BITSIGHT

Bitsight brochures

- Bitsight Corporate Overview
- Bitsight for Security Performance Management
- External Attack Surface Management Enhanced
- Bitsight for Third-Party Risk Management
- Bitsight Continuous Monitoring
- Bitsight Vendor Risk Management
- Bitsight Professional Services
- Financial Quantification for Enterprise Cyber Risk
- Cyber Risk Regulations & Compliance - DORA, NIS2...

BITSIGHT

DATA SHEET

A Global Leader in Cyber Risk Management

Bitsight is a global cyber risk management company, transforming how risk leaders navigate growing cyber risk uncertainty. Companies around the world trust our integrated solutions to drive critical workflows across exposure, performance, and risk. We're stabilizing cyber risk uncertainty and enabling control, ownership, and confidence for business leaders, risk leaders, and boards.

Unparalleled Industry Leadership

The world's largest community of cyber risk leaders turn to our heritage of innovation and category leadership in cybersecurity.

3000+
customers

38%
of Fortune 500 companies

30+
countries

55,000+
users from every industry

4 of the Big **4** accounting firms

4 of the top **5** investment banks

180 government agencies and quasi-governmental authorities

50%+
of cyber insurance premiums are underwritten by Bitsight customers

It's time to be the growth enabler and bold strategist your company needs. The world's leading risk leaders rely on Bitsight to reduce the likelihood of financial loss, prioritize security investments, and build trust across the ecosystem.

Partnerships that Perform

Our long-time partnerships have bolstered our cybersecurity risk management solution for evaluating investment risk and improving investors' visibility into cyber risk.

- **Moody's Corporation:** Bitsight is the cyber risk input across Moody's solutions
- **Glass Lewis:** Bitsight ratings incorporated in 14,000 proxy reports
- **Marsh McLennan:** Independent study finding Bitsight to have the strongest correlation in the industry to the likelihood of a cyber incident

A Market-leading Cyber Risk Management Solution

With Bitsight's robust offering, CISOs can grow their ecosystems without worrying about expanded risk. Accelerate transformation without risking financial turbulence. Add vendors without their vulnerabilities. And get everyone talking a universal language across the board.

Powering our solution is the Bitsight Cyber Risk Analytics Engine that delivers market-leading data, insights, and workflows for enterprise security, digital supply chain and cyber insurance.

Market-Leading Cyber Risk Data

Get a complete picture of potential risk and vulnerabilities with the most extensive cyber risk data in the market.

Objective Universal Standard

Measure and communicate cyber risk with the world's most widely trusted and adopted universal standard.

Actionable Risk Insights

Confidently build your cyber risk program with our unique and actionable insights powered by extensive data and metrics.

40M+
actively monitored organizations worldwide

400B
security events processed daily

46
granted patents

1M+
entities mapped

Security Performance Management for Enterprise Security

A cybersecurity governance and exposure management solution that provides unique analytic insights in cyber risk governance and external attack surface management. It enables CISOs to confidently communicate and prove program performance and to stakeholders.

Third-Party Risk Management for Digital Supply Chain

An end-to-end solution that continuously monitors third and fourth parties eliminating blindspots across the supply chain. Third-Party Risk Management enables CISOs to respond to major security events, efficiently onboard vendors, hone in on pressing issues, and scale programs.

Cyber Insurance

Provides transparency into the cyber risks throughout the lifecycle of an organization's cyber coverage process. Insurers harness our data because it has proven correlation to breach, which drives underwriting decisions, mitigates losses, and influences operating efficiencies.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT

BITSIGHT

DATA SHEET

STRENGTHENING ENTERPRISE SECURITY

Security Performance Management

Reduce exposure. Improve performance. Manage risk.

Overcoming New Challenges

Waves of change have disrupted cybersecurity stability and increased cyber risk uncertainty. Massive digital footprints are expanding. Cyber threats are rising. Cyber insurance premiums are up 74 percent[1], and ransomware will cost companies $265 billion by 2031[2]. Capital markets, regulators, and insurers are paying attention.

CISOs and risk leaders have an opportunity to create meaningful change. To see what an attacker sees and prioritize remediation where they're vulnerable. To harness objective metrics to drive their strategy and improve performance. To efficiently understand financial exposure and take action. And to confidently report results with context. Bitsight Security Performance Management (SPM) empowers security leaders to get there.

Manage Risk and Empower the Business

Bitsight SPM is a cybersecurity governance and exposure management solution that gives CISOs unique analytics insights. Prioritize the right activities to reduce exposure, while also setting the right targets and improvement plans to manage cyber risks. Risk leaders use SPM to confidently tackle cyber risk governance and external attack surface management, then confidently communicate and prove program performance.

Benefits

1

Protect the business from external threats

2

Achieve consistent performance across the organization

3

Make informed cyber risk decisions

4

Assure stakeholders that cyber risk is under control

1 https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/insurers-revisit-cyber-coverage-as-demand-premiums-spike-70880071

2 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

> “You can’t manage what you can’t measure. Bitsight uses externally observable data and converts this insight into measurable values that can be transparently shared to get everyone on the same page."

Yuriy Goliyad
Head of Global Operations, EPAM

Exposure

Manage the expanding attack surface & monitor for the future

Performance

Instill strong governance with trusted metrics & insights

Risk

Make informed & prioritized risk decisions

External Attack Surface Management

Attack surfaces may be expanding, but cyber risk doesn’t have to. Bitsight’s external attack surface management (EASM) solution provides full visibility into the attack surface so risk leaders can understand where exposure exists today and monitor for the future. Prioritize and protect the most vulnerable areas. And continuously discover new assets to bring into the fold.

Governance and Analytics

Let the right metrics drive the strategy. Bitsight’s governance solution is built on objective, proven metrics correlated to outcomes. Identify areas to focus. Implement improvement plans that make sense. And track performance over time in a meaningful way and report on progress.

