BITSIGHT

Accelerate your TPRM program

Professional Services

Three drivers for scaling TPRM programs

Escalating Threat Landscape

Attackers employ sophisticated tactics to target organizations through their supply chain. Zero-day vulnerabilities are increasing.

How can organizations stay ahead of the risk?

Regulatory Pressure Rising

Regulatory bodies worldwide place greater emphasis on third party risk and supply chain management.

What's coming in 2024 and beyond?

Evolution of the CISO

Today's CISOs are business enablers, tasked with juggling critical tasks around strategy, ROI demonstration & stakeholder reporting.

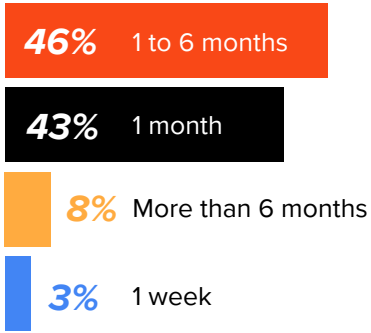
How can CISOs adapt to meet the needs?

Vulnerability remediation

Many organizations remain too slow to patch, giving threat actors time to exploit vulnerable attack surfaces

Patching duration
high-risk CVEs, all sectors

ENISA, 2023



Time to exploit
critical CVEs, all sectors

Qualys, 2023

44 days
Mean time to exploit high-risk vulnerabilities

25%
High-risk CVEs exploited on day of publication

Bitsight findings
CVE remediation, 101k enterprises

Bitsight, 2023

1.5x faster
Organizations with 700+ Bitsight rating vs 300-500 category

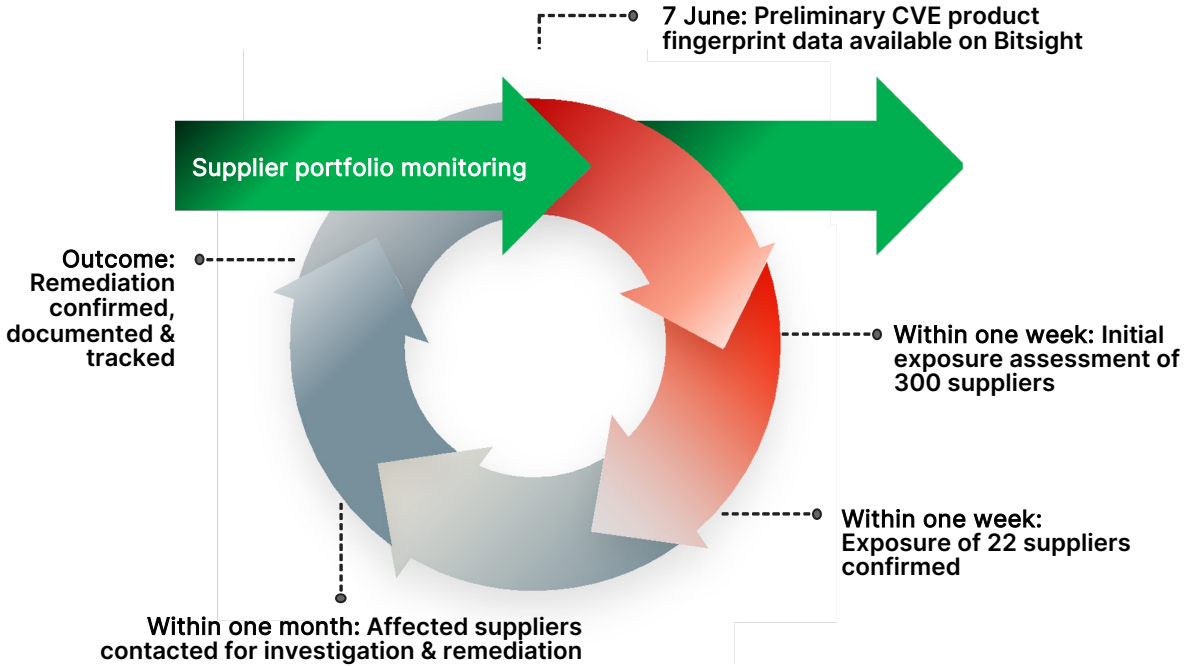
Only 5%
Instant vulnerability remediation rate

Customer story - Vulnerability remediation

Rapid MOVEit 0-day exposure identification & remediation across suppliers for Swiss financial services organization

Profile

- Switzerland
- Financial services
- Global investment and financial services firm



Progress MOVEit

CVE-2023-34362: SQL injection vulnerability in MOVEit Transfer database allowing unauthenticated attacker to gain administrative access, exfiltrate files, and gain arbitrary code execution.

