FORRESTER®

Improved Visibility Reduces Compliance Risk In Financial Services

Leverage Trusted Vendors For Comprehensive Risk Insight

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY AKAMAI | OCTOBER 2024

Shine The Light On Hidden Risk With Comprehensive Visibility

Increasing threat levels, expanding attack surfaces, higher regulatory scrutiny, and stricter risk management requirements are some issues that make financial services institutions vulnerable today. Invisible risks exist; and a lack of visibility is costing organizations substantial time, money, and trust.

In September 2024, Akamai commissioned Forrester Consulting to explore the impact of an incomplete view of cyber risks and how financial services institutions plan to mitigate them. We found that many organizations have suffered financial and reputational loss due to material impact events and noncompliance — the hardest hit were those who were using many vendors to monitor risk. Nine in 10 respondents said their organizations should prioritize engaging trusted vendors who provide comprehensive visibility to improve their ability in mitigating risk and addressing current and future regulations.

Key Findings

Many financial institutions have suffered material impact events and noncompliance issues due to a lack of visibility — causing revenue loss, operational disruption, and reputational damage.

Vendor sprawl significantly increases the risk of material impact events. In addition to piecemealed tooling, organizational silos and limited team resources reduce visibility.

Enabling comprehensive visibility to mitigate compliance risk will require engaging fewer vendors — allowing you to engage only trusted vendors with an intimate understanding of the financial services industry.

Invisible Risks Exist Due To A Lack Of Visibility

The cyber risk landscape is growing by the day. Being able to detect risks and respond quickly enough to mitigate damage requires visibility into an organization's users, assets, applications, sensitive data, and infrastructure. Yet, less than half of respondents had confidence in their organization's ability to detect risks in these areas and move fast enough to avoid consequences (e.g., fines and noncompliance). A lack of visibility into and/or across these areas is likely to blame: 52% of respondents agreed/strongly agreed that their organization lacks full visibility of all its users, assets, infrastructure, and applications.

52% of respondents agreed/strongly agreed that their organization lacks full visibility of all its users, assets, infrastructure, and applications.

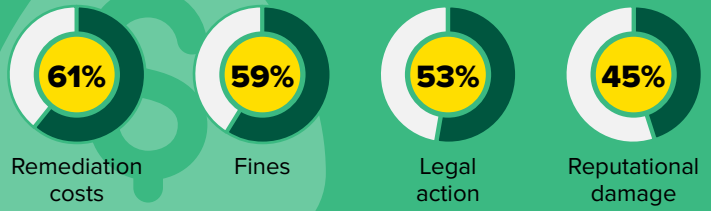
"How confident are you that your organization can detect and respond quickly enough to all vulnerabilities and threats in the following areas?"

Base: 322 global directors and above in compliance, risk, IT, and/or operations at financial services institutions with at least $500 million in annual revenue
Source: Forrester's Q3 2024 FinServ Cybersecurity Visibility Survey [E-61244]

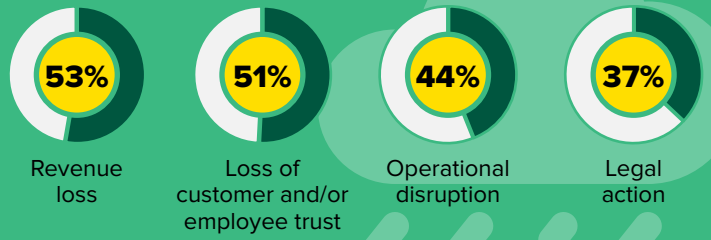
This Lack Of Visibility Is Draining Financial Services Institutions

Respondents admitted their organizations lack full visibility of their environments, and that they struggle to detect and respond to all threats and vulnerabilities, but what is the cost to the business? We found that nearly nine in 10 organizations have suffered at least one material impact event in the past 18 months, resulting in revenue loss, operational disruption, legal action, and a loss of customer and employee trust. Most organizations have also faced noncompliance, which has resulted in remediation costs, fines, legal action, and reputational damage. The consequences of unidentified risks are real — and costly.