Cyber Risk Quantification

Get everyone talking the same language about cyber risk. Bitsight’s solution for cyber risk quantification puts cyber risk in financial terms so leaders can manage risk. Set the right priorities. Calibrate cyber insurance based on unique risk appetites. And prove ROI over time to stakeholders.

BITSIGHT

DATA SHEET

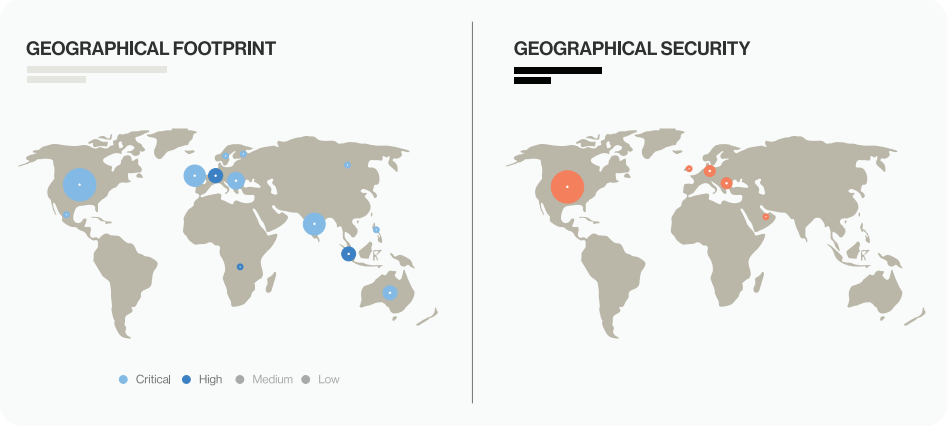
SECURITY PERFORMANCE MANAGEMENT

External Attack Surface Management Enhanced

Uplevel Your EASM Program

Reduce Exposure Across the Organization

Securing a business in today's complex digital landscape is challenging. The first crucial step is understanding your external digital footprint—because you can't protect what you can't see. With ransomware attacks on the rise and digital infrastructure expanding rapidly, External Attack Surface Management (EASM) is essential to identify your business's risk areas.



Highlights

1

Clearer visibility to your external digital footprint

2

Detailed asset insights & analysis

3

Faster vulnerability responses with robust information

Gain Deeper Asset Analysis

Bitsight's EASM Enhanced module provides powerful capabilities for securing digital assets, offering detailed insights into products, services, hosting providers, OT / ICS protocols and vulnerabilities with Attack Surface Analytics. Users can easily identify and address unsupported product versions, uncover shadow IT, and track changes in the attack surface for enhanced visibility and control.

Prioritize & Respond More Quickly to Vulnerabilities

Focus fixes on all affected assets with Vulnerability Detection. Bitsight's EASM Enhanced dataset includes robust vulnerability information, fed by Bitsight vulnerability researchers and by product fingerprinting at internet scale. This allows you to rapidly understand and remediate exposure to the latest high profile vulnerabilities in your external footprint, the place an attacker is most likely to find them.

Capabilities	EASM FOUNDATIONS *Included in Base module of all SPM packages	EASM ENHANCED + EASM FOUNDATIONS
Your assets, attributions data and change log (Infrastructure)	✓	✓
Entity Mapping (Ratings tree)	✓	✓
Bitsight findings, forensics and remediation tips	✓	✓
Risk Vectors classification	✓	✓
Issue tracking	✓	✓
Attack Surface Analytics, which includes:		✓
Attack Surface Analytics Dashboard		✓
Enhanced asset details data (Products, Services, Hosting Provider, Vulnerabilities)		✓
Vulnerability Detection, which includes:		✓
Vulnerabilities compiled in a chart view		✓
Able to filter by severity, and confidence		✓
Enhanced vulnerability coverage beyond what is in Patching Cadence (included in Foundation)		✓
Work From Home (WFH)		✓
EASM reports:		✓
Infrastructure Change		✓
Attack Surface Exposure		✓
Vulnerability Detection		✓
Vulnerability Detection Evidence		✓
Detailed Vulnerabilities tab on the Assets table drill-in		✓

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT

BITSIGHT

DATA SHEET

SECURING THE DIGITAL SUPPLY CHAIN

Third-Party Risk Management

Mitigate risk. Enable the business. Reduce exposure.

Overcoming New Challenges

Waves of change are disrupting cybersecurity stability and increasing cyber risk uncertainty. But CISOs and risk leaders have an opportunity to navigate that uncertainty with confidence. To manage and mitigate cyber risk from third parties effectively and efficiently. To assess and onboard new vendors while managing changing risk throughout the entirety of the relationship. And to identify and respond to critical exposure and major security events in the ecosystem.

Manage Third-Party Risk End-to-End

Bitsight TPRM is an end-to-end solution that allows CISOs and risk leaders to excel in their third-party risk programs. Risk leaders turn to Bitsight to efficiently assess and onboard vendors who match their risk tolerance, mitigate risk throughout the vendor lifecycle, accelerate outreach to third parties during majority security events, and scale the team's capacity with managed services. Bitsight TPRM serves the entire vendor relationship.

> "Bitsight opens conversations with our vendors' security teams. By informing them about risks they may not know about, we set ourselves up for successful business relationships from the get-go."

Ambrose Neville,
Head of Information Security at the University of Surrey

Benefits

1. Assess new and existing vendor risk
2. Continuously monitor third and fourth parties
3. Effectively respond to major security events
4. Scale team capacity to match business needs

Risk

Onboard & assess third-party vendors to empower business growth

Performance

Gain visibility into your vendor network to improve ecosystem security posture

Exposure

Prioritize, initiate, and track vendor outreach during major security events

Vendor Risk Management

Accelerate onboarding and assessment processes to enable company growth. With Bitsight Vendor Risk Management (VRM), cyber risk leaders expedite assessments more efficiently with automated workflows, verifiable data, and a growing vendor network. Reduce vendor risk with more confidence.

