BITSIGHT

ARCTIC WOLF

The Hartford

Beyond the Policy: Active Cyber Risk Management in Action

Jennifer Birnbaum - Cyber Underwriting Officer - The Hartford

Daniel Silverman - Underwriting Director, Specialized CyberTech - The Hartford

Keith Tagliaferri - Director, Cyber Claim Practices - The Hartford

Will Ricciardi - Strategic Customer Success Manager - BitSight

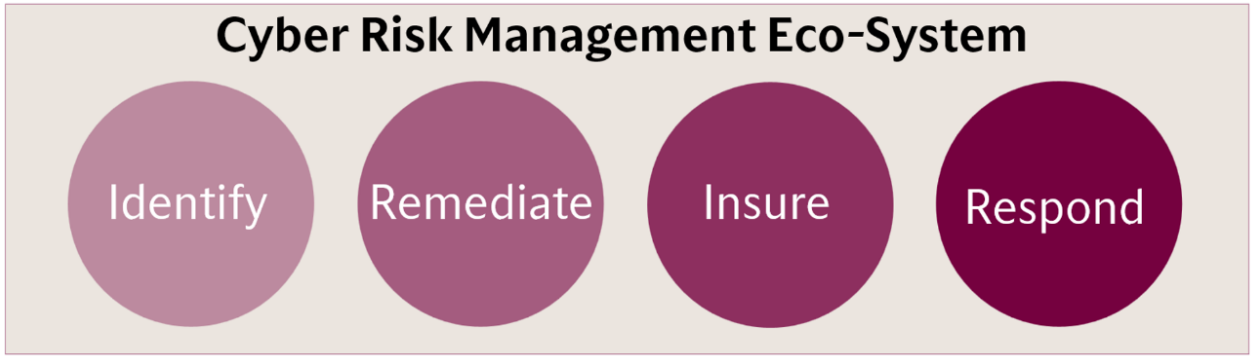
Scott Wood - Strategic Account Manager - BitSight

Alex Quevedo - Senior Incident Response Engineer - Arctic Wolf Incident Response

October 21, 2025

Our Role – CyberTech Insurance & Risk Management

The Hartford



Agenda

Topic	Discussion Lead(s)
Introduction to Active Insurance & Why It Matters: Risk Management & Active Portfolio Monitoring	Jennifer Birnbaum Keith Tagliaferri Dan Silverman
Bitsight Exposure Management: What is a CVE? BitSight's Detection Methods & Calculations	Will Ricciardi Scott Wood
Step 1: Active Portfolio Monitoring— Outreach from the Hartford	Jennifer Birnbaum Keith Tagliaferri Dan Silverman
Step 2: Artic Wolf's Cybersecurity Remediation & Hardening	Alex Quevedo
Questions?	

Active Portfolio Monitoring

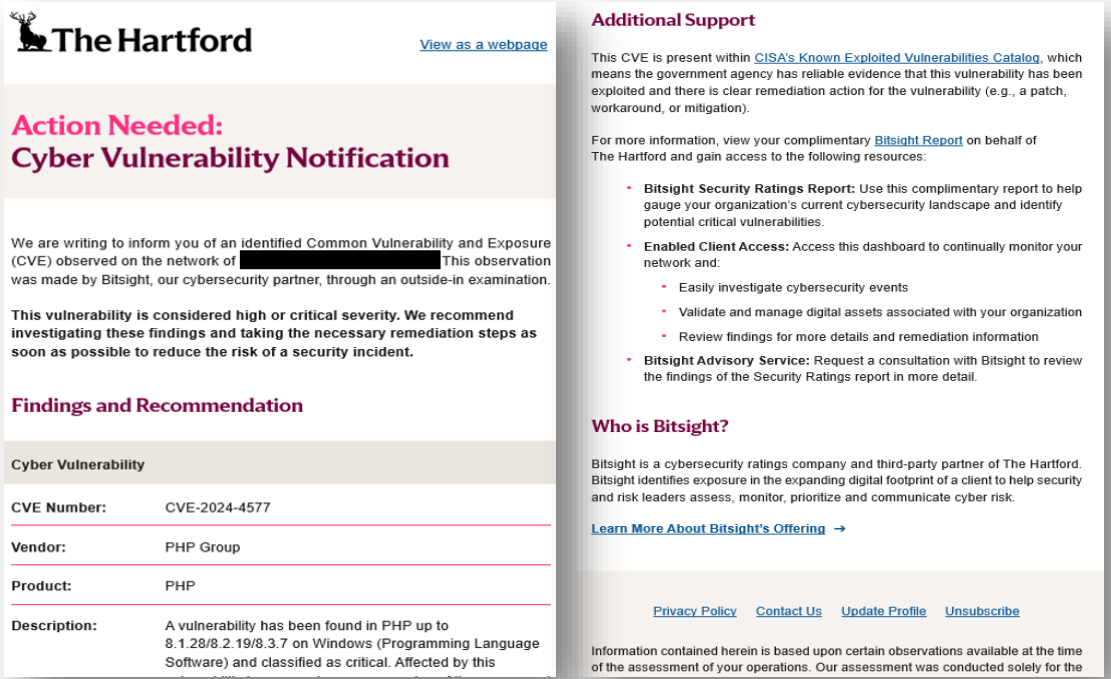
Active Portfolio Monitoring leverages the same outside-in view observed of an individual risk at underwriting, but continuously throughout the term, and of the entire in-force portfolio. We can observe exposure to certain critical vulnerabilities or common software, which enables us to help existing customers remediate vulnerabilities and correct configurations before an incident occurs.

