BITSIGHT

EBOOK

A Critical Guide to Closing Your Exposure Management Gaps

A Blueprint For Using Exposure Management Visibility to Level Up Security Maturity

Table of Contents

Executive Summary 3

CISOs in Crisis 5

- Exposures Grow Exponentially
- Stakes Are Higher Than Ever

Enter Exposure Management 9

- Moving From Protector to Risk Leader
- Tackling the Security Visibility Problem
- Exposure Management 101
- Wading Through Exposure Management Alphabet Soup
- The Difference Between Exposure Management and Cyber Risk Metrics

Getting the Most Out of Exposure Management 16

- 10 Ways CISOs Can Use Exposure Management to Enhance Security Activities
- What Exposure Management Gives CISOs
- How Bitsight Powers Exposure Management

01 Executive Summary

01 Executive Summary

Exposure management practices and attack surface management tooling can provide CISOs with a sound path to transform themselves from tactical enterprise protectors to strategic risk leaders.

The visibility and context afforded by exposure management offers security leaders and the practitioners that execute their strategies with the information they need to:

Prioritize security investments

Take action to close the exposures that pose the biggest risk to the business

Validate the organization's cyber risk posture to the board and regulators with meaningful data

Quickly respond to software supply chain incidents and industry-wide zero-day attacks

This is your guide to understanding why leading CISOs and industry analysts call exposure management one of the strategies most uniquely positioned to help security leaders prioritize their efforts.

02

CISOs in Crisis

02 CISOs in Crisis

Exposures Grow Exponentially

As digital infrastructure in the enterprise keeps expanding, work models grow more fluid, and digital ecosystems expand far outside the confines of corporate boundaries, CISOs have been stretched to the limit.

They're challenged to manage risks across an enterprise attack surface that grows by the day. As enterprises double down on cloud-native software, lean on more digital vendors than ever, and engage in development practices that use and reuse countless open source and proprietary software components, it has become harder than ever to track exposures across the digital supply chain. Meantime, cybercriminals push to exploit every exposure to the fullest, spurred by financial and political motivations—and the advantages of scale that flaws in the supply chain can afford them

ATTACK SURFACE GROWTH....

62%
of orgs say their attack surface has increased over the past two years[1]

26,447
vulnerabilities were disclosed in 2023[3]

78%
believe their application attack surface is unmanageable[5]

...EXPANDS EXPLOIT OPPORTUNITIES....

20%
There were 20% more breaches in the US during the first nine months of 2023 than any prior year[2]

37%
There was a 37% increase of exploited 0days discovered in the wild in 2023[4]

11 seconds
Around the world there's a ransomware attack attempt every 11 seconds[6]

[1] https://www.techtarget.com/esg-global/research-report/research-report-security-hygiene-and-posture-management-remains-decentralized-and-complex/

[2] https://www.apple.com/newsroom/2023/12/report-2-point-6-billion-records-compromised-by-data-breaches-in-past-two-years/

[3] https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one#:~:text=MITRE%20ATT%26CK%20tactics.-,2023%20Statistics,found%20than%20the%20year%20before

[4] Based on data from Google Project Zero https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit#gid=1746868651

[5] https://cycode.com/state-of-aspm/

[6] https://www.forbes.com/sites/forbesbusinesscouncil/2023/04/06/understanding-ransomware-attacks-and-how-data-centers-can-protect-themselves/?sh=361af765d063

...EXACERBATING CISO RISK MANAGEMENT STRUGGLES

68%
say they struggle to prioritize security actions and improvements to security posture that will have the biggest risk reduction[7]

8%
Only 8% of security leaders are completely confident in their ability to detect and respond to cyber threats [8]

[7] https://www.techtarget.com/esg-global/research-report/research-report-security-hygiene-and-posture-management-remains-decentralized-and-complex/

[8] https://www.isaca.org/resources/reports/state-of-cybersecurity-2023

Attackers are not only barraging organizations with an ever-growing volume of attacks, but getting more efficient by targeting flaws in the software supply chain that allow them to exploit many downstream organizations all at once.. Supply chain attacks like last year's MOVEIt attacks that exploited thousands of organizations through a single vulnerability in a little-known but widely used file transfer app demonstrated this in full effect.