Organizations That Have Experienced The Following Due To Regulatory Noncompliance In The Past 18 Months



Impact To Organizations That Experienced At Least One Material Impact Event In The Past 18 Months*

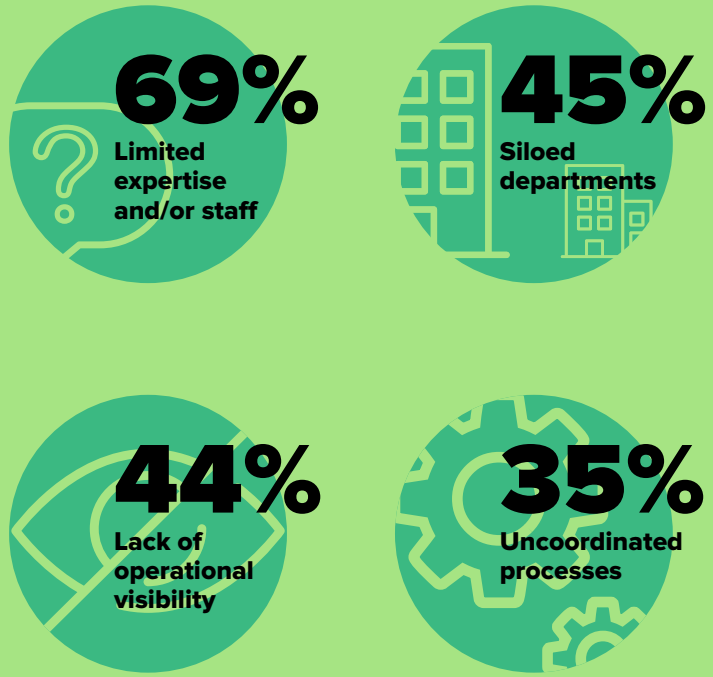


Base: 322 global directors and above in compliance, risk, IT, and/or operations at financial services institutions with at least $500 million in annual revenue
*Base: 283 global directors and above in compliance, risk, IT, and/or operations at financial services firms with at least $500 million in annual revenue that have suffered at least one material impact event in the past 18 months
Source: Forrester's Q3 2024 FinServ Cybersecurity Visibility Survey [E-61244]

Resource Constraints And Operational Silos Are Top Organizational Challenges

It is difficult to have a holistic understanding of your organization's cyber risk landscape when IT departments are not collaborating with one another, or when there is a lack of expertise to draw the right insights together. Sixty-nine percent of respondents noted that limited expertise and/or staff was a top reason material impact and noncompliance events occurred at their firms — and 49% of respondents said this lack of expertise prevents them from capturing a full view of their environment and sharing it with compliance teams. Forty-five percent of respondents also said siloed departments are to blame and 51% of respondents said their organization lacks consistent communication and integration points for their application and infrastructure teams.

Internal Reasons That Contributed To Material Impact Event(s) And/Or Noncompliance Issues



Base: 292 global directors and above in compliance, risk, IT, and/or operations at financial services institutions with at least $500 million in annual revenue that experienced material impact event(s) and/or regulatory noncompliance issues in the past 18 months
Source: Forrester's Q3 2024 FinServ Cybersecurity Visibility Survey [E-61244]

