HUNTER X

PLAYBOOK

HUNTERX RISK REPORT

Sales & Prospecting Playbook

Table of Contents

liongard

1. Purpose of This Playbook

This playbook is designed to help Sales teams use the HunterX Risk Report as a prospecting and deal-acceleration tool.

HunterX is marketed first and foremost as a sales-led risk intelligence platform. In this motion, the Risk Report is used to:

- Open doors with credible, data-backed insight
- Create urgency through context and comparison, not fear
- Shift conversations from tools to business risk and impact
- Justify why security services matter *before* discussing solutions
- Accelerate deals by aligning stakeholders early

Key Principle

The Risk Report is not a technical assessment. It is a conversation catalyst that frames risk in a way executives understand and act on.

2. When Sales Should Use the Risk Report

1 Primary Sales Use Cases

Sales teams should use the Risk Report:

- To prioritize and engage prospects whose external risk profile suggests higher likelihood of meaningful security need
- During initial prospect outreach
- As a centerpiece in first or second discovery meetings
- To support multi-stakeholder conversations (IT, exec, finance)
- When differentiating from competitors during active evaluations

2 Ideal Prospect Profiles

The Risk Report is especially effective for:

- Prospects with cyber insurance requirements
- Regulated or data-sensitive industries
- Mid-market organizations where execs influence security decisions
- Prospects struggling to justify security spend internally

3. What the Risk Report Is

1 What It Shows

The HunterX Risk Report provides:

- A probability-based view of cyber incident likelihood
- Benchmark comparisons against:
  - Peer organizations
  - Breached companies
  - Organizations with stronger security maturity patterns
- Modeled financial impact of potential cyber incidents
- Common attack patterns and data exposure trends by industry

Key Principle

This allows you to lead with risk context and business impact, not features or vulnerabilities.

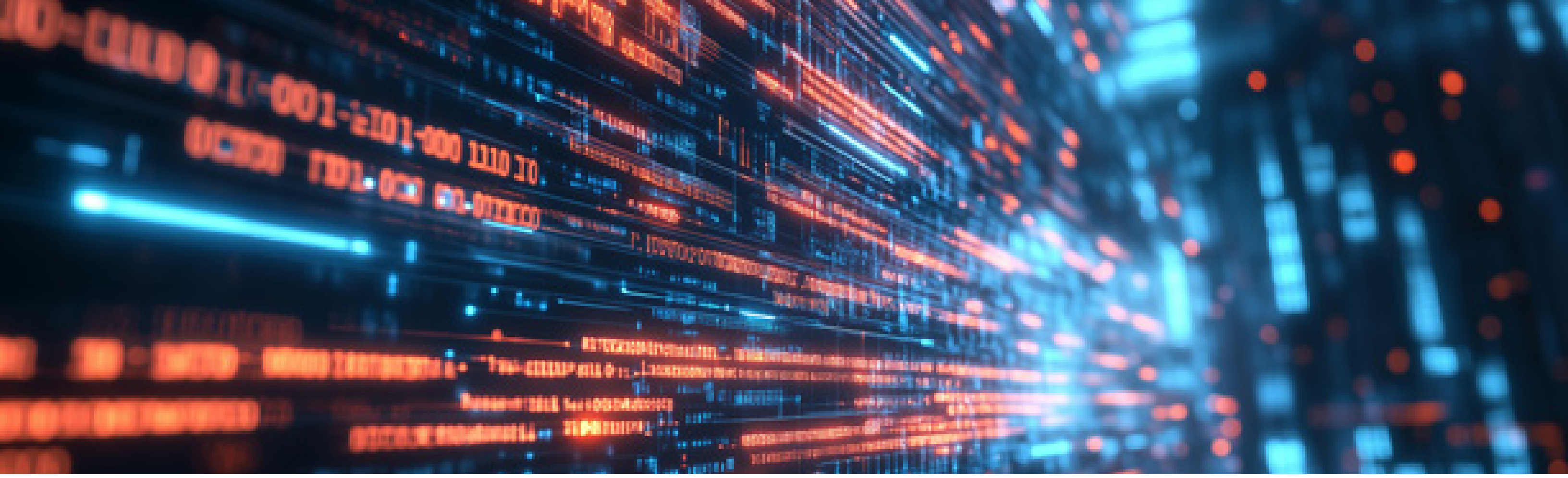
2 What It Does *Not* Do

To set expectations correctly, be clear that the report:

- Is not a vulnerability scan
- Does not inspect internal tools or configurations
- Does not prescribe remediation steps
- Does not guarantee risk score reduction

Sales framing:

> “This gives us an external, industry-benchmarked view of cyber risk and business impact. It helps frame why security matters before we talk about how to address it.”