The bad guys are also still making plenty of trouble using their old playbooks for attacks, too. Attackers can still earn a decent living picking apart old vulnerabilities that have been known for a long time. That's because as digital footprints expand, organizations struggle to keep all their systems updated, continuously monitor for threat indicators, audit vendors, and generally keep their risk postures strong.

Stakes Are Higher Than Ever

This increasingly difficult threat environment is pushing poor security outcomes that are raising the stakes for cyber risk management. CEOs and boards are witnessing how major breaches like those at Clorox, MGM, and Okta have materially impacted stock prices and bottom-line financial statements.

POST-BREACH FINANCIALS HIT HARDER

$100M MGM Resorts reported that its September 2023 breach caused a $100 million impact on EBITDAR[9]

$365M Clorox told investors it experienced a 20% decline in net sales—$365 million in losses—following its October 2023 breach[10]

11.5% Okta shares fell 11.5% on the news of its October 2023 breach [11]

They're paying closer attention than ever when the CISO speaks, and asking for higher levels of accountability as security teams deliver their board reports. At the same time, regulators are turning up the heat with new directives from the US Securities and Exchange Commission, NIS2, and the European Union Digital Operational Resilience Act (DORA) that are slashing the time that organizations have to report these breaches, bolstering requirements for cyber risk protection and planning, holding management accountable for security maturity, and increasing financial penalties for non-compliance.

These tightening conditions pose unprecedented professional and even personal ramifications for CISOs today. Not only are security leaders' jobs on the line with the slightest misstep, but they may even be held personally culpable in some circumstances. In 2023, two landmark court cases held CISOs legally culpable for their failures in the wake of huge data breaches:

- The former CISO of Uber was sentenced to serve three year's probation and to pay a $50,000 fine in connection with how he handled a 2014 breach[12]
- The SEC brought charges against the CISO for SolarWinds for allegedly misleading investors about the risks that I ed to the massive supply chain breach disclosed by the company in 2020[13]

Clearly, CISOs can't afford to stay stuck in the security status quo. They need to improve their risk management practices across the board in order to meet these challenges head-on.

[9] https://www.secureworld.io/industry-news/breach-mgm-resorts-hotel-access

[10] https://www.industryweek.com/technology-and-iiot/article/21274431/updated-clorox-cyberattack-cost-356-million

[10] https://www.cnbc.com/2023/10/20/okta-shares-fall-after-company-says-client-fles-were-accessed-by-hackers-via-its-support-system.html#:~:text=Shares%20of%20cybersecurity%20frm%20Okta,system%20using%20a%20stolen%20credential.

[12] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data

[13] https://www.sec.gov/news/press-release/2023-227

03

Enter Exposure Management

03 Enter Exposure Management

Moving From Protector to Risk Leader

Leading CISOs can turn crisis into opportunity if they can change their role and their mindset. They need to move from being protectors to risk leaders.

Whereas protectors operate with a mindset geared toward protecting everything at all costs, risk leaders manage risks and make good, fiscally responsible decisions about what, when, and where to put the most important defenses and controls. Risk leaders take a big-picture approach—rather than just triaging isolated incidents within assets, they're seeking to minimize losses across an organization's entire digital footprint.

Ultimately, the shift from protector to risk leader will position CISOs as growth enablers for the organization rather than business gatekeepers—and strengthen the risk posture of their enterprises in the process.

But to get there, CISOs need the infrastructure in place to gain a crucial element of support to help them guide the business in making sound risk decisions. That element is effective visibility—driven by exposure management technology and practices.

PROTECTOR		RISK LEADER
Protect everything	>	Manage risk; make good decisions
Incident triage of your assets	>	Minimize loss for the entire digital footprint
Business gatekeeper	>	Growth enabler

Tackling the Security Visibility Problem

Many security leaders today struggle to understand where the biggest security gaps lay in their existing controls because of a fundamental visibility problem. According to a report by ESG, the majority of organizations—76%— admit that they've experienced at least one cyber incident due to the exploitation of one or more unknown, unmanaged, or poorly managed internet-facing assets. Approximately 37% say that these kinds of blind spots have been the source of breaches numerous times.