Continuous Monitoring

Address ongoing risk in the digital ecosystem through the life of third-party relationships. Bitsight Continuous Monitoring empowers organizations to manage and surface ongoing risk through continuous visibility into vendor security controls, comprehensive alerting for quicker mitigation efforts, and automatic discovery of fourth-party concentrated risk. Take action as risk arises.

Exposure Management

Respond to zero-day events with speed and precision. Bitsight Vulnerability Detection & Response enables risk leaders to prioritize, initiate, and track vendor exposure. Leverage scalable templated questionnaires, tailored exposure evidence, and traceable reporting to reduce risk during critical moments.

Managed Services

Resource-constrained? Need help getting a TPRM program up and running, or improving it? Bitsight Advisory Services provides a managed service across third-party programs to manage assessments, conduct vendor outreach, support remediation plans, and improve cyber risk operations without disrupting the business.

BITSIGHT

DATA SHEET

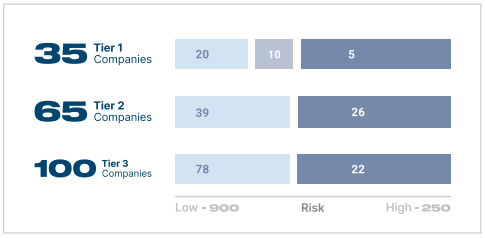
DRIVING EFFECTIVE THIRD-PARTY RISK MANAGEMENT

Bitsight Continuous Monitoring

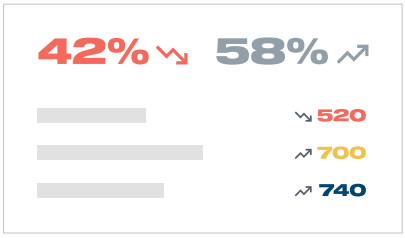
Detect emerging threats. Manage changing risk.

As your digital supply chain grows, managing third-party risk becomes increasingly difficult. **Bitsight Continuous Monitoring** empowers you to manage and address vendor risk over time with objective, market leading data—that has proven correlation to security incidents.

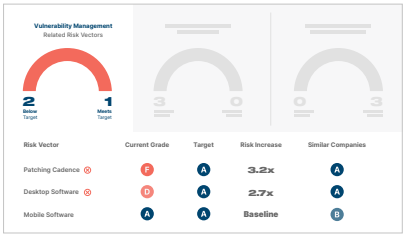
Mitigate vendor risk with precision



Quickly tier vendors for better visibility into critical risk.



Take action when vendor risk is surfaced.



Strengthen mitigation efforts with actionable data.

“Bitsight has allowed us to automate our security monitoring process, resulting in about 50% time and efficiency savings. We can get real-time information right from the easy-to-use dashboard.”

Kanitra Tyler,
ICT Supply Chain Risk Management Service Element Lead, NASA

Read Case Study →

Understand third-party cyber risk. Accelerate mitigation efforts.

Correlated risk vectors	• Bitsight risk vectors correlate to vendor likelihood of suffering from ransomware or data breach, so you can focus your mitigation efforts.
Vulnerability detection & response	• Surfaced evidence and scalable questionnaire outreach enable you to prioritize and respond to major security events and zero day vulnerabilities.
Effective vendor collaboration	• Evidence-based collaboration empowers you to reduce risk more efficiently, with quicker and more effective remediation.
Extended ecosystem visibility	• Automatic product discovery shows areas of concentrated risk and facilitates fourth-party risk management.
Integrated third-party risk management	• Native integration with Bitsight VRM assessment tool, data feeds, and business tools such as GRC or BI, streamline a flexible TPRM program and increase overall efficiency.
Managed services	• Expert professional support allows you to continuously assess third-party risk, actively identify vulnerabilities, and collaborate with vendors to remediate threats.

Do more with less.

Accelerate third-party risk mitigation and remediation.

Respond to changing third-party risk over time.

Manage an expanding supply chain with limited resources.

Gain visibility into extended vendor ecosystem concentrated risk.

Report critical risk insights and results to stakeholders.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT

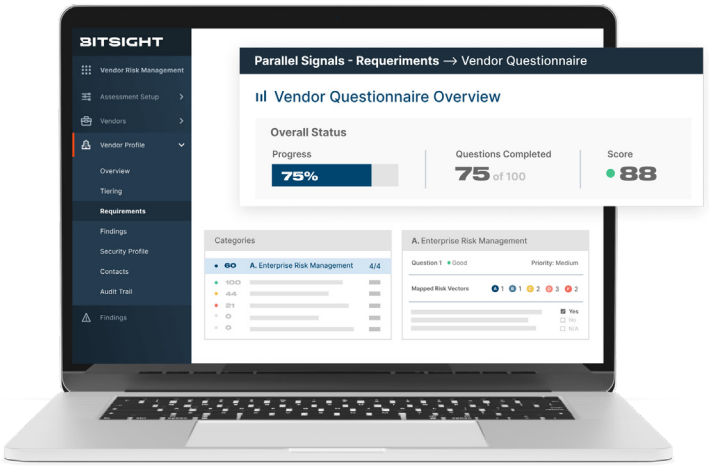
BITSIGHT

DATA SHEET

SCALING YOUR VRM PROGRAM

Vendor Risk Management

Accelerate assessments. Enable business growth.



- On-board vendors in hours, not weeks.
- Validate vendor responses with verified data and external evidence.
- Consolidate your third-party risk management program in one platform.

Manage the entire vendor lifecycle in one place

Step 1. **Build**

Build your third-party inventory by inviting your vendors to connect in the Bitsight VRM platform.

Step 2. **Review**

Review their uploaded documents, such as insurances, external audits or assessments, certifications, and questionnaires.

Step 3. **Analyze**

Analyze your evidence and leverage Bitsight analytics to make informed decisions to improve the health of your portfolio.