Active Portfolio Monitoring Outreach is LIVE!

Leveraging 3rd party data custom reports and cybersecurity contact information where available, we will reach out to insureds with high severity critical vulnerabilities monthly in custom emails, and copy brokers.

Outreach occurs for CVEs that meet this criteria:

- CVSS Score/severity 8.0 or higher
- Are actively being exploited in the wild
- Have a remediation available
- Were observed by Bitsight in the last 3 weeks



The Hartford

View as a webpage

Action Needed:
Cyber Vulnerability Notification

We are writing to inform you of an identified Common Vulnerability and Exposure (CVE) observed on the network of [redacted] This observation was made by Bitsight, our cybersecurity partner, through an outside-in examination.

This vulnerability is considered high or critical severity. We recommend investigating these findings and taking the necessary remediation steps as soon as possible to reduce the risk of a security incident.

Findings and Recommendation

Cyber Vulnerability	
CVE Number:	CVE-2024-4577
Vendor:	PHP Group
Product:	PHP
Description:	A vulnerability has been found in PHP up to 8.1.28/8.2.19/8.3.7 on Windows (Programming Language Software) and classified as critical. Affected by this

Additional Support

This CVE is present within CISA's Known Exploited Vulnerabilities Catalog, which means the government agency has reliable evidence that this vulnerability has been exploited and there is clear remediation action for the vulnerability (e.g., a patch, workaround, or mitigation).

For more information, view your complimentary Bitsight Report on behalf of The Hartford and gain access to the following resources:

- **Bitsight Security Ratings Report:** Use this complimentary report to help gauge your organization's current cybersecurity landscape and identify potential critical vulnerabilities.
- **Enabled Client Access:** Access this dashboard to continually monitor your network and:
  - Easily investigate cybersecurity events
  - Validate and manage digital assets associated with your organization
  - Review findings for more details and remediation information
- **Bitsight Advisory Service:** Request a consultation with Bitsight to review the findings of the Security Ratings report in more detail.

Who is Bitsight?

Bitsight is a cybersecurity ratings company and third-party partner of The Hartford. Bitsight identifies exposure in the expanding digital footprint of a client to help security and risk leaders assess, monitor, prioritize and communicate cyber risk.

Learn More About Bitsight's Offering →

Privacy Policy Contact Us Update Profile Unsubscribe

Information contained herein is based upon certain observations available at the time of the assessment of your operations. Our assessment was conducted solely for the

Third-party service providers discussed herein, though not affiliates of The Hartford, are pre-approved by The Hartford to provide cyber-related services. You are not required to avail yourself of their services. Sharing any information with any such vendor is at your sole discretion. References to any vendor are provided for your convenience only and are not intended as a substitute for your own due diligence and selection of vendors to suit your company's needs. The vendors are independent contractors that charge their own rates. Discounted rates offered by any vendor are not offered by The Hartford, nor on any premium for a policy of insurance. Any such vendor discount is subject to change without notice and is not guaranteed by The Hartford. The Hartford does not warrant the performance or services of the vendors or their websites. The Hartford assumes no responsibility for the control, correction or legal compliance of your cyber security measures or other business practices and operations. Notice of any claim, act, fact or circumstance to a vendor does not constitute notice thereof to The Hartford. Approved vendors are current as of August 2025 and may change at our discretion at any time, with or without notice.