> "Unfortunately, this pattern will likely persist as most organizations continue to approach security hygiene and posture management with point tools, spreadsheets, and manual processes."
>
> **Writes Jon Oltsik**
>
> *Distinguished analyst and ESG Fellow*[14]

When CISOs don't have continuous, automated means to validate and manage their security exposure levels across an enterprise, they lack the means to:

- Understand where industry-wide zero-day incidents impact their internal assets and supply chain
- Identify unknown assets, whether sanctioned business-led assets or shadow IT assets
- Gain a picture of risk across distributed cloud environments
- Gauge the risk posed by third-party vendors
- Understand where zero-day impacts hit their supply chain

76%
of orgs have experienced at least one cyber incident due to exploitation of unknown or unmanaged assets

[14] https://www.techtarget.com/esg-global/research-report/research-report-security-hygiene-and-posture-management-remains-decentralized-and-complex/

For many enterprises the issue is not that security teams lack monitoring or scanning capabilities. The problem is that those capabilities are often fractured and uncontextualized. One recent study estimated that almost a third of CISO time is spent sifting through 20 or more dashboards at a time to piece together a view of their exposure risk.[15]

Security teams are typically awash in vulnerability discoveries, but lack contextual information about the business domain in which flawed assets operate or the importance of the asset to the business. Further complicating matters is that even amid the firehose of monitoring data, there are blind spots and CISOs are rarely fully confident they understand the full scope of their assets or the risks posed by them.

This scattershot of unfiltered, raw data makes it very difficult for CISOs to take meaningful action and it stymies them in quickly updating the board, regulators, or insurers who want lightning-fast answers about the real risk of their exposures as security incidents unfold.

CISOs not only need to be able to more reliably discover assets and exposures across the enterprise, but they need a way to loop in business context and other risk cues to those views. Some exposures are more risky than others depending on the kind of asset, the nature of the exposure, and the importance of the asset to business processes or regulatory compliance.

Exposure management platforms—often referred to synonymously as attack surface management tooling—provide the visibility that CISOs need to scope risk across their entire attack surface. When well-deployed, these tools not only discover but also provide contextual information about potential exposures in internal and external assets, including previously unknown SaaS, cloud, and third-party assets.

4 days

New SEC reporting requires organizations report material cybersecurity incidents within 4 days

[15] https://team8.vc/wp-content/uploads/2023/09/2023-CISO-Summit-Security-Survey.pdf

Exposure Management 101

Exposure management provides a consolidated and contextualized view of risk from cyber exposures across an entire organization's digital ecosystem. The idea is an evolution of vulnerability management tooling, which does some level of discovery but is typically fixed on the technical details around bugs within scanned applications.

Exposure management visibility provides more continuous, less isolated, and more prioritized information about risks across an organization's extended asset portfolio—in the most advanced platforms that includes visibility into exposures within connected third-party assets.

> "Continuous threat exposure management is a pragmatic and effective systemic approach to continuously refine priorities and walk the tightrope between two modern security realities. Organizations can't fix everything, nor can they be completely sure what vulnerability remediation they can safely postpone."
>
> **Jeremy D'Hoinne**
> *Gartner VP analyst* [16]

EXPOSURE: SO MUCH MORE THAN CVES

The contextual information that exposure management can layer into a CISO's line of sight expands visibility far beyond traditional CVE information. The mix of data includes:

- Third-party risk
- Cloud misconfigurations
- Exposed credentials
- Social media risk
- Physical/safety issues from critical systems
- Geographical risk

[16] https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

Wading Through Exposure Management Alphabet Soup

As a rapidly evolving practice area for security teams, exposure management still lacks a unified or standardized market definition. This is a function of the fact that it's an area of product consolidation on a number of fronts—security vendors in some niches are bleeding over into others with varying degrees of overlap.

