BITSIGHT

Cyber Risk Landscape, Trends & Changing Risk

Stephen Boyer

Co-Founder & Chief Technology Officer

Cyber Risk Landscape, Trends, and Changing Risks

Bitsight Luminate Exchange DACH Region

May 2024

BITSIGHT

An error message was displayed on a kiosk at MGM's Aria Resort and Casino, Sept. 11. PHOTO: DANIEL PEARSON/LAS VEGAS REVIEW-JOURNAL/ASSOCIATED PRESS

MGM Cyber Event Triggered an Issuer Comment

MGM's cyber event deemed "credit negative"

Observed patching performance demonstrated **3.2X** higher likelihood of incident

CORPORATES

Moody's
INVESTORS SERVICE

ISSUER COMMENT
13 September 2023

Send Your Feedback

MGM Resorts International

Confirmed cybersecurity incident is credit negative

On 11 September, MGM Resorts International (B1 stable) identified a cybersecurity issue that was affecting some of the company's systems. The cybersecurity incident is credit negative for the company and highlights key risks related to business operations' heavy reliance on technology and the operational disruption caused when systems need to go offline or are inoperable.

Additional risks to MGM include potential revenue losses while systems were down, reputational risk and any direct costs related to investigation and remediation. Litigation expense or liability that the company may have because of compromised data, to the extent there is any, is also a risk. While the company's casino floors are back online and operational, its website is currently unavailable.

MGM in 2020 disclosed that it was a victim of a 2019 data breach that involved unauthorized access to a cloud server containing guest information. The incident pointed out key risks to entertainment and hospitality companies that handle large amounts of personal data on customers.

In the cyber risk heat map we published in September 2022, we identified the gaming and gambling industry as carrying moderate cybersecurity risk, mainly because of their highly digitized nature and the large amount of valuable personal data the companies maintain. Data on guests in some cases may include personal information about US executives and government officials with security clearances, which is particularly prized by nation-state hacker communities. For sectors scored moderate overall, the primary driver is their average exposure to cyber risk and average mitigation practices. A moderate cyber risk exposure reflects a sector's material reliance on digitization to operate their businesses, but whose more localized, less interconnected nature with other sectors would guard against a successful cyber attack on one not have wide-ranging knock-on effects to the rest of the economy.

Bitsight, a cybersecurity ratings and analytics company, most recently scored MGM an "F" for patching cadence, which is the speed at which an organization remediates its exposure to known vulnerabilities. In previous studies, Bitsight has shown that an organization scoring an "F" grade in patching cadence is 3.2x more likely to fall victim to a cyber incident (see exhibit) than a higher rated organization. A cyber incident is defined as a malicious attack such as ransomware, business interruption, and data breaches that has resulted in a cyber insurance notification or claim.

Contacts

Adam McLaren +1.212.553.2753
VP-Senior Analyst
adam.mclaren@moodys.com

CLIENT SERVICES

Americas 1-212-553-1653
Asia Pacific 852-3551-3077
Japan 81-3-5408-4100
EMEA 44-20-7772-5454

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigation

Cybersecurity

UnitedHealth to take up to $1.6 billion hit this year from Change hack

By **Sriparna Roy** and **Leroy Leo**

April 16, 2024 4:09 PM UTC · Updated a month ago

UnitedHealth Group's headquarters building is seen in Minnetonka, Minnesota, U.S. in this handout picture taken in 2019. UnitedHealth Group/Handout via REUTERS/File Photo *Purchase Licensing Rights*

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigat

Cybersecurity

Almost all US hospitals took financial hit from Change hack, AHA says

By **Amina Niasse**

April 30, 2024 8:57 PM UTC · Updated 14 days ago

The corporate logo of the UnitedHealth Group appears on the side of one of their office buildings in Santa Ana, California, U.S., April 13, 2020. REUTERS/Mike Blake/File Photo *Purchase Licensing Rights*

First and third-party financial impact

BITSIGHT

Cybersecurity Risk is Growing Quickly

Expanding digitization, increased sophistication of threat actors and a heightened regulatory environment has resulted in a world in which cyber losses are growing in frequency and severity

Expanding Digitization

Organizations have massive, growing digital footprints and are increasingly interconnected

Sophistication of Threat Actors

Threats are growing with increased monetization for bad actors

Heightened Regulatory Environment

DORA Digital Operational Resilience Act

U.S. Securities and Exchange Commission

Anti Money Laundering Act of 2020

Capital markets and regulators are paying attention

Increased Cyber Losses

$22T Cyber

$8T Social

$4T Climate

Moody's Investors Services (MIS) found that cyber risk outweighs other credit-adjacent enterprise risk factors, and losses can be existential in nature

Exposure & Vulnerability

CISA’s KEV Catalog
Who's at risk and who’s fastest to fix

Benjamin Edwards, PhD
Principal Research Scientist, Bitsight

BITSIGHT

What is the KEV Catalog?

List of vulnerabilities known by CISA to be the subject of **active exploitation** attempts in the wild

Three (official) criteria for inclusion

1. Common Vulnerability Enumeration (CVE) ID must have been issued
2. Remediations are available (patches or workarounds)
3. Evidence of active exploitation

Not all vulnerabilities that meet the criteria are included in the KEV.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

BINDING OPERATIONAL DIRECTIVES

BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities

November 03, 2021

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

What's a KEV look like?

Product and Vendor

Vulnerability Type

Remediation Actions

Ransomware use

Deadline for federal agencies

Description and resources.

CONNECTWISE | SCREENCONNECT

CVE-2024-1709

ConnectWise ScreenConnect Authentication Bypass Vulnerability

ConnectWise ScreenConnect contains an authentication bypass vulnerability that allows an attacker with network access to the management interface to create a new, administrator-level account on affected devices.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Known
- **Date Added:** 2024-02-22
- **Due Date:** 2024-02-29

Resources and Notes +

https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

What's a KEV look like?

Product and Vendor

Vulnerability Type

Remediation Actions

Ransomware use

Deadline for federal agencies

Description and resources.

CONNECTWISE | SCREENCONNECT

CVE-2024-1709

ConnectWise ScreenConnect Authentication Bypass Vulnerability

ConnectWise ScreenConnect contains an authentication bypass vulnerability that allows an attacker with network access to the management interface to create a new, administrator-level account on affected devices.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Known
- **Date Added:** 2024-02-22
- **Due Date:** 2024-02-29

Resources and Notes +

https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

What's a KEV look like?