4. Using the Risk Report in a Sales Conversation

1 Recommended Meeting Flow

1. Context Setting

> “Here’s how organizations like you typically compare.”

2. Relative Risk

> Peer and breach comparisons.

3. Business Impact

> Financial exposure and loss modeling.

4. Industry Reality

> Common attack paths and outcomes.

5. Transition to Solutions Setting

> “Given this context, let’s talk about how organizations address this risk.”

The goal is alignment, not alarm.

5. How the Risk Factors Should Be Explained

1 SignetScore & Risk Categories

How to use it:

- Treat them as a directional benchmark, not a grade
- Focus on relative position, not the number itself
- Use comparisons to spark conversation

What to say:

> “Risk factors help us understand how your organization compares to others like you. It’s a benchmark for context, not a target to optimize.”

2 Important Context for Sales

Higher risk factors often reflect:

- Risk concentration in widely used platforms or services
- Industry-wide exposure patterns
- Historical incident similarities

The score and risk categories represent an organization’s relative risk position compared to others in their industry. A lower score does not mean tools are bad or decisions were wrong, it highlights where risk may be more concentrated and impactful.

This is not a score that can be “improved.”
It is a reflection of how risk is distributed based on external factors, industry patterns, and exposure, not something a service provider can raise or lower through services.

Sales should be clear:

- We are not trying to improve or optimize the score
- We are not selling services to change the rating

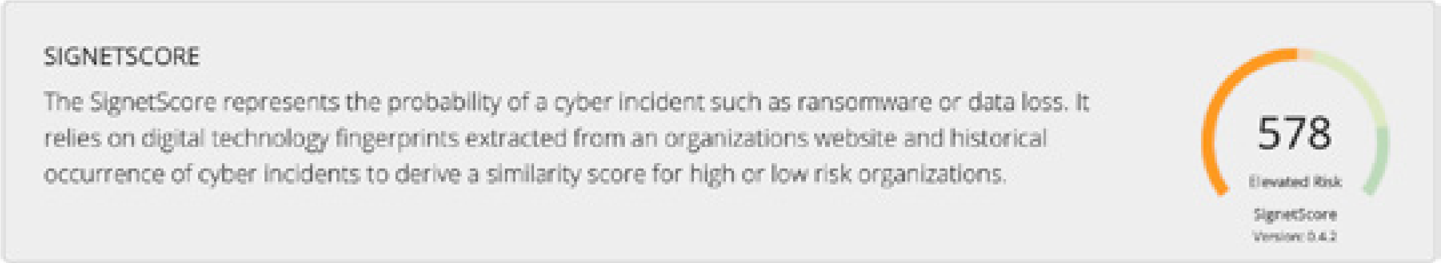
Instead, the role of the Service Provider is to:

- Help the organization protect itself appropriately given its relative risk position
- Put controls, services, and safeguards in place that reduce disruption and business impact
- Ensure the business is prepared to withstand and recover from incidents that are more likely given that position

4. How Sales Should Read The Risk Report

Sales effectiveness with HunterX depends on guiding the conversation, not explaining every chart. The goal is to control the narrative, anchor urgency in context, and transition naturally to solutions.

1 SignetScore & Risk Category



SIGNETSCORE

The SignetScore represents the probability of a cyber incident such as ransomware or data loss. It relies on digital technology fingerprints extracted from an organizations website and historical occurrence of cyber incidents to derive a similarity score for high or low risk organizations.

