير إلى أن العديد من الفرق الحكومية لم تضع أمان واجهة برمجة التطبيقات على رأس أولوياتها بعد. في الواقع، يحتل أمان واجهة برمجة التطبيقات المرتبة السادسة بين أولويات الأمن السيبراني للعام المقبل بنسبة 17.9%.



وكما هو الحال في القطاع الخاص، يصعب على الجهات الحكومية التمييز بين نشاط واجهة برمجة التطبيقات الحقيقي والضرر. يرجع هذا، جزئيًا، إلى ضعف مستوى الرؤية في ما يتعلق بالأماكن التي تكون فيها واجهات برمجة التطبيقات عرضة للخطر على وجه التحديد. بينما يقول 66.9% من الأقران إن لديهم جردًا كاملاً لواجهات برمجة التطبيقات الخاصة بهم، فإن 18.5% فقط من هؤلاء يعرفون أي الواجهات يُرجع بيانات حساسة، بما في ذلك معلومات التعريف الشخصية (PII) مثل رقم الهوية الوطنية والبيانات البيومترية ومعلومات الاتصال.

ضع في حسابك ما يمكن أن يحدث لواجهة برمجة تطبيقات غير مصرح بها تم نشرها بواسطة قسم أو شركة تابعة لمؤسسة حكومية من دون تعاون أو إشراف من فرق تكنولوجيا المعلومات أو الأمان المركزية الحديثة.

قد تكون واجهة برمجة التطبيقات هذه:

- مصممة لتوفير الوصول إلى البيانات الشخصية أو المالية للمواطنين من دون ضوابط التفويض الملائمة، ما قد يؤدي إلى الكشف عن معلومات حساسة
 - تم استبدالها بإصدار جديد لكن لم يتم إيقاف تشغيلها بشكل صحيح، ما يترك نقطة نهاية قديمة عرضة للاستغلال
 - تعمل خارج مستوى رؤية فرق تكنولوجيا المعلومات والأمان المركزية، متجنبًا أدوات المراقبة التقليدية وفحوصات الامتثال
 - تم استغلالها من قبل جهات خبيثة للوصول غير المصرح به إلى الأنظمة الحكومية، ما قد يؤدي إلى حدوث خروقات للبيانات أو سرقة الهوية أو الاحتيال المالي
- هذا ليس مجرد افتراض — فمشهد الأمن السبراني بالنسبة إلى الوكالات الحكومية الأمريكية يفرض تحديات كبيرة. وفقًا لمؤشر الأعمال الرقمية من Cybernews، يواجه العديد من الهيئات والإدارات الحكومية صعوبة في الحفاظ على مواقف أمنية قوية، حيث تحصل نحو 4 من كل 10 منها (38.8%) على تصنيفات "مخاطر حرجية" في تقييماتها، ويشهد 75% منها اختراقًا للبيانات.

تعكس هذه الإحصائيات الواقع المعقد الذي يواجه الفرق الأمنية الحكومية، التي يتعين عليها أن توازن بين أهداف المهمة والأنظمة القديمة والتهديدات المتطورة مع العمل تحت قيود وتدقيق فريدين. مع تفاقم هذه التحديات، خاصة في مجال أمن واجهة برمجة التطبيقات، تحتاج الهيئات إلى شركاء يفهمون متطلباتها الخاصة ويمكنهم تقديم حلول مصممة خصيصًا للبيئات الحكومية.

كيف تؤثر حوادث واجهة برمجة التطبيقات في الثقة والتكلفة والضغط على الفريق




نظرًا إلى تكرار هجمات واجهة برمجة التطبيقات وتكاليفها، فلا عجب أن يصبح تأمين واجهات برمجة التطبيقات أولوية متزايدة بالنسبة إلى الحكومات حول العالم. في الولايات المتحدة، تعمل مبادرة Data.gov، التي تديرها إدارة الخدمات العامة، على توحيد واجهات برمجة التطبيقات عبر الهيئات الفيدرالية لتحسين الاتساق والأمان وقابلية التشغيل التفاعلي. تُبذل جهود مماثلة على مستوى العالم — بدءًا من أطر البيانات المفتوحة في الاتحاد الأوروبي والمملكة المتحدة إلى مبادرات التحول الرقمي في مختلف أنحاء منطقتي آسيا والمحيط الهادئ والشرق الأوسط، حيث تتبنى الحكومات واجهات برمجة تطبيقات موحدة لضمان تبادل البيانات بشكل آمن وسلس.