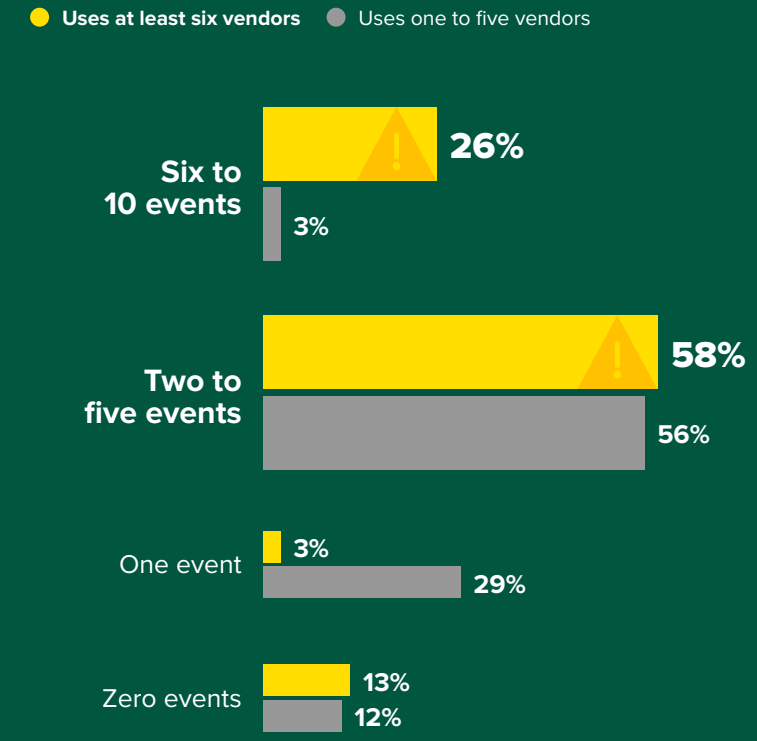
Vendor Sprawl Increases Organizational Risk

One of the most significant findings from this study is that organizations that use six or more vendors for full visibility into their environments are 1.4 times more likely to have suffered multiple material impact events in the past 18 months, and eight times more likely to have suffered at least six impact events. Sixty-one percent of respondents also called out ineffective and/or piecemeal tooling as a top reason for experiencing material impact events and/or noncompliance issues. While vendor consolidation introduces its own risks, there's a happy middle ground as organizations strive to improve risk visibility. In this study, those using not more than five trusted vendors experienced significantly fewer incidents.

61%

of respondents noted that ineffective and/or piecemeal tooling contributed to material impact events and/or noncompliance issues in the past 18 months.

Number Of Material Impact Events Suffered By Organizations In The Past 18 Months

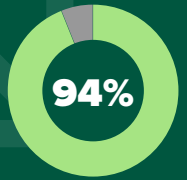


Base: 322 global directors and above in compliance, risk, IT, and/or operations at financial services institutions with at least $500 million in annual revenue
Source: Forrester's Q3 2024 FinServ Cybersecurity Visibility Survey [E-61244]

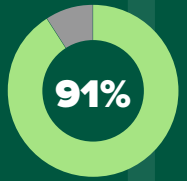
Short-List Vendors To Combat Sprawl And Resource Gaps

Given that vendor sprawl and a lack of internal expertise and resources were the top hurdles, it should be no surprise that nine in 10 respondents seek to engage partners with proven success in the financial services industry. They look for trusted partners that offer expertise and solutions across all vectors — users, applications, infrastructure, and assets — to enable comprehensive visibility.

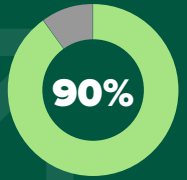
"How important are the following to improving your organization's ability to address current and future regulations?"



Enabling holistic visibility



Enabling a solution provider with proven success in my organization's industry



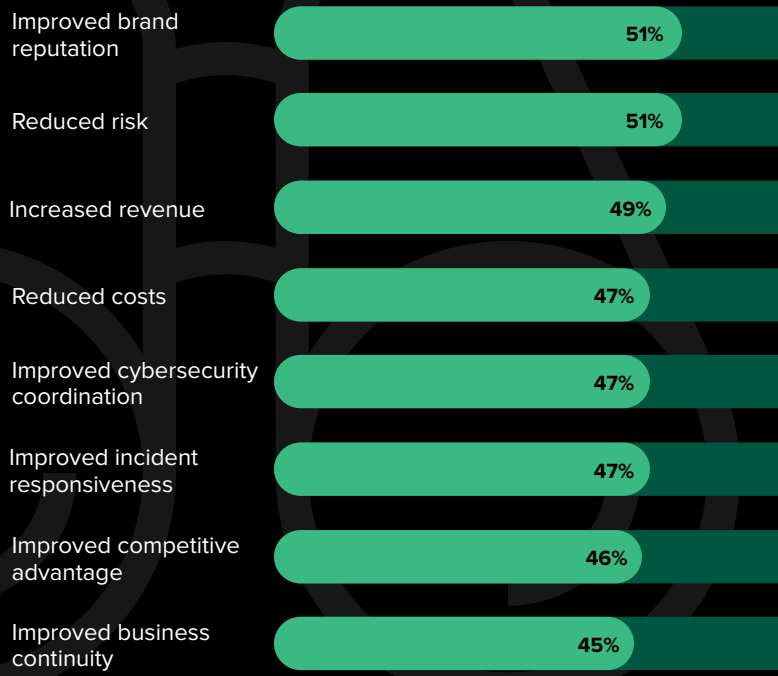
Engaging a technology partner that provides user, application, infrastructure, and asset visibility