BITSIGHT

Cyber Risk Reduction with the Hartford and Arctic Wolf

How Bitsight Helps Prioritize, Communicate, and Mitigate Cyber Risks

Will Ricciardi and Scott Wood

October 21, 2025

Bitsight Speakers

Will Ricciardi

Distinguished Strategic Customer Success Manager

Scott Wood

Strategic Account Manager, Insurance

Ashley Ritrovato

Manager, Professional Services

BITSIGHT

Customers and Analysts

3500+
Customers

50%
Cyber insurance policies

50,000
Active users

4/5
Top investment banks

130+
Government agencies

4/4
Big 4 consulting firms

CHUBB · NASA · Lufthansa

Google · Snowflake · Schneider Electric

Leader, Frost Radar

External Attack Surface Management |
External Risk Mitigation and Management

Leader, The Forrester Wave

Cybersecurity Risk Ratings Platforms

Leader, KuppingerCole

External Attack Surface Management

Our Vulnerability Data Differentiation

1. **Scale** - we continuously scan and detect vulnerabilities across the entirety of the public-facing Internet
2. **Confidence** - we go beyond inferring the presence of possible vulnerabilities to creating high-confidence, active detections for specific vulnerabilities
    a. This often requires reverse engineering software based on vulnerability disclosures often with little-to-no public information available

Tracking Vulnerabilities

Detection Capabilities

Bitsight uses a combination of active probing, fingerprinting, and automated mapping to detect vulnerabilities, delivering accurate and timely insights into exposure risk.

Active Probes

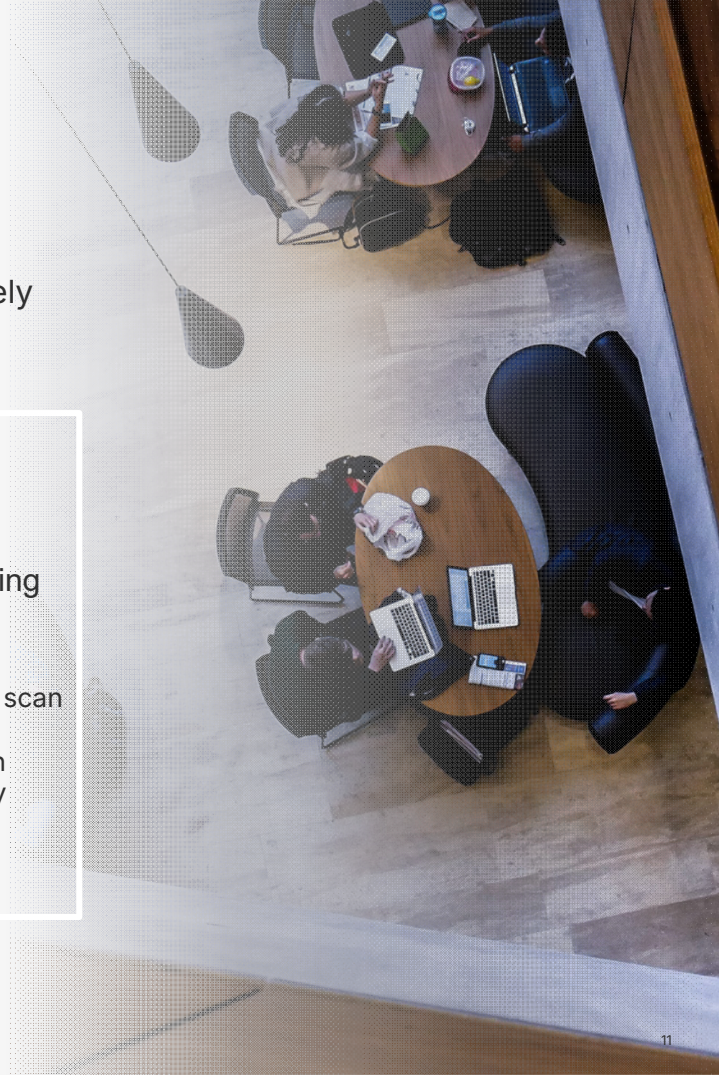
Interact directly with a vulnerable component to assess if it is in a vulnerable state

Fingerprinting

Actively probe a system to identify a software version and evaluate vulnerable status based on vendor advisory

Automated Mapping

Passively observe software versions in scan data and lookup vulnerability status in National Vulnerability Database (NVD)



Exposure Detection & Evidence Certainty

Exposure detection and evidence certainty describes how conclusively evidence shows that a company is exposed to or has mitigated a vulnerability.

Possible

This level indicates that Bitsight has detected some relationship or usage of a product known to have CVEs, but cannot determine whether the specific vulnerability is present or exposed in the environment.