Product and Vendor

Vulnerability Type

Remediation Actions

Ransomware use

Deadline for federal agencies

Description and resources.

CONNECTWISE | SCREENCONNECT

CVE-2024-1709

ConnectWise ScreenConnect Authentication Bypass Vulnerability

ConnectWise ScreenConnect contains an authentication bypass vulnerability that allows an attacker with network access to the management interface to create a new, administrator-level account on affected devices.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Known
- **Date Added:** 2024-02-22
- **Due Date:** 2024-02-29

Resources and Notes +

https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

What's a KEV look like?

Product and Vendor

Vulnerability Type

Remediation Actions

Ransomware use

Deadline for federal agencies

Description and resources.

CONNECTWISE | SCREENCONNECT

CVE-2024-1709

ConnectWise ScreenConnect Authentication Bypass Vulnerability

ConnectWise ScreenConnect contains an authentication bypass vulnerability that allows an attacker with network access to the management interface to create a new, administrator-level account on affected devices.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Known
- **Date Added:** 2024-02-22
- **Due Date:** 2024-02-29

Resources and Notes +

https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

What's a KEV look like?

Product and Vendor

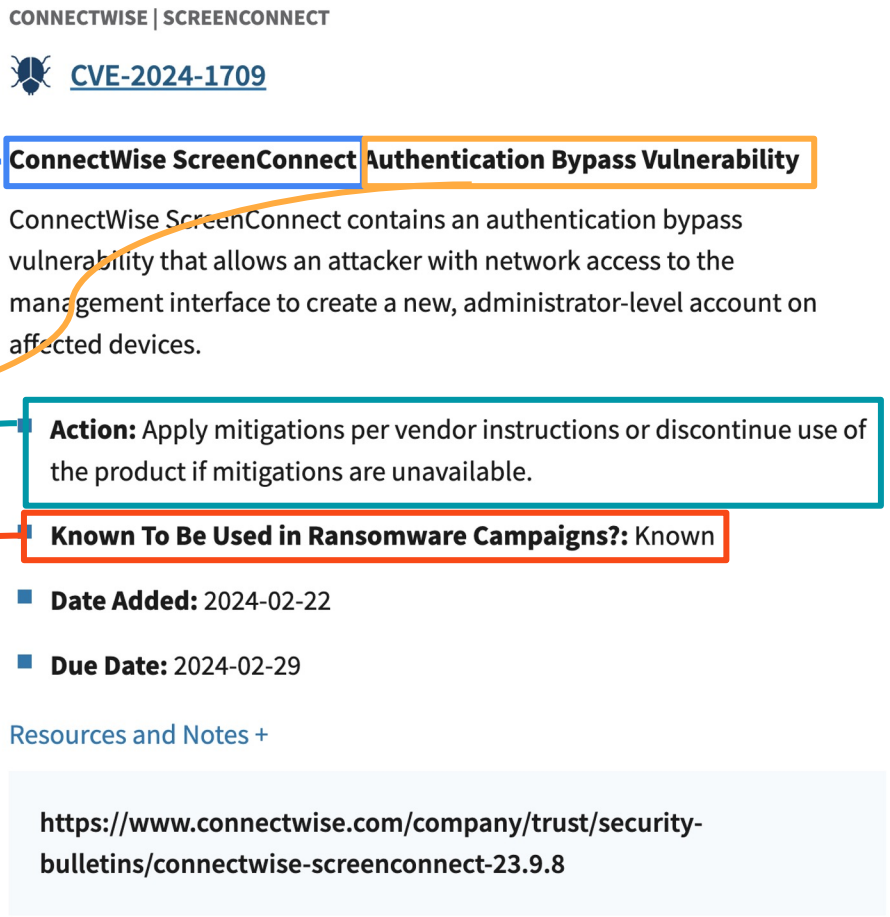
Vulnerability Type

Remediation Actions

Ransomware use

Deadline for federal agencies

Description and resources.



What's a KEV look like?

Product and Vendor

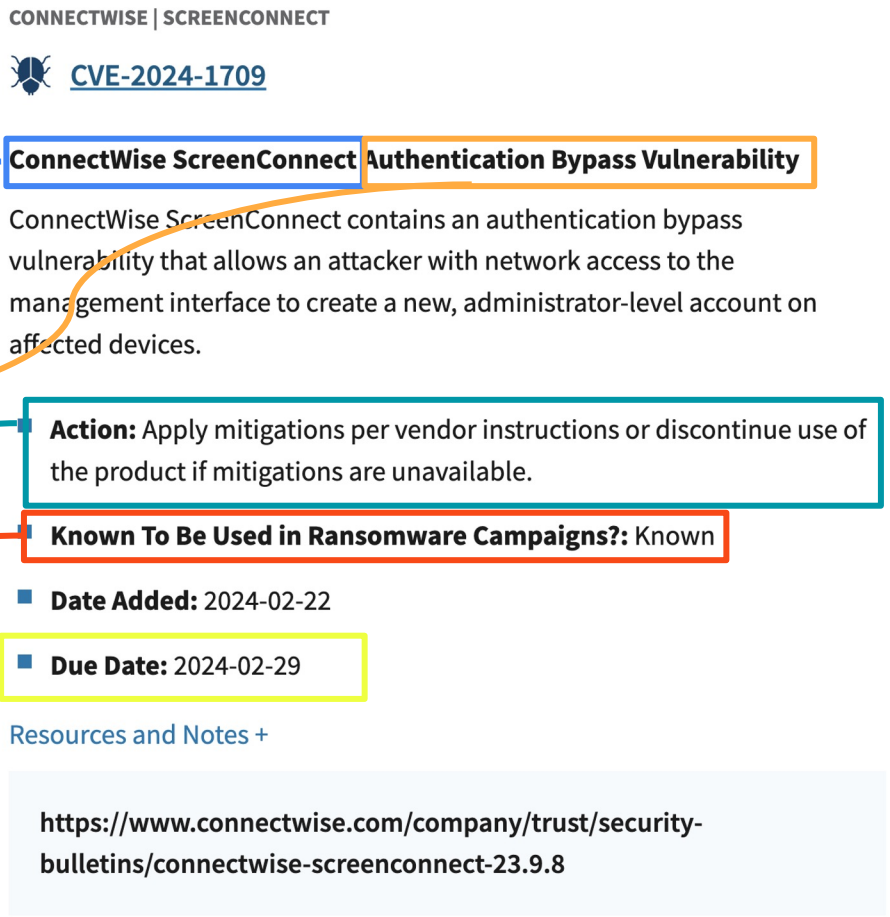
Vulnerability Type

Remediation Actions

Ransomware use

Deadline for federal agencies

Description and resources.