يتوافق العديد من هذه المبادرات مع اللوائح الإقليمية، مثل اللائحة العامة لحماية البيانات الخاصة بالاتحاد الأوروبي ونظام الإبلاغ عن خروقات البيانات في أستراليا وقانون الرقم الشخصي في اليابان. من خلال فرض المعايير والأطر المشتركة، تعمل الحكومات على ضمان التبادل الآمن للبيانات مع الحد من المخاطر الناجمة عن عمليات التكامل مع جهات خارجية والوصول غير المصرح به.

من الواضح أن الهيئات الحكومية تدرك تمامًا عواقب تهديدات واجهات برمجة التطبيقات. ولأول مرة، طلبنا من المشاركين في البلدان الثلاثة التي شملها الاستطلاع مشاركة التأثير المالي المقدر لحوادث أمان واجهات برمجة التطبيقات التي تعرضوا لها خلال آخر 12 شهرًا.

على الرغم من أن التأثيرات المالية كبيرة، فقد سمعنا بكل وضوح من المشاركين في الدراسة أن التكاليف تتجاوز بكثير هذه المحصلة المالية.

عندما طلب منهم ذكر أهم التأثيرات الناجمة عن حوادث أمان واجهات برمجة التطبيقات، لم تكن الإجابة هي التكلفة. كما ذكرنا سابقًا، أشار المشاركون في الاستطلاع إلى "زيادة التوتر و/أو الضغط على الفريق/القسم" و"الإضرار بسمعة القسم لدى كبار القادة و/أو مجلس الإدارة" بمنزلة التأثيرين الرئيسيين.

متوسط جميع الصناعات	الحكومة	
591,404.01 دولارًا	717,500.50 دولارًا	 الولايات المتحدة
420,103.18 جنيهًا إسترلينيًا	378,140.69 جنيهًا إسترلينيًا	 المملكة المتحدة
403,453.26 يورو	296,975.79 يورو	 ألمانيا

س3. إذا تعرضت لحادث أمان متعلق بواجهة برمجة التطبيقات، فماذا كان إجمالي التأثير المالي المقدر لهذه الحوادث مجتمعة؟ يُرجى تضمين جميع التكاليف ذات الصلة مثل إصلاحات النظام ووقت التوقف عن العمل والرسوم القانونية والغرامات وأي نفقات أخرى مرتبطة.

تترك هذه العواقب أثرًا دائمًا. تؤدي الخروقات إلى فقدان الثقة، ما قد يعرض التمويل المستقبلي للخطر ويضعف ثقة الجمهور. وفي الوقت نفسه، قد تؤدي خسائر الإنتاجية في الهيئات التي تعمل تحت ضغط بالفعل إلى الإرهاق وانخفاض مستوى مشاركة القوى العاملة.

لكن الضغط لا يقتصر على بعض المناطق. على الرغم من تركيز هذا التقرير على أسواق محددة، فإن أمان واجهة برمجة التطبيقات أصبح يشكل قضية بالغة الأهمية بالنسبة إلى مؤسسات القطاع العام حول العالم، حيث تواجه الهيئات في منطقة آسيا والمحيط الهادئ وأمريكا اللاتينية وغيرها تحديات مماثلة في تأمين البنية التحتية الرقمية وتلبية معايير الامتثال وحماية البيانات الحساسة من التهديدات المتطورة.

تقليل المخاطر والتوتر من خلال أمان واجهة برمجة التطبيقات الاستباقي

تتزايد هجمات واجهات برمجة التطبيقات ضد الحكومة من حيث النطاق والحجم والتعقيد والتكلفة. يشمل ذلك هجمات الروبوتات التي تعمل بالذكاء الاصطناعي التوليدي (GenAI) والتي تتكيف بسرعة لتتجاوز أدوات أمان واجهات برمجة التطبيقات التقليدية وغيرها من الدفاعات المحيطة. يواجه العديد من فرق الأمان في مجال هذه التهديدات بشكل مباشر ويشعر بالتأثيرات المالية والبشرية على حد سواء. لكن حتى عندما تدرك المؤسسات خطورة تهديدات واجهة برمجة التطبيقات، يبقى لديها السؤال: ماذا يمكننا أن نفعل حيال ذلك؟

إن اتخاذ التدابير اللازمة الآن لتأمين واجهات برمجة التطبيقات الخاصة بك بشكل أفضل -البيانات المتبادلة بينها- من شأنه أن يمكّن مؤسستك من حماية إيراداتها وبياناتها الحساسة، وتخفيف العبء على فرق الأمان، مع الحفاظ على ثقة مجالس الإدارة وقادة الحكومة المكتسبة بشق الأنفس. تتضمن هذه التدابير زيادة معرفة فريقك بتهديدات واجهات برمجة التطبيقات المتقدمة والقدرات اللازمة للتصدي لها.