Regulations emphasize third party risk

New risk regulations signal a shift toward strengthening resilience & enforcing accountability across supply chains

The regulatory horizon

Expansion of regulatory scope

Expansion of relevant audiences

Vendor due diligence & monitoring

Common thread: Independent, comparable measure of assessing and quantifying cyber risk

> *Supply Chain Diligence:*
> Continuously document your IT suppliers and IT service providers. Assess them via due diligence, security ratings services, security certifications, security audits, and other risk mitigation techniques.
>
> NIS2 Directive

Customer story – Regulatory readiness

Preparing Belgian businesses and essential service providers for upcoming regulatory compliance

Profile

Belgium

Government

National Cybersecurity Authority

BITSIGHT

CASE STUDY

Centre for Cybersecurity Belgium (CCB)

Belgium Government Partners with Bitsight to Measurably Reduce National Cyber Risk

The Centre for Cybersecurity Belgium (CCB) is the national authority for cybersecurity in Belgium. The CCB supervises, coordinates, and monitors the application of the Belgian cybersecurity strategy. The CCB's mission is to ensure coordination and information exchange so that Belgian companies, the government, providers of essential services, and the population can protect themselves appropriately.

The CCB also plays a key role in the realization of Belgium's Cybersecurity Strategy 2.0, which was approved by the country's National Security Council in 2021. It is a framework for the country's cross-cutting approach to cyber threats and opportunities. Its intention is to make Belgium one of the least vulnerable countries in Europe. The CCB plays a key role in helping Belgium achieve this objective.

Bitsight is a critical partner to helping the CCB achieve this vision.

CENTRE FOR CYBER SECURITY BELGIUM

- Government
- Belgium

Challenge:

Lacked visibility into Belgium's cybersecurity posture – both at a national level and compared with other countries in the European Union (EU).

Solution:

National Cybersecurity Application and Bitsight Advisors

"Before Bitsight, we lacked visibility into Belgium's cybersecurity posture – both at a national level and compared with other countries in the European Union (EU),"

Miguel De Bruycker
Director general at the CCB

Supporting CCB regulatory needs

Cyber Fundamentals Assessment mapped to Bitsight for NIS2 compliance

Cyber security visibility, guidelines & benchmarking

Findings & best practices via awareness campaigns with impacted organizations

Policy decisions based on data-driven measurement

Customer story – Regulatory readiness

Road to optimizing insights and compliance through enhanced VRM & Managed Assessments

Profile

- Germany
- Pharmaceutical
- Privately-owned manufacturer

- Manual third-party control reviews
- Resource limitations

BITSIGHT VRM

- Custom IRQ integrated into VRM
- Transitioned to SIG Lite questionnaire
- Aligned questions with Bitsight Risk Vectors