What's a KEV look like?

Product and Vendor

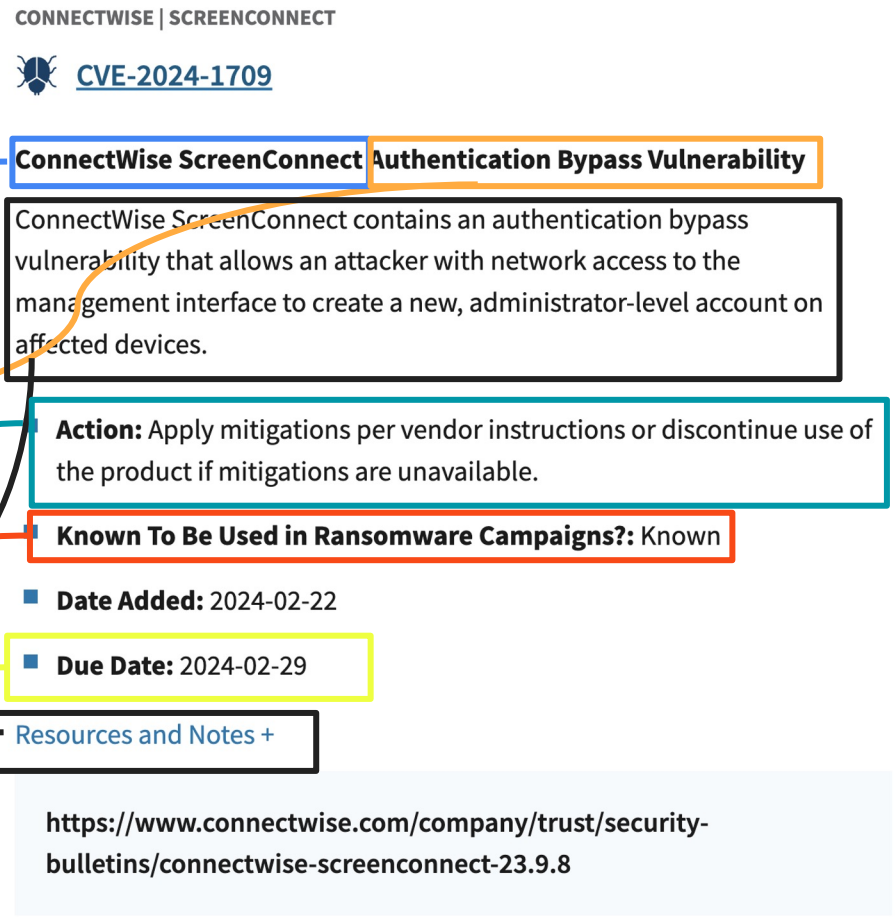
Vulnerability Type

Remediation Actions

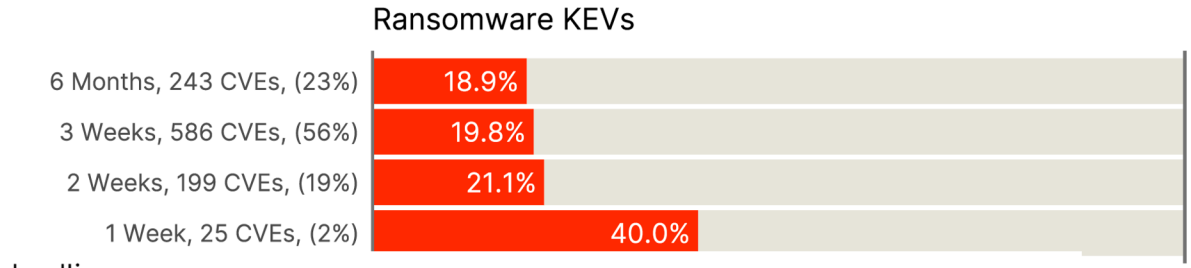
Ransomware use

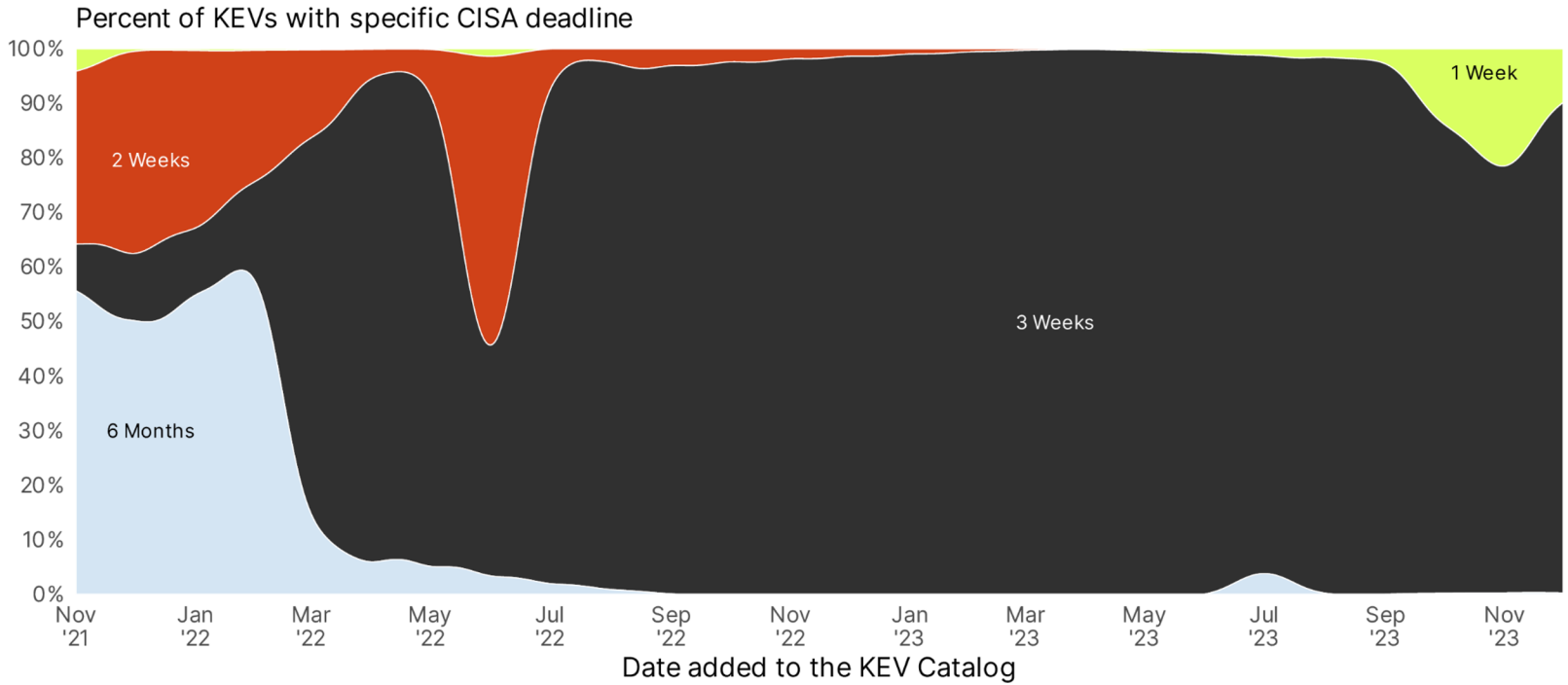
Deadline for federal agencies

Description and resources!



Deadlines & Ransomware





What Bitsight sees and why it's different than other views