هل أنت مستعد لإجراء محادثة حول التحديات التي تواجهها وكيف يمكن لشركة Akamai مساعدتك؟

طلب عرض توضيحي مخصص لأمان واجهة برمجة التطبيقات من شركة

لقراءة التقرير الكامل والتعرف على أفضل الممارسات لتحسين مستوى رؤية واجهة برمجة التطبيقات وحمايتها، قم بتنزيل

دراسة تأثير أمان واجهة برمجة التطبيقات لعام 2024.



تحمي وسائل الأمان المقدمة من شركة Akamai التطبيقات التي تقود أعمالك في كل نقطة من نقاط التفاعل، من دون المساس بالأداء أو تجربة العملاء. من خلال الاستفادة من حجم منصتنا العالمية ومستوى رؤيتها للتهديدات، نتعاون معك لمنع التهديدات واكتشافها والتخفيف من أثارها — حتى تتمكن من بناء الثقة في العلامة التجارية وتحقيق رؤيتك. أطلع على المزيد من المعلومات حول حلول Akamai للحوسبة السحابية والأمن وتسليم المحتوى على akamai.com و akamai.com/blog، أو تابع حساب Akamai Technologies على [LinkedIn](https://www.linkedin.com/company/akamai) و [X](https://twitter.com/Akamai). تم النشر في 25/05.

2024 API SECURITY IMPACT STUDY

Government

API incidents are on the rise. Learn how the government is addressing this top security concern — and what your organization can do to stay safe.

Governments around the world are under growing pressure to secure digital services in an **API-first era**. In 2024, 86.1% of public sector organizations reported an API security incident — a sharp jump from 76.8% the year before. This increase places the public sector above the all-industry average of 84%, underscoring the growing scale of the challenge. From meeting [General Data Protection Regulation \(GDPR\)](#) requirements to enforcing data residency across multicloud systems and confronting sovereign security threats, agencies face a universal need for greater visibility, stronger governance, and built-in resilience.

The true cost of government API security incidents

Government agencies are increasingly adopting APIs to enable digital services, facilitate interagency data sharing, and modernize infrastructure. But this trend has introduced a host of new vulnerabilities that threat actors are eager to exploit. Poor authentication mechanisms, API misconfigurations, and insufficient awareness of critical risk indicators have left the government particularly susceptible to API security breaches. The consequences of these incidents extend far beyond data theft by posing risks to operational continuity, regulatory compliance, and public trust.

How do we know this? Akamai surveyed more than 1,200 IT and security professionals — from chief information security officers to application security staff — to learn about their experiences with API-related threats.

Here, we've filtered our findings for government respondents, who said the top impacts of their API security incidents were:

- "Increased stress and/or pressure for the team/department" (28.5%)
- "It hurt our department's reputation with senior leaders and/or board of directors" (27.2%)
- "Fines from regulators" (25.2%)

These intertwined consequences are easy to understand, given that your peers placed the cost of addressing API incidents at US\$717,500 — 21.3% higher than the average across all eight industries surveyed.

Read on to gain industry-specific insights from the [2024 API Security Impact Study](#).

As attacks rise, visibility is a growing concern

When asked to cite the top causes of their API security incidents, your peers identified two key vulnerabilities:

- Lack of API authentication controls (25.2%)
- Traditional tools used for securing APIs (25.2%)

Despite mounting evidence of the consequences of API threats — from high remediation costs to an erosion of trust — our findings suggest many government teams have yet to make API security a top priority. In fact, API security ranks sixth among cybersecurity priorities for the year ahead at 17.9%.

86.1% of government organizations reported experiencing an API security incident in 2024 — a significant increase from 76.8% in 2023

\$717,500 is the average financial cost of an API security breach for government organizations in the United States, exceeding the all-industry average of \$591,404

66.9% of government entities maintain an **API inventory**, yet only 18.5% have full visibility into which APIs handle sensitive data, leaving critical information at risk

Top 3 impacts

1. **Increased stress and pressure on security teams**
2. **Damaged team's reputation with leaders and board**
3. **Regulatory fines for noncompliance**

Source:
[2024 API Security Impact Study](#)

For government agencies, the costs of API attacks are steep — including financial and human impacts. Losing trust at the leadership level because of breaches can mean increased scrutiny, operational disruptions, and more work for teams that are already stretched thin and struggling to meet compliance demands.