Likely

This level indicates that Bitsight has observed more specific technical evidence, such as product name and version details, that match known vulnerable versions.

Bitsight cannot determine whether security mitigations are present that would prevent exploitation, as Bitsight does not conduct intrusive penetration tests.

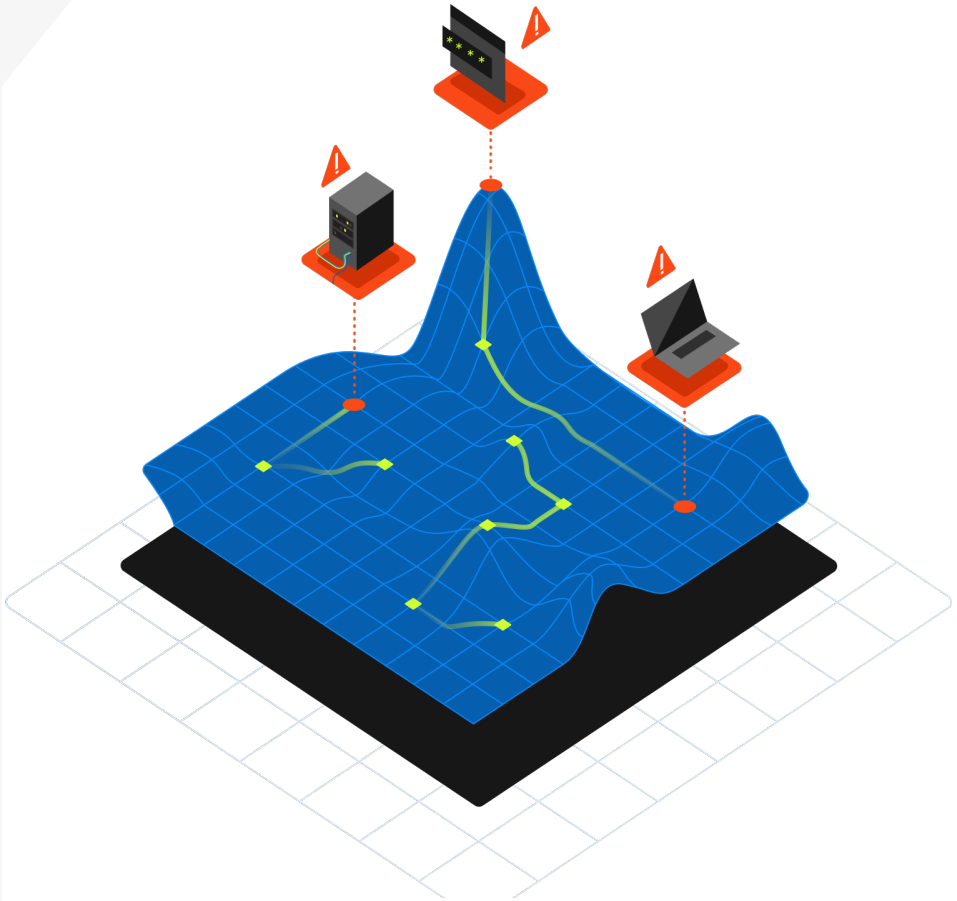
Confirmed

This level means that Bitsight has observed all necessary technical evidence to determine that the CVE is not only present but also unprotected or unmitigated in the company's environment.

Defining CVE Risk

CVE Criteria

- **High Severity:** CVSS v3.1 score of 8.0 or greater.
- **Exploited:** Listed on CISA's Known Exploited Vulnerability (KEV) list.
- **Bitsight Evidence Certainty:** “Confirmed” or “Likely”
- **Recently Observed:** Observed within the last 3 weeks.