The following alphabet soup of analyst-defined acronyms all fall within the general banner of 'exposure management':

- Attack Surface Management (ASM)
- External Attack Surface Management (EASM)
- Continuous Attack Surface Management (CASM)
- Continuous Threat Exposure Management (CTEM)

Each acronym has a different flavor of meaning and the various vendors who have waded into the exposure management market take a range of different approaches. But the overarching theme that stretches across all of the acronyms is risk prioritization and measurement.

Forrester analysts offer one of the most concise summations of what all these various categories are trying to do, explaining that exposure management "consolidates vulnerabilities and exposures with an organizational perspective, maps them on an attack path, and identifies choke points for remediation teams to prioritize."

The Difference Between Exposure Management and Cyber Risk Metrics

As leading CISOs start to leverage exposure management to shift from the role of protector to a true risk leader, they're increasingly exploring the relationship between exposure, security performance, and cyber risk:

- Exposure management data provides real-time telemetry to security teams
- Performance data is a summarized view of exposure data over time
- Cyber risk metrics (such as security ratings and red, yellow, green dashboards for boards/CEOS) are a simplified type of performance data

Risk management reporting to the board is the story and analysis around that performance data that a CISO provides to business leadership. When well packaged, the narrative helps the business make better decisions and keeps the CISO accountable for improvements and declines over time.

So, exposure management feeds directly into cyber risk metrics, and it can be an important component for reporting to the board. Even though many boards will never see data directly from exposure management tooling, CISOs have a feed of continuous data from which they can "show their work" if directors want to understand the methodology that goes into ratings and performance data.

With the backing of a provable methodology provided by exposure management monitoring, security leaders can start to provide consistent internal benchmarks and comparisons that can offer CEO and boards of directors performance data by:

- Region
- Business group
- Network segments
- Asset or application groups

If CISOs can leverage exposure management and security performance management tooling that also adds in the power of external benchmarking data—offering comparative data and data about how they stack up to their industry, direct competitors, or high-performing companies—then directors can also understand how their actions compare to others.

04

Getting the Most Out of Exposure Management

04 Getting the Most Out of Exposure Management

10 Ways CISOs Can Use Exposure Management to Enhance Security Activities

Many security leaders today struggle to understand where the biggest security gaps lay in their existing controls because of a fundamental visibility problem. According to a report by ESG, the majority of organizations—76%—admit that they've experienced at least one cyber incident due to the exploitation of one or more unknown, unmanaged, or poorly managed internet-facing assets. Approximately 37% say that these kinds of blind spots have been the source of breaches numerous times.

1. **Asset Discovery:** Discovers unknown assets brought in through business-led digital investments; identifies shadow IT
2. **Vulnerability Management:** Works in concert with internal vulnerability management programs, adding continuous visibility into flaws and better prioritization of remediation recommendations
3. **SOC Operations:** Encourages proactive remediation of risky exposures, rather than reactive response to threats that have already unfolded
4. **Threat Hunting:** Offers data for experienced threat hunters to start making hypothesis for potential hidden attacks and seeking out relevant IOCs
5. **Incident Response:** Helps responders quickly understand if they're impacted by industry-wide zero-days
6. **AppSec:** Tracks important appsec/DevSecOps improvements over time
7. **Third-party Risk Management:** Offers visibility into exposures across the IT supply chain
8. **Risk Assessments:** Provides important details in comprehensive risk assessments
9. **Board Reporting:** Feeds and informs risk reporting to board with data based on demonstrable methodology; this can ideally be tied to financial quantification of risk
10. **Security Roadmapping:** Identifies controls gaps to help leaders prioritize and stage security investments based on where the biggest risks lie

What Exposure Management Gives CISOs

When done right, exposure management provides CISOs insight to lead both proactive and reactive tactical action. It can serve to prioritize proactive remediation of exposures found on the daily based on risk levels. And it can help security practitioners triage when incidents are going down.

3x less likely

By 2026, organizations that prioritize their security investments based on a continuous exposure management program will be 3x less likely to suffer a breach. [17]

However, it also brings a ton of strategic value to CISOs and business stakeholders. The big-picture view of exposure management visibility stands to drive strategic planning of security roadmaps and provide data-backed, real-time updates to the board and regulators as to the status of an organization's risk posture.