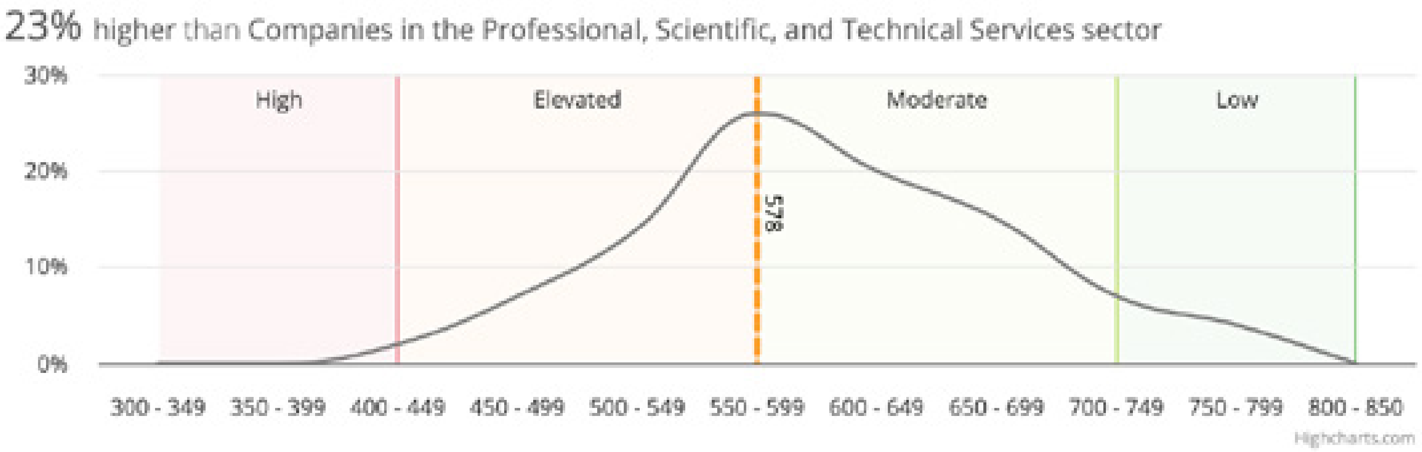
How to use it:

- Establish relative risk position early
- Focus on how the prospect compares to peers and breached organizations
- Avoid treating the score as a pass/fail metric

Sales talk track:

"Much like a credit score, this provides relative context rather than a pass/fail result. It helps frame where you sit compared to similar organizations and informs planning discussions."

2 Peer & Industry Comparisons



23% higher than Companies in the Professional, Scientific, and Technical Services sector

How to use it:

- Create immediate relevance through comparison
- Highlight meaningful gaps or strengths versus peers
- Reinforce that risk is relative, not theoretical

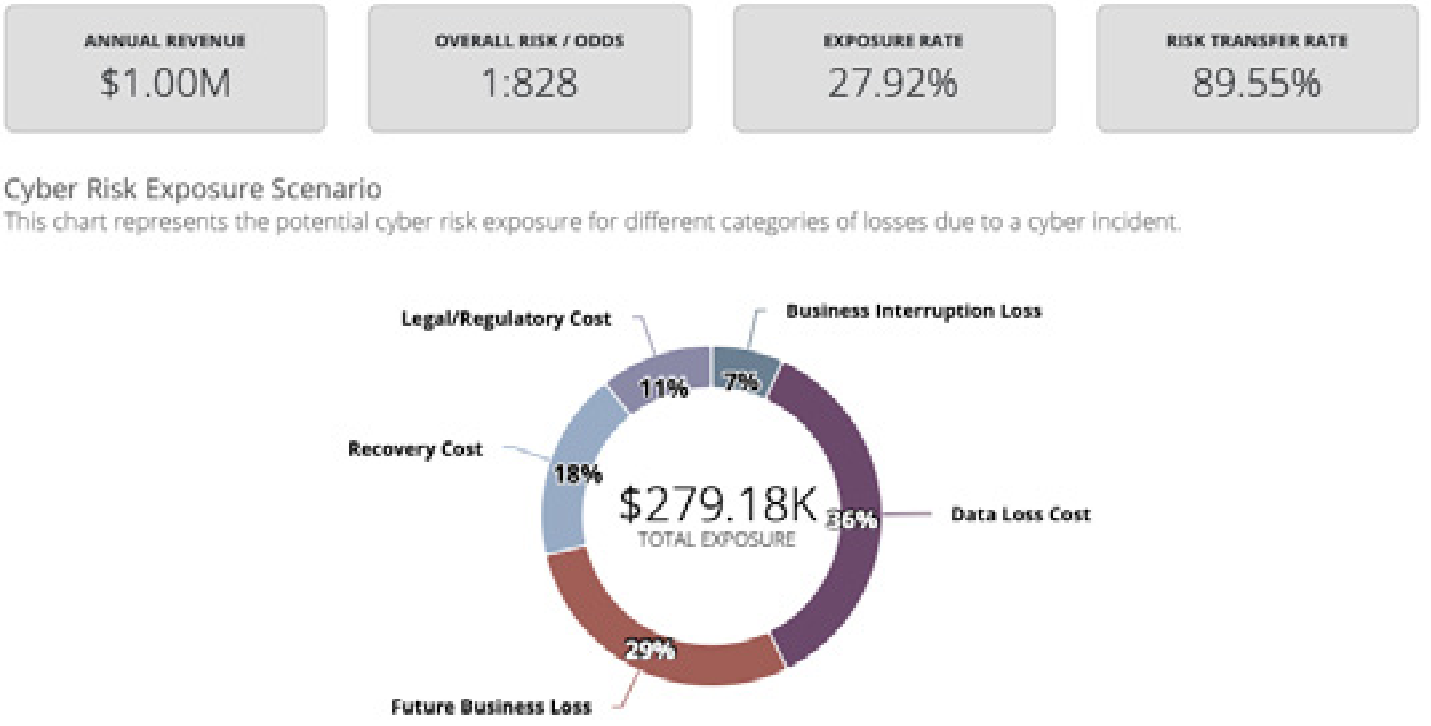
Why it matters:

- Comparisons help prospects quickly understand why the conversation matters without relying on technical detail.

Sales talk track:

“These comparisons show how your organization aligns with peers and with companies that have experienced real-world incidents. It gives us a grounded way to talk about risk without getting lost in technical detail.”

3 Cyber Risk Quantification



ANNUAL REVENUE	OVERALL RISK / ODDS	EXPOSURE RATE	RISK TRANSFER RATE
$1.00M	1:828	27.92%	89.55%

Cyber Risk Exposure Scenario

This chart represents the potential cyber risk exposure for different categories of losses due to a cyber incident.

What This Section Is

This section translates cyber risk into financial and operational impact, making it one of the most important parts of the Risk Report for net-new sales conversations.

It directly connects cyber risk to business cost and return on investment, helping prospects understand what downtime, disruption, and recovery realistically cost, and why investing in MSP services delivers measurable value before an incident occurs.

This section exists to frame ROI in terms of cost avoided, downtime reduced, and recovery accelerated.

How to use it:

- Translate cyber risk into business costs prospects care about (downtime, lost productivity, operational disruption)
- Frame ROI as the difference between reacting to incidents and proactively reducing impact
- Justify investment in MSP services by tying them to continuity, resilience, and faster recovery
- Support prioritization by showing where disruption would hurt the business most

Why it matters:

- Net-new buyers need a business justification, not a security explanation
- This section shows how cyber risk turns into real financial loss when services aren't in place
- It positions MSP services as an investment that protects revenue and operations, not discretionary spend
- It provides a clear ROI narrative based on impact reduction, not feature comparison