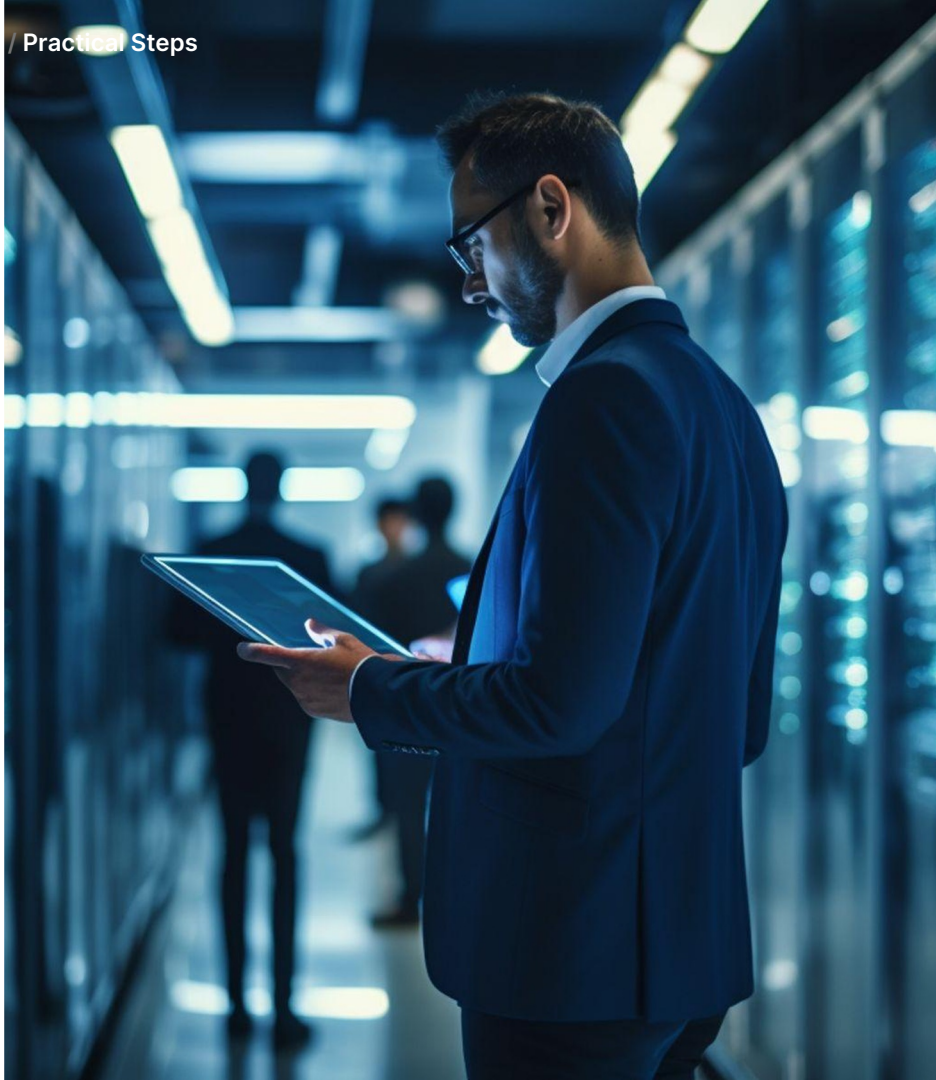
Customer success metrics

- ✓ 75% faster assessment turnaround time
- ✓ 80% vendor response rate
- ✓ 3x vendors assessed with the same resources
- ✓ Enhanced compliance with regulations

Evolution of the CISO

Today's CISOs are expected to ...

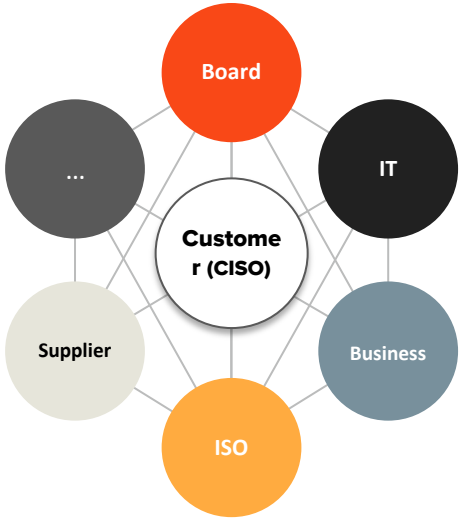
- Develop & Communicate
- Demonstrate ROI
- Adapt & Respond
- Enable Compliance
- Build a Security Culture
- Report on Security Performance



Customer story - Program development

TPRM program development strategy for European automation & energy management organization

Define key stakeholder groups



Collect feedback & demands

Objectives

- Obtain good & bad feedback from key stakeholders
- Understand target operating model for TPRM program

Guiding Questions

- What are stakeholder expectations?
- What are typical escalations – how to avoid those?
- How is the quality of the current program?
- What is the program's reputation?
- What are key improvement areas to meet demands?

Outcomes

What is good?

What must be improved?

Develop program improvements

Better reporting & more frequent stakeholder communications

Supplier communication & outreach workflows

Standardized risk articulation & documentation

Program improvement plan

Bitsight Third-Party Risk Management

Strategies for scaling your TPRM program

Powered by Managed Services

- Program development
- Managed vendor assessments
- Continuous monitoring & risk hunting
- Surfaced insights and reporting

Vendor Risk Management

- Automated assessments
- Growing vendor network
- Evidence to validate

Continuous Monitoring

- Inspect vendor controls at any moment
- In-context vendor collaboration
- Automatic discovery of concentrated 4th-Party risk

Thank you!

111 Huntington Ave
Suite 2010
Boston, MA 02199
USA

bitsight.com
sales@bitsight.com

BITSIGHT