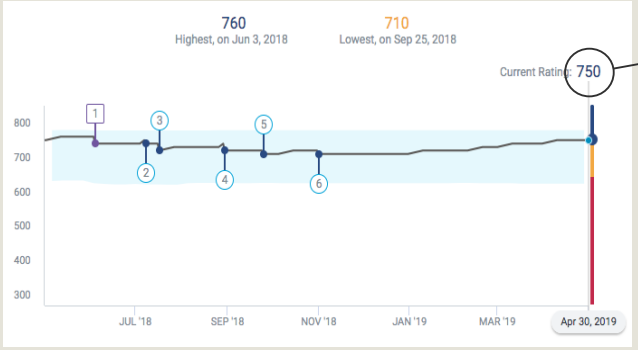
Bitsight
Methodology Overview

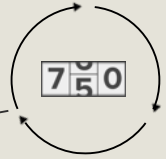
The Bitsight Rating

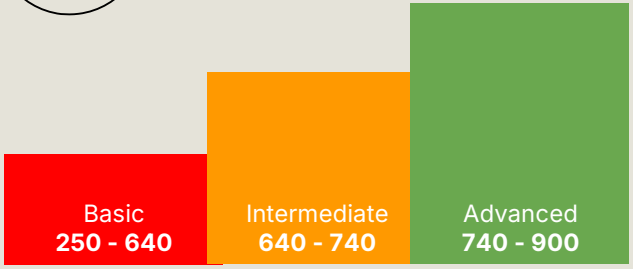
Translate Complex Cybersecurity Issues into Simple Business Context

Objective, Continuous, Data-Driven Ratings of Organizational Security Performance

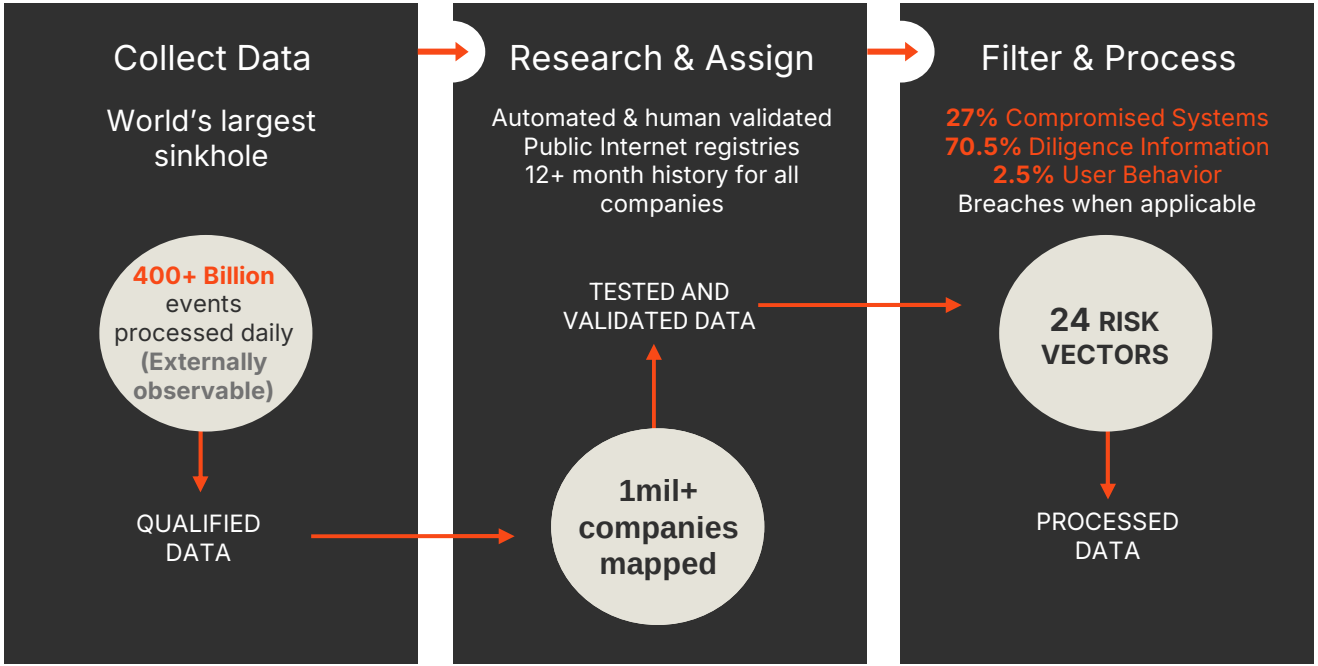
- Unbiased common metrics to measure cybersecurity performance of organizations worldwide
- Data-driven rating of security performance
- Non-intrusive SaaS platform
- Daily ratings and alerts