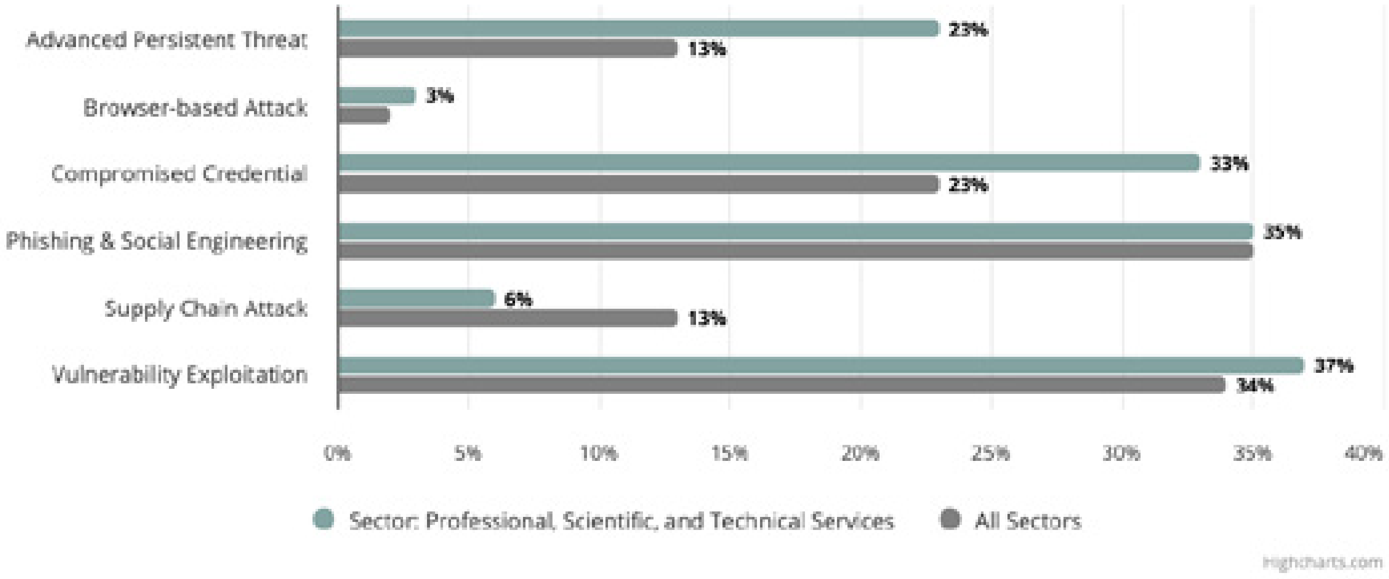
Sales talk track:

"This is one of the most important sections of the report because it connects cyber risk directly to business impact. It shows what downtime and disruption typically cost organizations like yours, and why investing in services that reduce that impact delivers real return."

4 Industry Attack & Data Trends

Attack Vector

The chart below shows the relative frequency with which specific attack vectors were successfully deployed against targets in a given industry. This can be useful in helping a company understand potential attack vectors and to prioritize remediation actions if necessary.



How to use it:

- Normalize the conversation ("this is common in your sector")
- Show where attackers typically succeed
- Set up logical areas where organizations invest to reduce impact

Sales reminder:

Use this section to guide solution discussions based on real-world attack patterns, not to overwhelm prospects with data.

Sales talk track:

"This just shows what's common in your industry. It helps focus the conversation on where organizations typically invest to reduce impact."

liongard

7. Handling Common Sales Objections

“This looks scary.”

> “The goal isn’t to scare anyone. It’s to put risk in context so decisions are informed, not reactive.”

“Does this mean something is wrong?”

> “No. This reflects probability and industry patterns, not a finding or failure.”

“Will this score go down if we buy something?”

> “The score isn’t designed to be optimized. It’s designed to frame risk so the right decisions can be made.”

8. Mapping Risk to Solutions

Sales should avoid jumping straight to tools.

Instead, transition by aligning risk themes to service categories, such as:

- Business interruption risk → Resilience & continuity services
- Credential-based attacks → Identity and email security
- Ransomware exposure → Backup, recovery, and response planning
- Regulatory exposure → Compliance and governance services

Key Rule

Position solutions as responses to risk patterns, not fixes for the score.

9. Connecting Risk Areas to MSP Services

Use this as a guide to translate risk signals in the report into relevant service conversations. The goal is not to map every risk to every service. Focus on the most material risks and connect them to services that reduce business impact.

1 Elevated Business Impact / Downtime Risk

What the report highlights:

- High financial impact from disruption
- Significant downtime or recovery cost exposure

Sales framing:

"These services are designed to limit downtime and help the business recover faster when incidents occur."

2 Credential-Based Attacks & Identity Exposure

What the report highlights:

- Common use of stolen credentials
- Account takeover trends in the industry

Relevant MSP services to discuss:

- Identity protection and access controls
- Email security and phishing protection
- User awareness and training programs
- Monitoring for suspicious authentication activity

Sales framing:

"These services help reduce the likelihood and impact of credential-driven incidents, which are one of the most common entry points we see."

3 Ransomware & Operational Disruption

What the report highlights:

- Ransomware prevalence in the sector
- High operational and recovery impact

Relevant MSP services to discuss:

- Ransomware preparedness and response
- Endpoint protection and monitoring
- Recovery testing and response planning
- Security operations and alerting support

Sales talk track:

"The focus here isn't just prevention, it's reducing disruption and accelerating recovery if an incident occurs."