Bitsight continuously, carefully scans the entire Internet

Some KEVs won't be visible to Bitsight

- Non Network Accessible
- Client Side Software
- Detectable without Active Exploitation
- ~20% of the KEV

A more relevant view

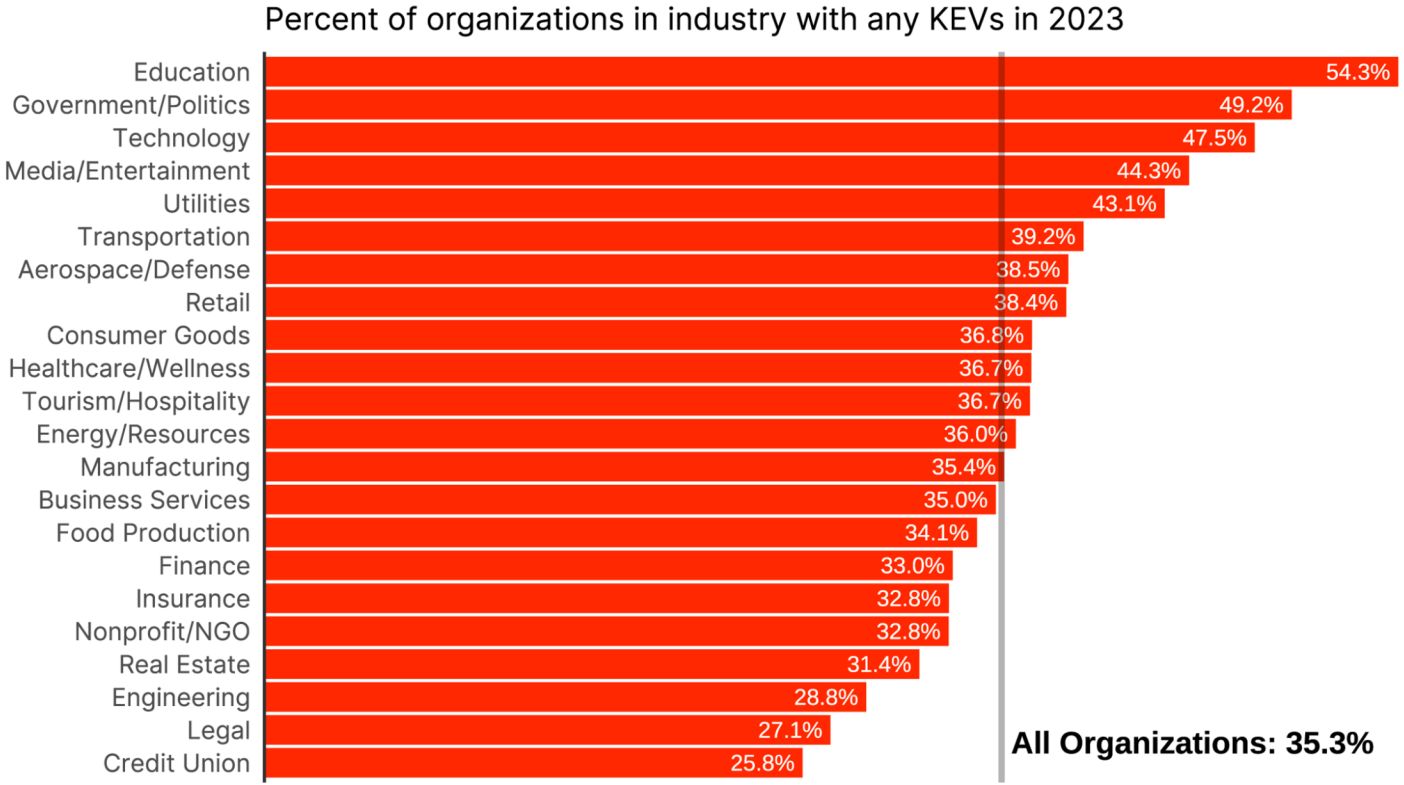
- Not limited to organizations with Vulnerability Management Software
- **Similar view to that of attackers**