How Bitsight Security Ratings are Calculated



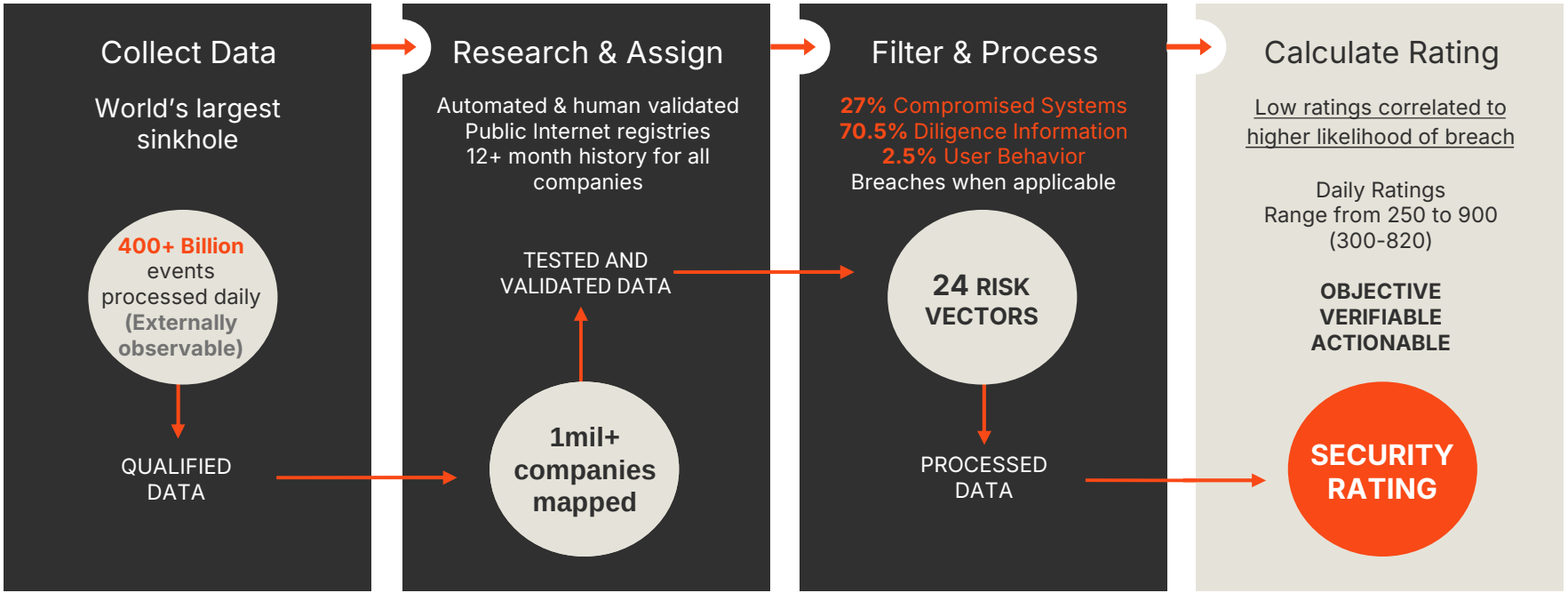
23 Risk Vectors

27% Compromised Systems
Botnet Infections
Spam Propagation
Malware Servers
Unsolicited Comms
Potentially Exploited

70.5% Diligence Information
SPF Domains
DKIM Records
SSL Certs/Config
Open Ports
Web Application Headers
Patching Cadence
Insecure Systems
Server Software
Desktop Software
Mobile Software
DNSSEC
DMARC
Mobile Application Security
Web Application Security
Domain Squatting

2.5% User Behavior
File Sharing
Breaches if Applicable

How Bitsight Security Ratings are Calculated



Strong validated correlation to data breach

IHS Markit · AIR · Advisen Transforming • Insurance

Likelihood of Data Breach

5x If the security rating drops below 400 as compared to an organization with a 700 or higher

BITSIGHT

Likelihood of Ransomware

6.4x If the security rating drops below 600 as compared to an organization with a 750 or higher

MarshMcLennan

Likelihood of Security Incident

14 14 risk vectors, including the rating itself, showed “statistically significant” correlations to the likelihood of a cybersecurity incident

2x

Botnet Grade is B or lower
File Sharing grade is B or lower
Open Ports grade is F

7x Patching Cadence Grade is **C or lower**
4x TLS/SSL Configurations Grade is **C or lower**
3x TLS/SSL Certifications Grade is **C or lower**

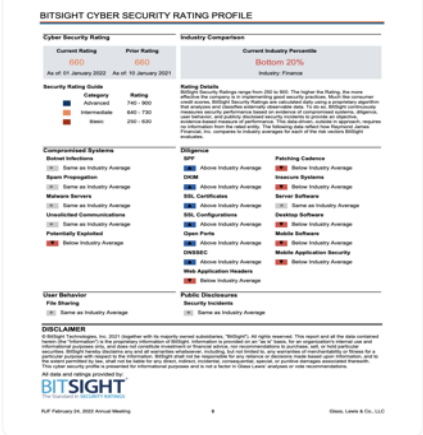
1 Patching Cadence
2 Desktop Software
3 Potentially Exploited