4 External Exposure & Attack Surface

What the report highlights:

- Exposed services or internet-facing assets
- Increased likelihood of external exploitation

Relevant MSP services to discuss:

- External attack surface monitoring
- Patch and vulnerability management
- Infrastructure hardening and configuration support
- Ongoing security monitoring

Sales framing:

"These services help reduce exposure and identify issues before they turn into incidents."

5 Regulatory or Compliance-Driven Risk

What the report highlights:

- Industry-specific regulatory pressure
- Higher consequences for incidents

Relevant MSP services to discuss:

- Compliance support and reporting
- Security governance and documentation
- Risk assessment and advisory services
- Ongoing compliance monitoring

Sales framing:

"These services help reduce both operational and regulatory impact when incidents occur."

6 Limited Internal Security Resources

What the report highlights:

- Higher impact due to delayed response
- Gaps in monitoring or response capability

Relevant MSP services to discuss:

- Managed detection and response (MDR)
- 24/7 monitoring and alerting
- Incident response coordination
- Security operations support

Sales talk track:

“These services are designed to fill response gaps and reduce the time it takes to contain incidents.”

9. Prospect Email Templates

The initial email earns the meeting by providing context.

The follow-up email reinforces how MSP services reduce business impact.

1 Cold Prospect Outreach Email

Purpose: Spark interest, establish credibility, and earn the meeting.

When to use: Outbound prospecting where the Risk Report is attached or linked.

Subject: A quick external risk snapshot for {{Company Name}}

Hi {{First Name}},

We recently ran an external, industry-benchmarked cyber risk review on {{Company Name}} as part of our work with organizations in your sector.

This report looks at how organizations like yours typically compare from an external risk perspective, and what that level of risk could mean in terms of business impact.

Many teams use this as a starting point to sanity-check whether their current security approach and protections align with the realities organizations in their industry face today.

If it's helpful, I'd be glad to walk through the highlights and share how similar organizations think about reducing disruption and downtime given their risk position.

Best,
{{Sender Name}}

Why this email works

- No fear language
- No "we found issues"
- Positions the report as context, not judgment
- Opens the door to a services conversation, not a pitch

2 Post–Sales Call Follow-Up Email

Purpose: Reinforce value, anchor services to business impact, move toward next steps.

When to use: After a discovery or first sales call where the Risk Report was discussed.

Hi {{First Name}},

Thanks again for the conversation today. I appreciated the discussion around how organizations in your space are thinking about cyber risk and business continuity.

As we reviewed, the Risk Report provides context around where {{Company Name}} sits relative to peers and common industry attack patterns. This gives us a way to understand where risk tends to be more concentrated and what that could mean operationally.

Based on that context, our next step would be to look at how our services help organizations reduce downtime, limit disruption, and recover more effectively when incidents occur, particularly in the areas we discussed.

Let me know if it makes sense to continue that conversation, and I'm happy to align on priorities and timing.

Best,
{{Sender Name}}

Why this email works

- Reinforces correct score interpretation
- Connects risk → business outcomes
- Clearly transitions to services
- Feels consultative, not transactional

10. Sales Success Indicators

A successful HunterX-led sales conversation results in:

- Prospects understanding their relative risk position
- Security framed as a business decision, not an IT problem
- Clear justification for security investment
- Faster movement to next steps
- Multi-stakeholder engagement

HunterX Works because it:

- Leads with intelligence, not features
- Uses comparison instead of fear
- Makes risk tangible for executives
- Creates urgency without pressure

Activate HunterX
Win the trust first. The deal follows.

About Liongard

Liongard is redefining asset intelligence with its AI-powered platform built for modern IT and security operations. Trusted by organizations worldwide to protect complex environments, Liongard delivers unified, real-time visibility across users, systems, networks, and SaaS Applications. Liongard empowers teams to uncover hidden risks, enforce controls, and automate critical security outcomes. By combining deep asset intelligence with AI-driven insights and scalable remediation, Liongard helps organizations reduce risk, strengthen cyber resilience, and operate more efficiently.

For more information, visit www.liongard.com

liongard™