Base: 322 global directors and above in compliance, risk, IT, and/or operations at financial services institutions with at least $500 million in annual revenue
Note: Showing sum of responses for "Important" and "Very Important."
Source: Forrester's Q3 2024 FinServ Cybersecurity Visibility Survey [E-61244]

Mitigate Risk With Trusted Partners Whose Solutions Facilitate Comprehensive Visibility

Engaging fewer but more trusted partners whose solutions enable comprehensive visibility can mitigate risk. The very consequences respondents have faced (e.g., reputational damage and fines) are reflected inversely in the benefits they anticipate: improved brand reputation (51%), reduced risk (51%), increased revenue (49%), reduced costs (47%), and improved cyber coordination (47%). Enhanced visibility will enable organizations to mitigate risks that cause material impact events. For example, improved visibility into network traffic and user behavior enables earlier attack detection, allowing security teams to contain incidents faster and minimize data loss. By monitoring application traffic and tracking user activities, organizations can generate audit logs and reports, ensuring compliance with industry standards and regulations.

Benefits Expected From Engaging A Technology Partner Whose Solutions Enable Holistic Visibility



Base: 322 global directors and above in compliance, risk, IT, and/or operations at financial services institutions with at least $500 million in annual revenue
Source: Forrester's Q3 2024 FinServ Cybersecurity Visibility Survey [E-61244]

Conclusion

Financial services institutions struggle to gain full visibility of their users, applications, infrastructure, and assets, and they blame that lack of visibility for the material impact events that they have suffered. To reduce the chances of material impact events and noncompliance, risk and compliance professionals must reduce vendor sprawl and:

- Take an inventory of the various tools and vendors in their environment and identify gaps in protection and areas where silos and lack of context inhibit visibility.
- Streamline and consolidate their environment by focusing on a few trusted vendors with deeper subject matter expertise and industry knowledge.
- Monitor the number of material impact events and the associated remediation costs to measure success.

Resources

Related Forrester Research:

The State Of Application Security, 2024, Forrester Research, Inc., June 7, 2024.

Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2023, Forrester Research, Inc., February 28, 2024.

Budget Planning Guide 2025: Security And Risk, Forrester Research, Inc., August 1, 2024.

Related Blogs And Podcasts

Sandy Carielli, Heidi Shey, What To Know: A Retrospective Of 2023's Top Breaches And Fines, Forrester Blogs.

Brian Wrozek (Principal Analyst) and Janet Worthington (Senior Analyst), Top Cybersecurity Threats In 2024, What It Means, May 2, 2024.

Project Team:

Mandy Polacek,
Senior Market Impact Consultant

Contributing Research:

Forrester's Technology & Security research group

Methodology

This Opportunity Snapshot was commissioned by Akamai. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 322 global directors and above in compliance, risk, IT and operations roles at their organization. All respondents work for financial services and/or insurance institutions that have at least $500 million in annual revenue. The custom survey began and was completed in September 2024. This study was conducted in a double-blind fashion.

Demographics

REGION	
Asia Pacific	**33%**
Europe	**33%**
North America	**34%**

DEPARTMENT	
IT	**31%**
Operations	**26%**
Compliance	**24%**
Risk	**19%**

COMPANY SIZE (ANNUAL REVENUE)	
More than $5 billion	**7%**
$1 billion to $5 billion	**33%**
$500 million to $999 million	**x%**

TITLE	
C-level executive	**16%**
Vice president	**20%**
Director	**64%**

Note: Percentages may not total 100 due to rounding.


FORRESTER®