Step 4.**Monitor**

Continuously monitor changes across your portfolio that impact your risk tolerance.

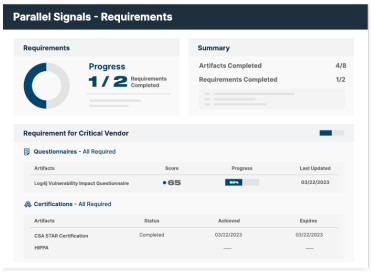
Elizabeth Olson Lennon

DIRECTOR OF VENDOR MANAGEMENT, ALAMEDA ALLIANCE FOR HEALTH

ALAMEDA Alliance FOR HEALTH

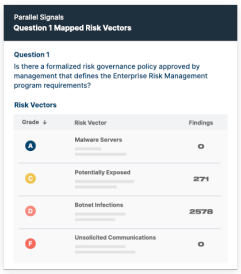
“**We save hundreds of hours** annually by using Bitsight. We’ve integrated Bitsight Vendor Risk Management into our onboarding and evaluation process, and it’s helped us identify the actual risk level associated with vendors.”

Simplified vendor risk management—at scale.



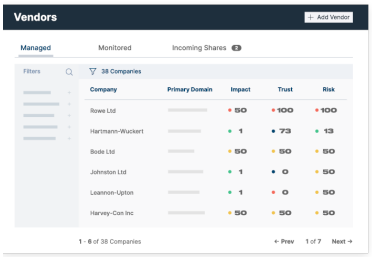
Customizable Assessments

Per criticality, per regulation, tailored to your need.



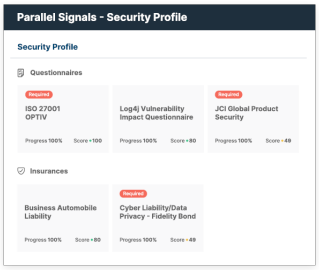
Evidence Mapped into Questionnaires

Validate with Bitsight data and analytics proven to be correlated to risk.



Simplified Vendor Scoring

Impact, Trust, and Risk Score as a simple formula to measure risks.



Centralized Repository

Manage hundreds of third-party vendors—all in one place.

The Power of the Network

Bitsight Vendor Risk Management enables you to instantly tap into a rapidly expanding network of over 40,000 vendor profiles — continuously updated — all in real time. The efficiency gains are extraordinary. The experience is even better.

40K+
Vendor profiles

3X ROI
Within first six months*

90%
Vendor acceptance rate*

75+%
Time reduction assessing vendors*

*As reported by existing Bitsight customers. Actual outcomes will depend upon a variety of factors unique to each customer and are not guaranteed.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT

BITSIGHT

DATA SHEET

Security Performance Management Advisor Services

Bitsight Advisors operate as a dedicated resource responsible for working with your team to execute and operationalize Bitsight within your Security program. Areas of service include assistance in developing a Bitsight-specific risk program, ongoing asset management, alert monitoring and prioritizing areas of work with a focus on reputation management.

How can we help?

Security Ratings Oversight

- Asset Management
- Remediation Plans
- Ongoing Monitoring

Executive Strategy

- Goal Setting
- Benchmarking
- Framework Alignment

Interpretation

- Trend Analysis
- Potential Impact
- Relevancy

Alignment to program objectives

- Prioritize and focus remediation for highest impact to Security Ratings
- Provide in depth options, proposed resolutions and timelines based on rating impact
- Define ideal ratings tree strategy and develop execution framework
- Develop asset management program for ongoing changes to infrastructure
- Monitor daily alerts for changes in posture across company, including subsidiaries
- Identify Bitsight integration points with existing systems, develop project plan
- Executive / Board Level Benchmarking / Peer Comparison Reporting
- Custom Trend Analysis/ Impact reports provided at regular cadence
- Dedicated support for on-demand, bespoke training
- Designated collaboration contact for incoming Security Ratings inquiries

Learn more

Bitsight Advisor Services are available based on the number of hours per week dedicated to program management, which can be determined by working with your Bitsight contact and based on your needs.

For more details on Bitsight Advisor Services and to add an expert resource to your team today, please contact Bitsight at **profservices@bitsight.com**

BITSIGHT

BITSIGHT

DATA SHEET

Managed Services for Third-Party Risk Management

Seasoned Experts to Enhance Your Practice

Managing third-party cyber risk has never been more important – or more difficult. Between the dynamic, expanding cyber risk landscape and the increasing rate of change in your own vendor ecosystem, it can be a challenge to keep pace with portfolio risk throughout the vendor lifecycle. Our team of **Bitsight Advisors** is here to help, providing managed services to deliver:

Managed Vendor Assessments

Vendor assessment management, including issue identification and remediation.

Continuous Monitoring & Risk Hunting

Ongoing mitigation of cyber risk through collaborative remediation with third-parties.

Effective Reporting & Assurance

Meaningful program, event,and vendor-specific reports with insights to drive organizational decision making.

Bitsight Managed Services for TPRM

Bitsight managed services provide resources and expertise to navigate the complexities, changes, and challenges of managing third-party risk.

Get the support you need to help scale and manage your growing third-party ecosystem while meeting regulatory requirements, with a best-in-class TPRM program that delivers real business value.

Services That Meet Your Requirements

Bitsight managed services are designed for our customers' needs. Whether you are building a program from the ground up, or looking to drive efficiencies and scale a particular part of your program, Bitsight Advisors are here to help.

of organizations express they do not have sufficient capabilities in-house to manage all the third-party risks they face

-KPMG TPRM OUTLOOK 2022

Delivering an end to end program that spans from onboarding to offboarding, with best in class technology and proven TPRM expertise.

Managed Services Supported by Bitsight Data

Bitsight Managed Services are powered by Bitsight Security Ratings. These analytics are trusted by over 180 government institutions across 30 countries, 38% of the Fortune 500 companies, and 4 of the top 5 investment banks.