Bitsight is the Standard in Cyber Analytics

Leading dataset and correlation to risk enables new applications

Moody's

GLASS LEWIS

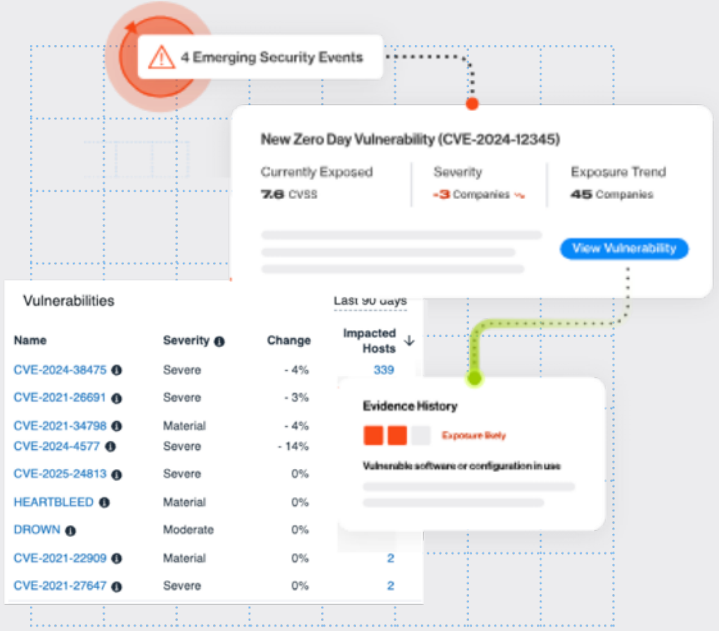


MarshMcLennan

EQUIFAX

Exposure Management

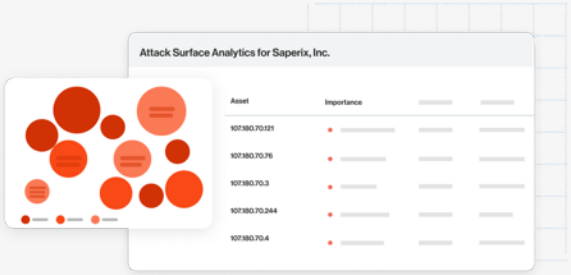
Combines external attack surface management, cyber threat intelligence, and governance reporting to enable security leaders to discover, prioritize, mitigate, govern, and communicate risk across their digital infrastructure.



Exposure Management

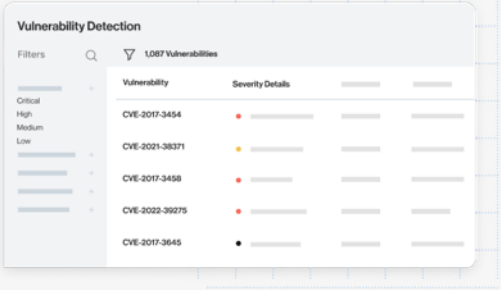
Map your assets

Gain full visibility across subsidiaries, cloud environments, assets, and third parties.



Identify & prioritize vulnerabilities

Add business context to allocate time and resources to remediate the most critical exposures.



Contextualize exposure with threat intelligence

Incorporate DVE scoring into your internal patching cadences

20% Reduction in time monitoring attack surface vulnerabilities

45% Reduction in probability of breach

Bitsight Professional Services

Dedicated Support Journey

Opt-In Access

- Client submits name/email on The Hartford's Bitsight landing page
- Client receives 60-day free access to Bitsight platform
- Consultant emails client to inquire on questions and/or schedule a call

Advisory Call with Consultant

- Review CVE findings, Bitsight rating & remediation priorities
- Guidance on data discrepancies (e.g. misattributed assets)
- Reach us anytime at *bitsight.thehartford.services @bitsighttech.com*

Ongoing Support

- Consultant stays in touch to guide remediation efforts
- Consultant updates shared with The Hartford's Strategic Shared Services Team
- For operational fixes (patching, closing ports, updating software, etc.), Consultant introduces Arctic Wolf