35% of organizations had a KEV in 2023

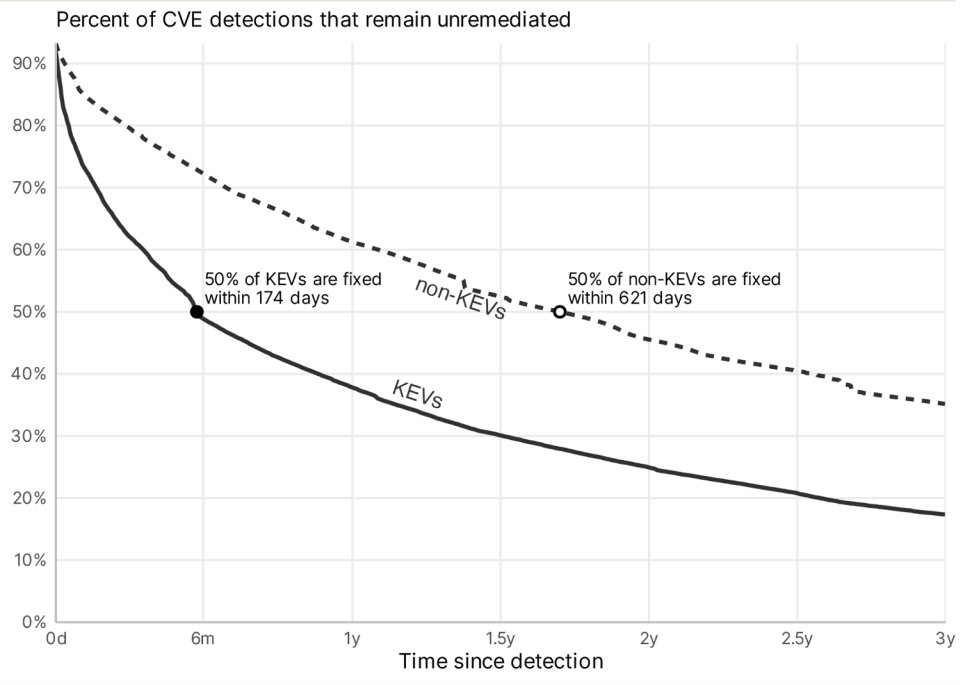
20% of organizations had a ransomware KEV in 2023

Analysis of detections during 2023.

KEV Prevalence and Industry



Remediating KEVs



Prevalence is not the only measure of risk, we are also interested in how organizations react.

KEVs are often zero (or near) days
Speed and completeness are both important

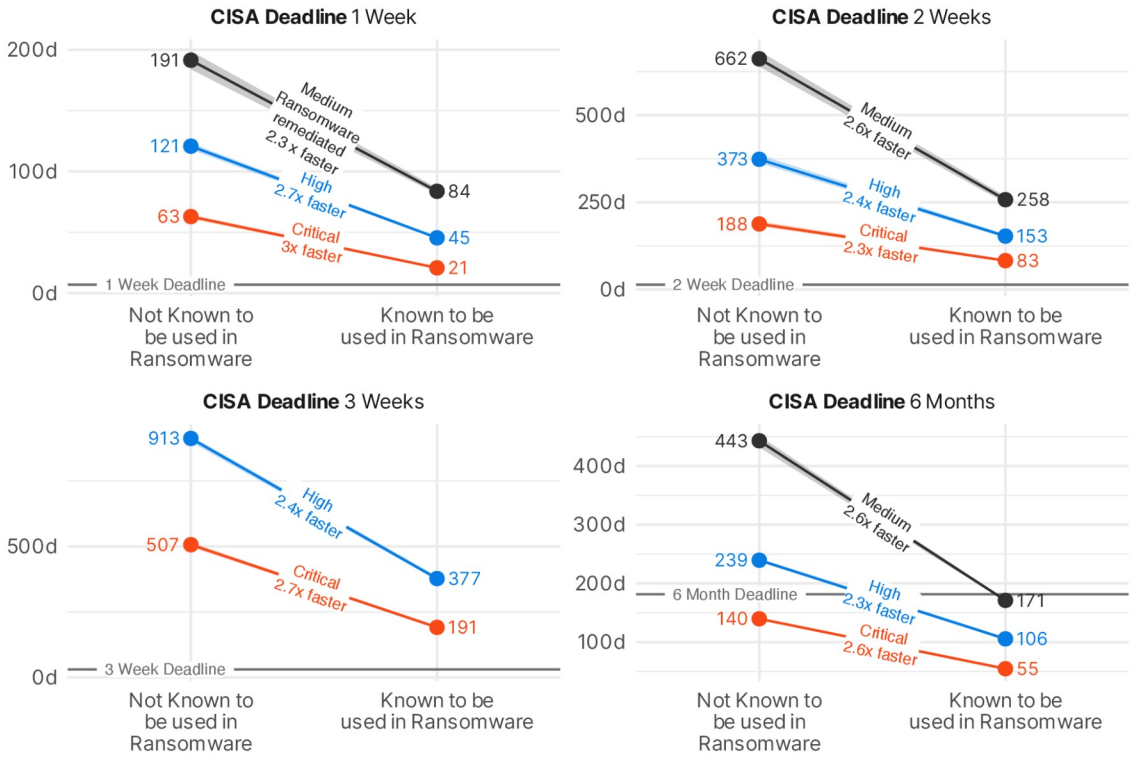
Survival Analysis

Developed in medical research
Measure first detection
Measure last detection and status

50% of KEVs are fixed in 174 days
50% of non-KEVS are fixed in 621 days

Organizations Fix Ransomware Faster

Median KEV remediation time (days)