BITSIGHT

DATA SHEET

Managed Services for Continuous Monitoring

Seasoned Experts to Enhance Your Practice

As organizations look to navigate an ever-increasing digital world, third-party cyber risk has become more prevalent than ever. Without the proper tools and people to manage and mitigate these threats, businesses often become reactionary with how they address issues that arise.

To better position your organization to address and remediate risk on an ongoing basis, our team of **Bitsight Advisors** offers expert managed services to:

Continuously monitor and assess third-party risk

Address third-party performance throughout the vendor lifecycle.

Identify vulnerabilities and actively hunt for risk

Quickly find hidden exposures and critical vulnerabilities across your vendor supply chain.

Collaborate with vendors to remediate and resolve threats

Work with your third parties to proactively improve their security posture and attend to critical issues.

Bitsight Managed Services for TPRM

Bitsight managed services provide resources and expertise to navigate the complexities, changes, and challenges of managing third-party risk.

Get the support you need to help scale and manage your growing third-party ecosystem while meeting regulatory requirements, with a best-in-class TPRM program that delivers real business value.

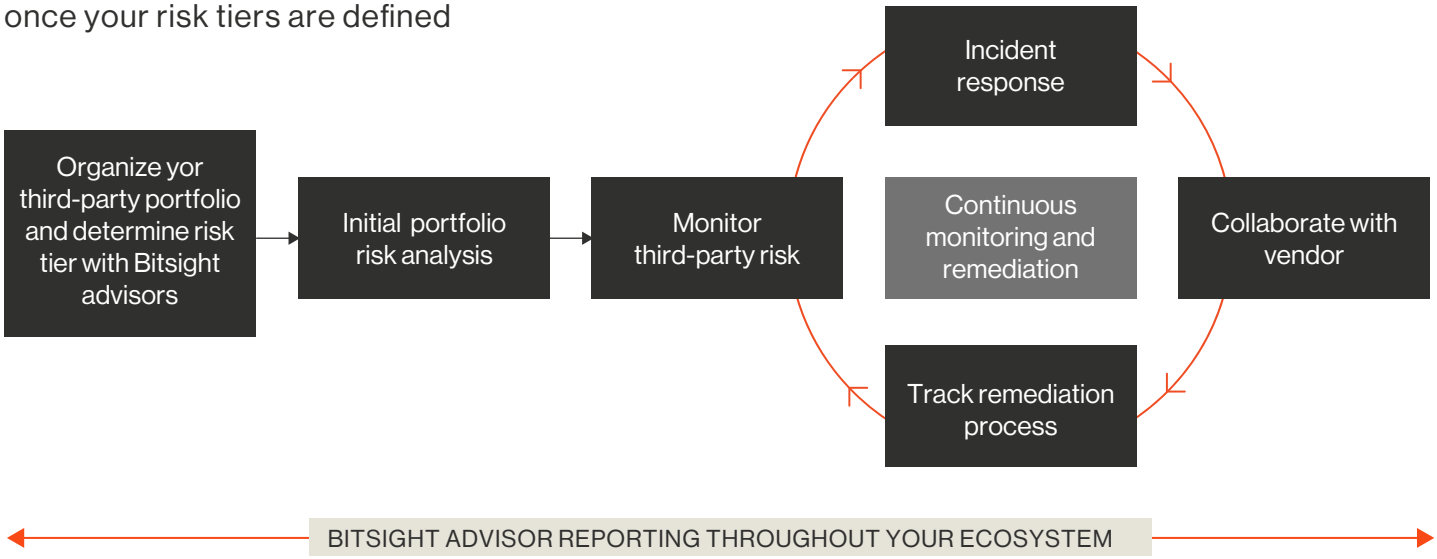
of legal and compliance leaders tell us that third-party risks were identified after initial onboarding and due diligence.

- GARTNER®

How Managed Services for Continuous Monitoring Works

Bitsight managed services help you continuously monitor cyber risk across your third-party portfolio to protect your business. In partnership with your team, we're able to organize and determine the risk appetite across your ecosystem so we can better monitor, respond to, and remediate risk with your vendors as efficiently as possible. See below for a quick snapshot on how it's done:

Bitsight Advisors drive performance once your risk tiers are defined



Managed Services Supported by Bitsight Data

Bitsight Managed Services are powered by Bitsight Security Ratings. These analytics are trusted by over 180 government institutions across 30 countries, 38% of the Fortune 500 companies, and 4 of the top 5 investment banks.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT

BITSIGHT

DATA SHEET

CYBER RISK QUANTIFICATION

Financial Quantification for Enterprise Cyber Risk

Demystify cyber risk for clearer cybersecurity insights

Empowering Cyber Risk Management

The ever-increasing sophistication of cyber threats has made it clear that understanding and managing cyber risk is more crucial than ever before. It's not just about protecting data; it's about comprehending the financial fallout of a breach and making informed decisions to become more proactive when it comes to managing risk. However, many cyber risk quantification (CRQ) offerings today are inefficient, subjective, and expensive.

Bitsight Financial Quantification is a modern CRQ solution for security and risk leaders, simplifying the evaluation of financial exposure to cyber risks. This data-driven approach eliminates the need for extensive, time-consuming data collection and facilitates quick, cost-effective deployment. It enables confident and informed decisions in the ever-evolving cybersecurity landscape.

Benefits

1

Communicate easily & instill confidence

2

Make informed decisions with results

3

Simplify deployment for greater efficiency

Key Use Cases

Board Reporting:

Communicate with a universal language to drive confidence with the board.

Cyber Insurance:

Calibrate cyber insurance coverage based on risk appetite.