[14] https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

Ultimately, exposure management can help CISOs both manage up and manage down:

Managing Up: Exposure management adds maturity and data-backed rigor to board-level discussions. It provides CISOs the confidence they're using a sound methodology for validating performance and exposure information to the board.

Managing Down: Exposure management helps CISOs hold security teams accountable to measurable KPIs that are tracked in real-time. The data drives risk-based action and remediation—and it provides a way to compare performance at the individual contributor and team level.

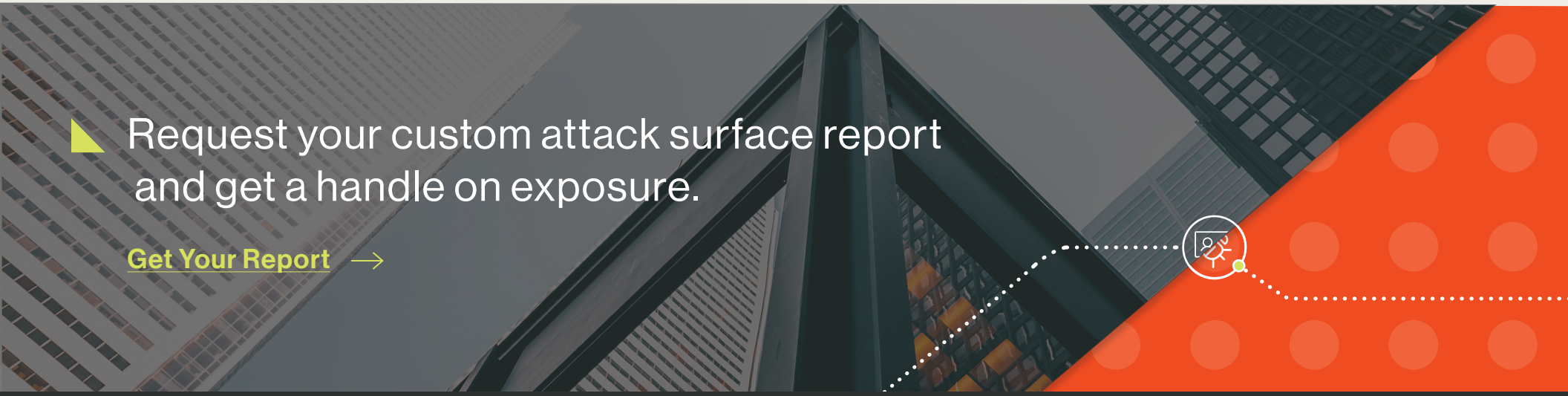
Finally, the compliance advantages are also clear. Exposure management speeds up reporting to regulators and helps CISOs meet even the most stringent demands from the SEC, internal auditors tracking to security frameworks, and insurance underwriters and adjusters who will seek out detailed information when writing and paying out on policies.

How Bitsight Powers Exposure Management

Bitsight invented the security ratings industry in 2011, and in the process of refining its ratings platform the company created a methodology for examining exposure that was essentially a frontrunner for exposure management visibility. The truth is that Bitsight has been enabling customers to manage their external attack surface and reduce exposures since the earliest iterations of the Bitsight platform. Today, Bitsight's research team constantly collects data from over 120 threat sources to power its exposure management tooling.

Bitsight's Security Performance Management platform performs automated and continuous asset and vulnerability discovery across a range of endpoints, servers, cloud instances, certificates, IoT devices, operational technology (OT) assets, and mobile apps. It's also on the hunt for other active threats and exposures that includes compromised assets, botnets, domain squatting, compromised credentials, misconfigurations, and dark web activity around assets.

One of the big differentiators Bitsight offers over competitors in the exposure management market is its Third-Party RiskManagement offering, which extends exposure visibility out across the IT supply chain. That's one of the reasons why KuppingerCole rates Bitsight as an Overall Leader, Product Leader, and Market Leader in the 2023 Leadership Compass for Attack Surface Management report.



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

BITSIGHT