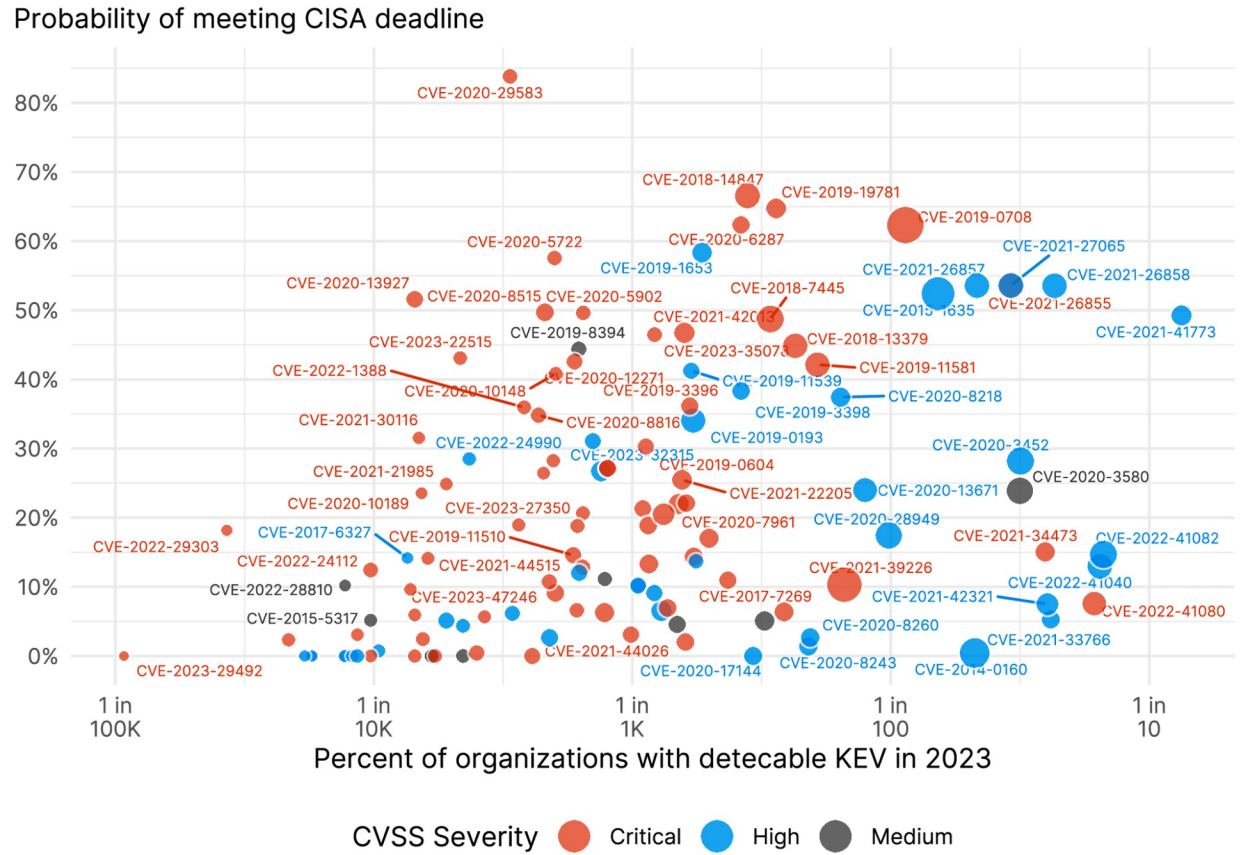


Ransomware KEVs are fixed

2.5x faster

than KEVs not known to be used in Ransomware

Deadline by Prevalence



40%

of KEVs are remediated by the CISA deadline

Operational Technology

Critical Infrastructure Attacks

Russian Cyber Attacks Against Germany and Czechia Deemed 'Malicious' by EU and NATO

Story by Jeff Rod • 1w • 2 min read

The European Union and NATO have issued strong statements condemning Russia for its alleged involvement in a malicious cyber campaign targeting democratic institutions, government entities, and critical infrastructure providers across the EU and beyond.

The statements, released on Friday, blame the Russian military intelligence service-linked group APT28 for the cyber attacks, which aimed to degrade critical infrastructure, weaken societal cohesion, and influence democratic processes, including the June elections to the European Parliament.

POLITICO

War in Ukraine | Israel-Hamas war | Farmers' protests | Newsletters | Podcasts | Poll of Polls | Policy news | E

NEWS ENERGY AND CLIMATE

Europe's grid is under a cyberattack deluge, industry warns

Cyberattacks against the energy sector have spiked. The sector needs to speed up, chief officials say.

Critical Infrastructure Attacks

NSA leadership discusses critical infrastructure cyber threats

David Luber, director of cybersecurity at the NSA, discussed cyber threats impacting critical infrastructure with his predecessor, Rob Joyce, at an RSAC 2024 session.

Source: Getty Images

*"I think the area of most concern for me is when **cyber** can turn to **physical**," Luber said.*

*"At some point, somebody's going to land one of these in a place against **critical infrastructure** that's going to matter," Joyce said*

OT Exposure

Top Most Vulnerable Countries

1. United States
2. Canada
3. Italy
4. United Kingdom
5. France
6. Netherlands
7. Germany
8. Spain
9. Poland
10. Sweden

8 / 10 most vulnerable countries are in Europe

Bitsight identifies nearly 100,000 exposed industrial control systems

BITSIGHT SECURITY RESEARCH

Written by Noah Stone | Research by Pedro Umbelino | October 02, 2023 SHARE

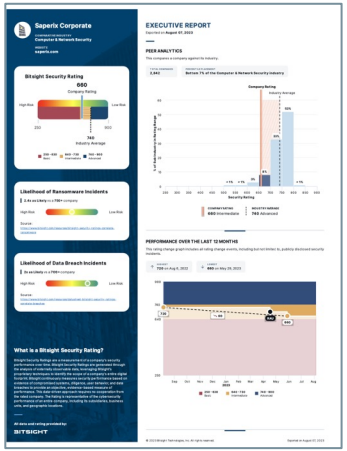
Business Under Pressure

Bitsight Cyber Analytics in Business Risk

Bitsight's leading dataset (and its correlation to risk) enable new applications of cyber analytics

Moody's

GLASS LEWIS



MarshMcLennan

NOMURA

*Bitsight ratings and metrics are cited in **100+** Annual / ESG / Sustainability Reports published by companies*

MSCI Capgemini NVIDIA DHL New York Power Authority EQUIFAX

Implied Cyber Risk (ICT) Capability

INTELLIGENT CIO

Bitsight and Moody's launch new cyber risk solution covering more than 325 million organisations