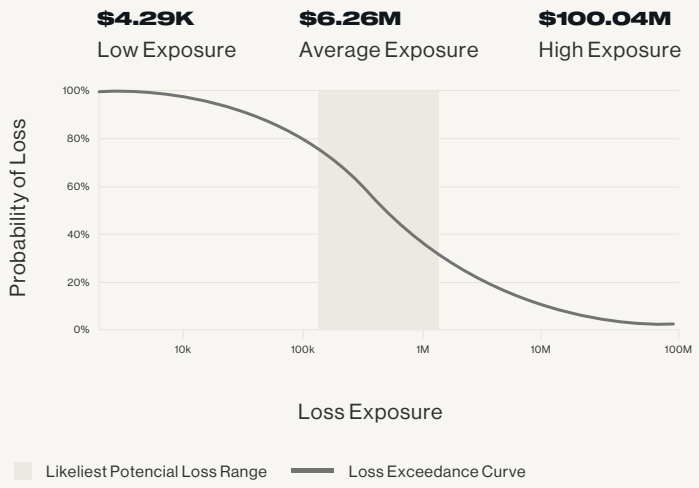
Resourcing:

Prioritize time, resources, and budget to what matters most.

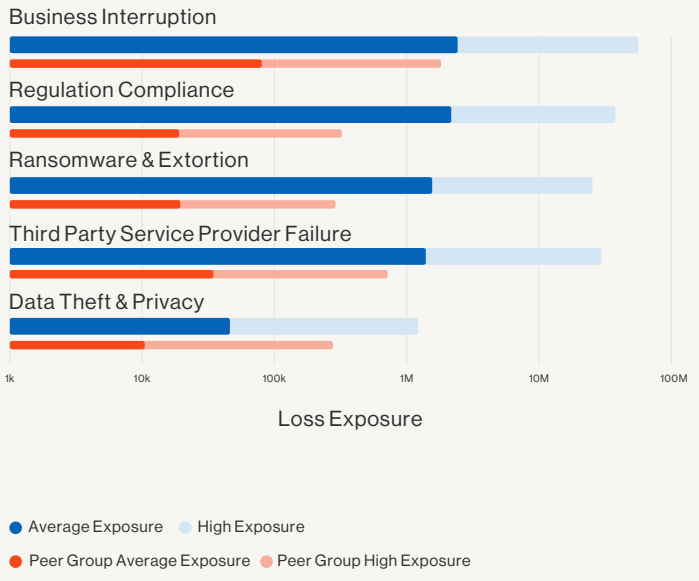
ROI:

Report progress and prove ROI by tracking risk over time.

Cyber Loss Exposure



Cyber Risk By Impact Scenario Annualized Loss Exposure



Drive confidence with the board:

- Equip your security team with context and insights to elevate board and executive discussions on risk.
- Share insightful reports, allowing you to visualize overall risk levels and drill into specific scenarios.

Cyber insurance & your risk appetite:

- Tailor cyber insurance coverage based on your risk appetite by evaluating probable loss scenarios aligned with common insurance categories.
- Distribute cyber insurance across business units and subsidiaries using quantified risk assessments.

Prioritize your resources:

- Focus resources on scenarios with the highest risk, enhancing return on investment.
- Assess the unique likelihood of damage across various cybersecurity scenarios to inform security investment decisions.

Report progress and prove ROI:

- Generate quantifications as needed and share results with stakeholders.
- Track and analyze how your organization's risk profile changes over time.

Bitsight Financial Quantification is a turnkey CRQ offering that provides a quick, efficient, and repeatable assessment of your financial exposure to cyber risk.

Our modern approach extends beyond turnkey software. Bitsight CRQ Enablement Services ensures your CRQ program is not only successful from the start, but scales over time to continuously improve.

Work directly with our CRQ experts to define your use cases and set up your CRQ program. Together, you will understand your Financial Quantification outputs, put an action plan in place, and scale your program over time.

“With Financial Quantification, I could quicky visualize the risk burndown of proposed security investments and the financial risk of not allocating funds to certain areas of our security program.”

Tim Grieveson
SVP, Global Cyber Risk Advisor, Bitsight
Former Chief Security Officer and SVP of Information Security, AVEVA

CRQ Enablement Services

1

Within 30 days

Actionable results within 48 hours

2

Within 60 days

Apply results to real business problems

3

Within 90 days

Sustainability and continuous monitoring

4

Beyond 90 days

Ongoing engagements to enhance insights

BITSIGHT

SOLUTION BRIEF

Enabling NIS 2 Compliance with Bitsight

NIS 2 - or Directive (UE) 2022/2555 - has replaced the original Directive 2016/1148/EC to strengthen security across critical sectors in the EU government and companies that operate in or within the European Union. The new version of NIS enhances cybersecurity capabilities and promotes resilience in critical infrastructure and digital services —and applies to all companies, suppliers, and organisations ("entities") that deliver essential or important services for the European economy and society.

The NIS 2 Directive will enter into force within EU Member States before the end of 2024. Failure to comply with NIS 2 can result in reputational damage and sanctions imposed by national authorities, including financial penalties and operational limitations. Organisations must prioritise NIS 2 compliance to avoid such consequences.

What changes in NIS 2 over the original version?

EXPANDED SCOPE

NIS 2 broadens its applicability to include a more extensive range of companies and sectors, recognising the diverse nature of cyber threats across industries—including transport, energy, banking and financial market infrastructure, digital infrastructure, ICT service management, healthcare, water supply, waste management public administration (central and regional levels), postal and courier services.

ENHANCED COOPERATION

NIS 2 emphasises cross-border cooperation and collaboration between Member States, enabling more effective incident response and threat mitigation.

UPDATED INCIDENT REPORTING

NIS 2 imposes stricter incident reporting obligations on organisations, ensuring prompt response and mitigation of cyber incidents.

How Bitsight supports NIS 2 main pillars

Bitsight empowers organisations to achieve compliance with NIS 2, as part of their overall compliance programme, while enhancing operational resilience. Through its comprehensive cybersecurity ratings, continuous monitoring capabilities, third-party risk management solutions, and incident response planning features, Bitsight assists organisations in meeting the main pillars of NIS 2.