Support at every step - from access to action

ARCTIC WOLF

Cybersecurity Remediation and Hardening

We Are Arctic Wolf

OUR MISSION: END CYBER RISK

10,000+
Customers

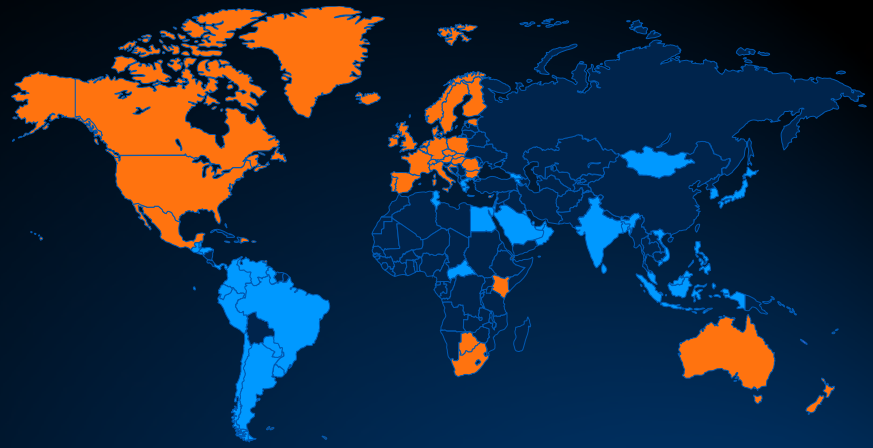
1,000+
Security Engineers

8+
Trillion Events per Week

1,000+
IR Engagements per Year

100+
Countries

2,250+
Partners Globally



Incident Response Other Services

ACROSS OUR FULL PORTFOLIO

PROACTIVE SECURITY
- Cyber Resilience Assessment
- Managed Security Awareness
- Managed Risk
- Incident360 Retainer

REACTIVE SECURITY
- Endpoint Security
- Managed Detection and Response
- Incident Response

RISK TRANSFER
- Insurance Alliances
- Security Operations Warranty

OUR WORK TOGETHER

Example vulnerabilities that have led to severe IR cases:

- **CVE-2024-40766 (Sonicwall/Akira)**
  - Disclosed in August 2024, but resurgence in use by Akira July 2025
  - Underscores criticality of taking ALL remediation steps outlined in vendor guidance – patching/upgrading alone left organizations still at risk

- **CVE-2022-41040, CVE-2022-41080, CVE-2022-41082 (ProxyNotShell, OWASSRF)**
  - ProxyNotShell disclosed in September 2022, patches released November 2022
  - Threat actors found a workaround (OWASSRF) to similarly exploit servers in December 2022

Voice of the Broker

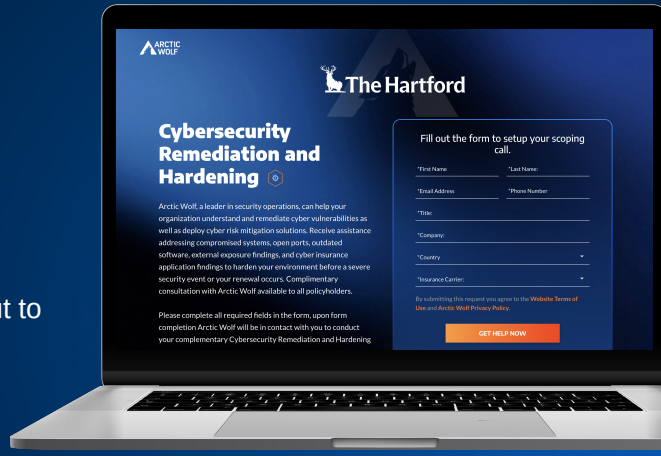
Now that you know the partnerships, vulnerabilities, pitfalls, and solutions available, what can you do?

Insurance-Alliances @ArcticWolf.com

The next disclosed vulnerability or alert from your carrier & technology partners, reach out to your clients with our Security Bulletins.

Does your client need assistance to ensure remediation of their vulnerabilities? They can engage our team here.

Are your clients IR ready? Broker partners can offer Arctic Wolf IR Readiness Resources by reaching out to our team:



Questions?

Disclaimer

The information provided in these materials is intended to be general and advisory in nature. It shall not be considered legal advice. The Hartford does not warrant that the implementation of any view or recommendation contained herein will: (i) result in the elimination of any unsafe conditions at your business locations or with respect to your business operations; or (ii) be an appropriate legal or business practice. The Hartford assumes no responsibility for the control or correction of hazards or legal compliance with respect to your business practices, and the views and recommendations contained herein shall not constitute our undertaking, on your behalf or for the benefit of others, to determine or warrant that your business premises, locations or operations are safe or healthful, or are in compliance with any law, rule or regulation. Readers seeking to resolve specific safety, legal or business issues or concerns related to the information provided in these materials should consult their safety consultant, attorney or business advisors. All information and representations contained herein are as of October 2025.