SC MEDIA

New Bitsight, Moody's service seeks to bolster cyber risk management

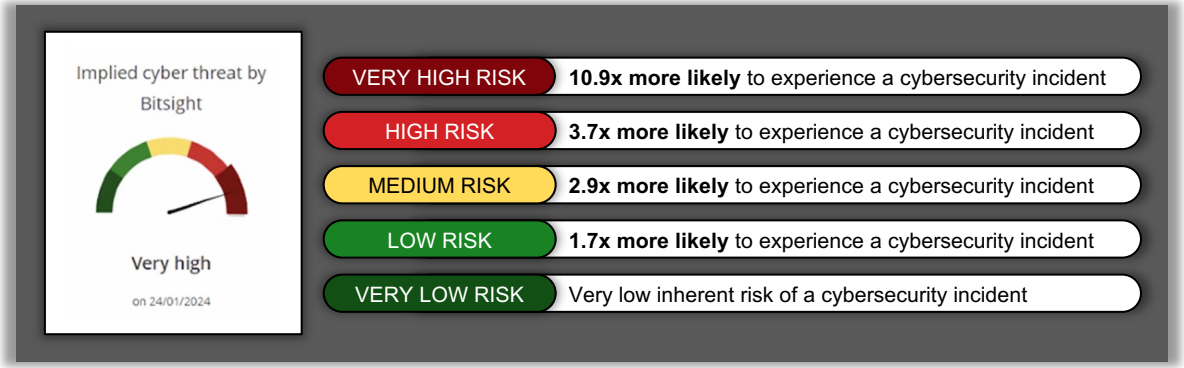
SC Staff April 23, 2024

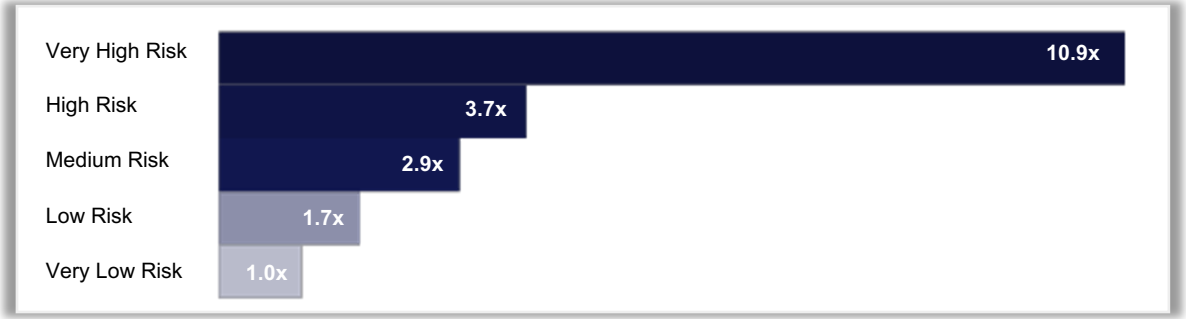
MOODY'S

Fortifying Risk Management with Advanced Cybersecurity Analytics: A Moody's and Bitsight Partnership

Elevate your holistic third-party risk management with cybersecurity insights

Likelihood of Cybersecurity Incident vs. Very Low Risk Category





Cyber & Credit in Practice

Corporate Cybersecurity Risk – A Guide for Investors: Part 1

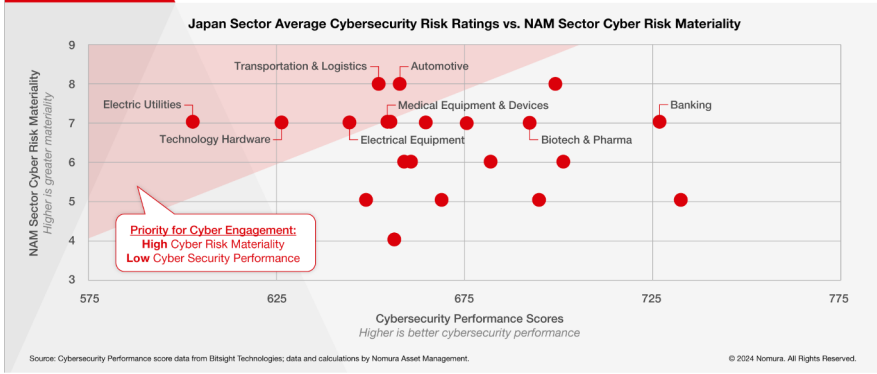
Corporate Cybersecurity Risk – A Guide for Investors: Part 2

- Cyber is Nomura's "biggest ESG risk"
- Cyber risk is **unpriced**, representing an opportunity for improved portfolio performance & underwriting
- Cybersecurity maturity can be seen as a unique proxy for corporate governance and as a positive indicator of effective systems & risk management
- Like investors, all organizations can use Bitsight cyber risk data & analytics as a downside early warning signal for adverse cyber events, as a low-latency proxy for broader corporate governance and technology management, or both

"Cyber performance data & analytics can enable data-driven cybersecurity engagement for measurable cybersecurity impact at portfolio companies"

NOMURA

Combine issuer-level cybersecurity performance with sector-level cyber risk materiality to prioritize at-risk corporates for cybersecurity engagement



Risk Mgmt Results

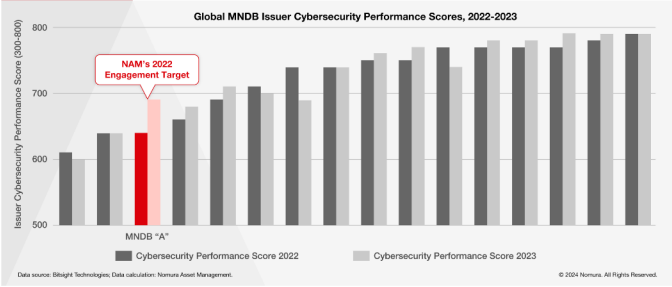
- Nomura can now track significant improvement across the firm in terms of cyber performance: **measurable results & impact**
- This results in significantly lower likelihood of material events across the portfolio and a greater urgency across portfolio to manage critical risk
- Bitsight enables the Sustainable Investment Fixed Income team to:
    1. Highlight data driven metrics that tangibly correlate to firm performance and losses
    2. Easily identify outliers within a peer group
    3. Prioritize outliers for light touch engagement and need for better performance

Corporate Cybersecurity Risk – A Guide for Investors: Part 1

Corporate Cybersecurity Risk – A Guide for Investors: Part 2

NOMURA

Nomura AM engaged with MNDB debt-issuers to improve organizational cybersecurity performance from 2022 to 2023 with measurable results and impact



NOMURA

Engagement Impact Analysis for MNDB "A" – Three Month Follow-up

MNDB "A"	Performance at Engagement *T*	Performance at Follow-up *T+3 months*	Calculated Engagement Impact
Relative Cybersecurity Performance Rating to Peers	**-1.2** standard deviations below sector average	**-0.2** standard deviations below sector average	**+1.0** standard deviations improvement in relative cybersecurity performance
Bitsight Cybersecurity Rating Score (300-820 scale)	**640** (Low-Intermediate)	**700** (Mid-Intermediate)	**+60** (Low-Intermediate to Mid-Intermediate)
Ransomware Incident Risk (vs. 750+ entity)	**4.6x** as likely	**1.9x**	**~60% relative improvement**
Data Breach Incident Risk (vs. <700 entity)	**2.0x** as likely	**0.5x**	**~75% relative improvement**
Risky User Behavior Detected?	**Yes** (Botnet Infection and File Sharing)	**No**	**Resolved**

Data source: Bitsight Technologies; Data calculation: Nomura Asset Management.