Security Program

Continuous Monitoring	• Bitsight provides real-time insights into an organisation's cybersecurity posture, enabling continuous monitoring and proactive risk management.
Cybersecurity Ratings	• Bitsight's comprehensive cybersecurity ratings evaluate an organisation's security controls and help measure compliance with NIS 2 requirements.

Risk Assessment

External Threat Intelligence	• Bitsight leverages external threat intelligence to identify emerging risks and vulnerabilities, enabling organisations to prioritise risk mitigation efforts effectively.
Third-Party Risk Management	• Bitsight assesses the cybersecurity posture of vendors and business partners, ensuring supply chain security and compliance with NIS 2 standards.

Security Safeguards

Identifying System Vulnerabilities	• Bitsight enables comprehensive cyber security vulnerability assessments by providing external verification and continuous insight into risk, helping organisations identify and address system vulnerabilities in line with NIS 2 requirements.
Incident Detection and Response	• Bitsight offers incident response planning capabilities, assisting organisations in promptly detecting and mitigating cyber incidents to minimise their impact.

Supply Chain

Vendor Risk Assessment	• Bitsight enables organisations to assess the cybersecurity posture of third-party vendors, ensuring compliance across the entire supply chain and mitigating potential vulnerabilities.

Incident Reporting

Actionable Insights	• Bitsight provides actionable insights and recommendations for incident response planning, helping organisations effectively meet NIS 2 incident reporting obligations.

Recommendations for NIS 2 compliance

The next steps and actions organisations need to consider include:

- Assess the current cybersecurity posture and identify gaps.
- Conduct comprehensive risk assessments and prioritise remediation efforts.
- Evaluate the cybersecurity posture of third-party vendors and business partners.
- Establish incident response plans and reporting processes.
- Implement robust security programs aligned with NIS 2 requirements.
- Continuously monitor and evaluate security controls to maintain compliance.

NIS 2 compliance with Bitsight

Bitsight enables organisations to systematically lower cyber risk by supporting critical workflows across risk, performance, and exposure. Security leaders can continuously measure the effectiveness of controls recommended by best practice frameworks and map risk vector data to control frameworks and questionnaire-based assessments—allowing them to trust but verify vendor responses and improve visibility over risk.

With increased reliance on the cloud and service providers, managing third-party risk has become increasingly challenging. But based on history in an industry we created in 2011, Bitsight gives leaders the confidence to make faster, more strategic cyber risk management decisions. To assess performance, qualify vendors, prioritise investments, and minimise financial loss. At scale.

By actively monitoring over 40 million organisations worldwide, Bitsight empowers security teams to establish a universal understanding of cyber risk, going beyond ratings to provide financial and business context. And we ensure organisations collectively reduce risk to foster digital operational resilience.

Partner with Bitsight in your journey to compliance →

BITSIGHT

SOLUTION BRIEF

Enabling DORA Compliance with Bitsight

The Digital Operational Resilience Act (DORA) is a regulation that proposes a comprehensive information and communication technology (ICT) risk management framework for the financial sector across the European Union (EU). DORA encompasses a set of technical standards that financial entities and their critical third-party service providers are required to adopt in their ICT systems by January 17, 2025. Here's what you need to know to meet the deadline.

After years of inconsistent, individual regulations pushed by EU member states, DORA is harmonizing efforts to establish a universal framework for managing and mitigating ICT risk in the financial sector. With a shared set of rules across the EU, DORA creates a comprehensive approach to ensuring organisations can withstand, respond, and recover from the impacts of ICT incidents, thereby continuing to deliver critical and important functions and minimizing disruption for customers and the financial system.

DORA promotes the need to establish robust measures and controls on systems, tools, and third parties—as well as the need to have the right continuity plans in place and test their effectiveness.

The five pillars of DORA

01 ICT Risk Management

02 ICT Incident reporting

03 Digital operational resilience testing

04 Information and intelligence sharing

05 ICT Third-Party Risk Management

The five pillars of DORA

1. ICT Risk Management

Scope of application	• Governance (accountable management body) • Risk management framework and associated activities (identification, protection and prevention, detection, response and recovery, learning and evolving, crisis communication)
How we can help	Bitsight helps organisations to comply with the governance principles around ICT risk. This includes identifying risk tolerance for ICT risk, based on the risk appetite of the organisation and the impact tolerance of ICT disruptions.
Bitsight features	• Security Rating measures the organisation and its third-party risk for financial service providers and their ICT vendor ecosystem • Mapping Risk Vectors to frameworks

2. ICT Incident reporting

Scope of application	• Standardized incident classification • Compulsory and standardized reporting of major incidents • Anonymized EU-wide reports
How we can help	Bitsight helps to assess incident classification based on a set of specific criteria such as number of users affected, duration, geographical spread, data loss, severity of impact on ICT systems, and criticality of services affected and economic impact.
Bitsight features	• Risk Vector Alerts based on business context and/or services • Data breach reporting and classification • Risk hunting through filters

3. Digital operational resilience testing

Scope of application	• Comprehensive testing program, with a focus on technical testing • Large-scale, threat-led live tests performed by independent testers every three years
How we can help	Bitsight partners with security and risk leaders focused on managing cybersecurity performance to systematically lower breach risk across the full ecosystem. Our cyber risk management capabilities span across organisations, its third- and fourth-parties —and empower teams to test and measure the effectiveness of the risk management framework.
Bitsight features	• Bitsight detects malware, botnets, and compromised systems data (at the event level) from the outside • Continuous monitoring of internet-facing resources based on potential breach risk drivers and risk-based analysis • Rating correlates to the likelihood of a data breach, providing risk quantification at scale • Fourth-party data allows for identification of risk concentration (such as which cloud providers are more prevalent) • Intel at scale for ICT/vendor ecosystem in an automated way (including alerts and risk tiering)