Just like in the private sector, it’s challenging for government agencies to distinguish between genuine and malicious API activity. This is due, in part, to low visibility into precisely where APIs are vulnerable. While 66.9% of your peers say they have a full inventory of their APIs, only 18.5% of that subset know which ones return sensitive data, including personally identifiable information (PII) such as national ID number, biometric data, and contact information.

Consider what can happen to an unauthorized API deployed by a department or subsidiary of a government organization without collaboration or oversight of up-to-date central IT or security teams.

That API may have been:

- Designed to provide access to citizens’ personal or financial data without proper authorization controls, potentially exposing sensitive information
- Replaced by a new version but not properly decommissioned, leaving an outdated endpoint vulnerable to exploitation
- Operating outside the visibility of central IT and security teams, evading traditional monitoring tools and compliance checks
- Exploited by malicious actors to gain unauthorized access to government systems, potentially leading to data breaches, identity theft, or financial fraud




This isn’t just hypothetical – the cybersecurity landscape for U.S. government agencies presents significant challenges. According to the [Cybernews Business Digital Index](#), many government agencies and departments are struggling to maintain robust security postures, with nearly 4 in 10 (38.8%) receiving “critical risk” ratings in their assessments, and 75% experiencing a data breach.

These statistics reflect the complex reality facing government security teams, who must balance mission objectives, legacy systems, and evolving threats while operating under unique constraints and scrutiny. As these challenges intensify, especially in the realm of API security, agencies need partners who understand their specific requirements and can provide solutions tailored to government environments.

How API incidents impact confidence, cost, and team stress

Given the frequency and costs of API attacks, it’s no surprise that securing APIs is a growing priority for governments worldwide. In the United States, the [Data.gov](#) initiative, managed by the General Services Administration, standardizes APIs across federal agencies to improve consistency, security, and interoperability. Similar efforts are underway globally – from open data frameworks in the European Union and United Kingdom to digital transformation initiatives across the Asia-Pacific and Middle East regions, where governments are adopting standardized APIs to ensure secure and seamless data exchanges.

Many of these initiatives align with regional regulations such as the EU’s GDPR, Australia’s Notifiable Data Breaches scheme, and Japan’s My Number Act. By enforcing common standards and frameworks, governments are working to ensure secure data exchange while reducing risks from third-party integrations and unauthorized access.

	Government	Average of all industries
 United States	\$717,500.50	\$591,404.01
 United Kingdom	£378,140.69	£420,103.18
 Germany	€296,975.79	€403,453.26

Q3. If you have experienced an API security incident, what has been the estimated total financial impact of these incidents combined? Please include all related costs such as system repairs, downtime, legal fees, fines, and any other associated expenses.

It's clear that government agencies are keenly aware of the consequences of API threats. For the first time, we asked respondents in the three countries we surveyed to share the estimated financial impact of the API security incidents they experienced in the past 12 months.

While the financial impacts are significant, we heard loud and clear from study participants that the costs go far beyond the bottom line.

When asked to list the top impacts of an API security incident, it wasn't cost. As mentioned earlier, our respondents indicated "increased stress and/or pressure for the team/department" and "it hurt our department's reputation with senior leaders and/or board of directors" as the top two.

These consequences leave a lasting impact. Breaches erode trust, which can jeopardize future funding and weaken public confidence. At the same time, productivity losses in already stretched agencies can drive burnout and lower workforce engagement.

But the pressure isn't limited to a few regions. Although this report focuses on select markets, API security has become a critical issue for public sector organizations worldwide, as agencies in Asia-Pacific, Latin America, and beyond face similar challenges in securing digital infrastructure, meeting compliance standards, and protecting sensitive data from evolving threats.

Reduce risk and stress through proactive API security

API attacks against the government are growing in scope, scale, sophistication, and cost. This includes GenAI-fueled bot attacks that quickly adapt to bypass traditional API security tools and other perimeter defenses. Many security teams in your industry are experiencing these threats firsthand and feeling the impacts, both financial and human. But even when organizations understand the significance of API threats, they're left with the question: What can we do about it?

Taking measures now to better secure your APIs — and the data they exchange — can empower your organization to protect its revenue and sensitive data, and alleviate the burden from security teams, all while preserving the hard-earned trust of boards of directors and government leaders. These measures include building your team's knowledge about advanced API threats and the capabilities you need to defend against them.



To read the full report and learn about best practices for API visibility and protection, download the **2024 API Security Impact Study**.

Ready for a conversation about your challenges and how Akamai can help?

Request a customized Akamai API Security demo



Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats — so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on [X](#) and [LinkedIn](#). Published 05/25.