© 2024 Nomura. All Rights Reserved.

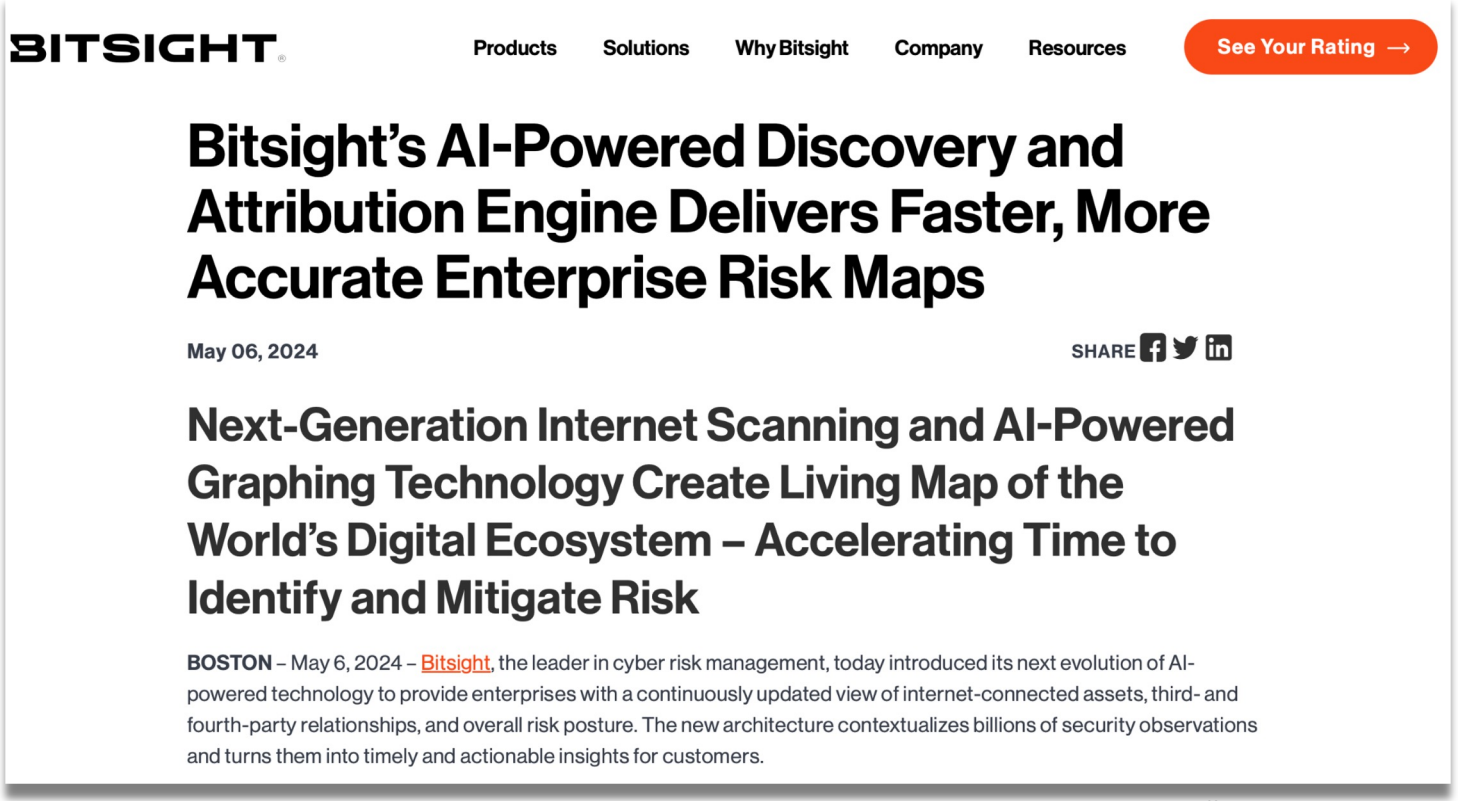
Artificial Intelligence

Bitsight Approach to AI

Multi-layered Approach

Layer	Approach
Governance	• Assure adherence to laws and policies to comply and manage risks • Risk-management process to enable rapid adoption
Operational Adoption	• *External*: Adopt tools and services to augment operational capability • *Internal*: Develop capabilities that permit the more efficient operations and delivery of customer facing services
Customer Delivery (incremental)	• AI-enabled features and functionality that solve and improve a customer job that we already offer or offer new capabilities that solve new jobs
Transformation (leap-ahead)	• Identify, develop, and operate capabilities that can leap-ahead of current capabilities and substantially transform the business

AI-Powered Discovery & Attribution



BITSIGHT

Products Solutions Why Bitsight Company Resources See Your Rating →

Bitsight's AI-Powered Discovery and Attribution Engine Delivers Faster, More Accurate Enterprise Risk Maps

May 06, 2024 SHARE

Next-Generation Internet Scanning and AI-Powered Graphing Technology Create Living Map of the World's Digital Ecosystem – Accelerating Time to Identify and Mitigate Risk

BOSTON – May 6, 2024 – Bitsight, the leader in cyber risk management, today introduced its next evolution of AI-powered technology to provide enterprises with a continuously updated view of internet-connected assets, third- and fourth-party relationships, and overall risk posture. The new architecture contextualizes billions of security observations and turns them into timely and actionable insights for customers.

Thank you!

111 Huntington Ave
Suite 2010
Boston, MA 02199
USA

bitsight.com
sales@bitsight.com

BITSIGHT