4. Information and intelligence sharing

Scope of application	• Guidelines on information sharing arrangements for cyber threats and vulnerabilities
How we can help	Bitsight facilitates sharing of information and intelligence on cyber threats between financial organisations —enabling them to be better prepared to address digital vulnerabilities.
Bitsight features	• EVAs allow for information sharing between stakeholders

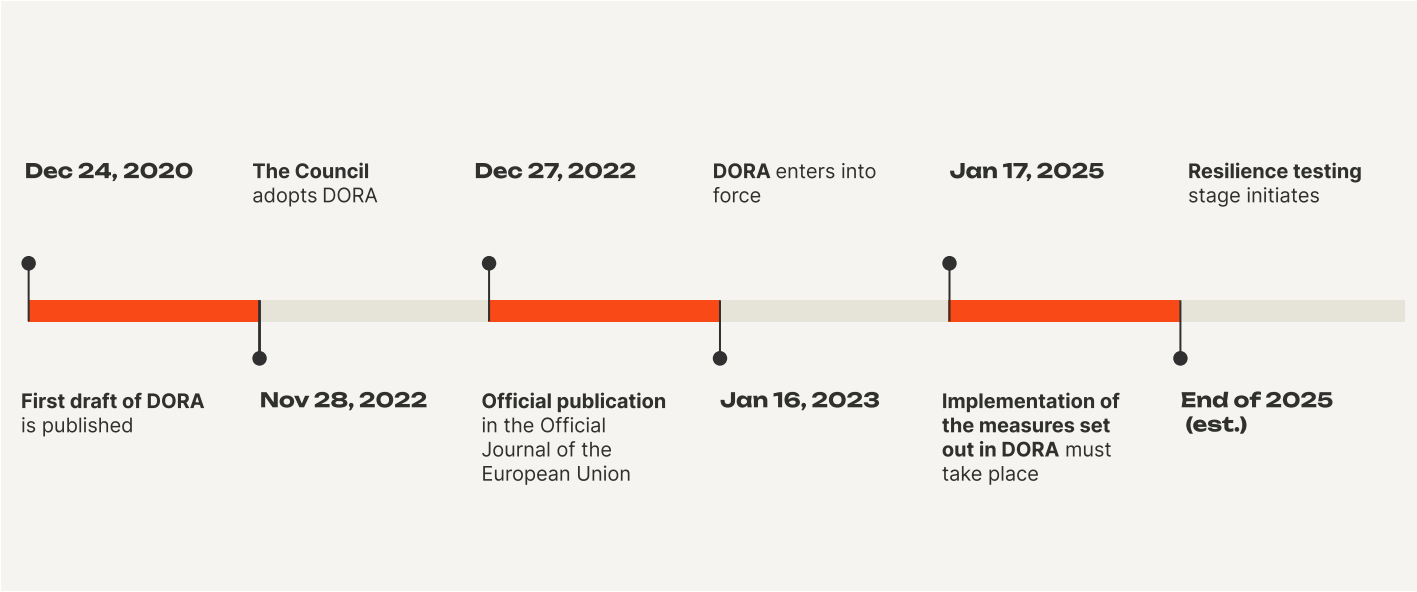
5. ICT Third-Party Risk Management

Scope of application	• Strategy, policy, and standardized register of information • Guidelines for pre-contract assessment, contract contents, termination, and stressed exit • Create oversight framework for critical providers across the EU with clear requirements and penalties
How we can help	Bitsight helps firms ensure they have an appropriate level of effective security controls and monitoring of their ICT third parties in place —specifically targeting those that can be deemed critical to their supply chain, as well as setting up oversight on specific providers that can be considered critical to the global market.
Bitsight features	• Continuous Monitoring provides immediate warnings of changes in vendors' security status, rather than point-in-time annual assessments of vendor risk • Tiering and segmenting vendors by business context aligned with third-party inventory • Bitsight VRM automates and scales vendor onboarding and risk assessments with custom requirements • Improved collaboration through EVAs to create an onboarding baseline • Customers can dictate to vendors how the rating or event / risk level KPIs need to be managed (or additional measures allowed) • Third-party vulnerability detection and response shows vendor exposure to known vulnerabilities and enables collaborative, evidence-based remediation • Bitsight currently has NIST based alerts, and is able to map risk vectors to specific frameworks such as ISO 27001 or common vendor questionnaires

The road to DORA

The European Commission proposed DORA in September 2020 as part of a larger package that also includes a Digital Finance Strategy with legislative proposals on crypto-assets and digital resilience. The Council of the European Union and the European Parliament formally adopted DORA in November 2022, and the European Supervisory Authorities (ESAs) are drafting the regulatory technical standards (RTS) and implementing technical standards (ITS) that will pave the way for compliance. These standards, as well as an oversight framework for critical ICT providers, are anticipated to reach their definitive form in 2024.

With the clock ticking, financial entities and third-party ICT service providers are working towards the imminent deadline of January 17, 2025.



DORA compliance with Bitsight

Bitsight enables organisations to systematically lower cyber risk by supporting critical workflows across risk, performance, and exposure. Security leaders can continuously measure the effectiveness of controls recommended by best practice frameworks, and map risk vector data to controls frameworks and questionnaire-based assessments—allowing them to trust but verify vendor responses and improve visibility over risk.

With increased reliance on the cloud and service providers, managing third-party risk has become increasingly challenging. But based on history in an industry we created in 2011, Bitsight gives leaders the confidence to make faster, more strategic cyber risk management decisions. To assess performance, qualify vendors, prioritise investments, and minimize financial loss. At scale.

By actively monitoring over 40 million organisations worldwide, Bitsight empowers security teams to establish a universal understanding of cyber risk, going beyond ratings to provide financial and business context. And we ensure organisations collectively reduce risk to foster digital operational resilience.

Partner with Bitsight in your journey to compliance →