LockThreat

The Enterprise GRC Buyer's Guide

How to Evaluate, Select, and Implement the Right Platform

A practical guide for security and risk leaders who are ready to buy, not just browse.

YOU'RE READY TO BUY

You Know What You Need. Now You Need to Buy It.

If you have read our companion guide, ***"Enterprise GRC Platform or Compliance Tool? How to Tell the Difference,"*** you already know what to look for in a GRC platform. You understand the gap between a compliance tool and an enterprise GRC platform. You have the evaluation criteria and the vendor questions.

This guide picks up where that one left off.

Knowing what good looks like is only half the challenge. The other half is running the buying process without getting lost in it. Enterprise GRC purchases are expensive, political, and easy to get wrong. The wrong process leads to the wrong choice, even when the right option is sitting on your shortlist.

This guide covers the six things that many GRC buying guides skip: **how to align your internal team, how to define what you actually need, how to run the evaluation, how to calculate the real cost, how to plan the implementation,** and **how to avoid the mistakes that derail the whole project.**

You can use this guide on its own or together with its companion. Either way, the goal is the same: **help you buy well.**

Read first

Haven't read the companion guide yet?

Download "Enterprise GRC Platform or Compliance Tool? How to Tell the Difference" for detailed evaluation criteria and vendor questions.

www.lockthreat.ai/resources/ebooks →

YOUR STARTING POINT

Which Type of GRC Buyer Are You?

Not all GRC buyers start from the same place. The challenges you face, and the questions that matter most to you, depend on where you are in your journey.

01

First-time Buyers

Are replacing manual processes: spreadsheets, email workflows, shared drives, and point tools that no longer scale. The primary challenge is building a compelling internal case for change and making sure the organization is ready to adopt something new.

02

Replacement Buyers

Are moving off an existing GRC platform, one that failed to deliver, was abandoned by most users, or no longer fits the organization's needs. The primary challenge is honestly diagnosing what went wrong before, so the same mistakes are not repeated with a new vendor.

03

Consolidation Buyers

Are rationalizing multiple tools: different teams using different platforms, frameworks managed separately, and no unified view of the organization's risk posture. The primary challenge is reconciling diverse stakeholder requirements and managing the complexity of what already exists.

All three profiles will find this guide useful from cover to cover. Depending on which profile fits you, certain chapters will feel especially relevant to your specific situation. Read the whole guide and see which parts are relevant to your buyer profile.

CHAPTER 01

Before You Start, Get Your Team Aligned

The number one reason enterprise GRC purchases stall is not budget. It is internal misalignment. Different stakeholders want different things from the same platform; often, nobody finds out until the evaluation is already underway.

Eight Stakeholders. Eight Different Priorities

Here is what happens in most organizations:

- The Chief Information Security Officer wants cyber GRC and continuous control monitoring.
- The Chief Risk Officer wants enterprise-wide risk visibility and board reporting.
- The compliance leader wants audit automation and framework mapping.
- Legal wants policy traceability, regulatory change management, and confidence that the platform can defend the organization's decisions under scrutiny.
- Internal audit wants independent access to controls, evidence, and testing results with clear separation from the first line.
- The Chief Financial Officer wants lower total cost than the current setup.
- IT wants something that fits the existing technology stack without a six-month integration project.
- The Chief AI Officer or CTO wants AI deployments governed, auditable, and compliant, without slowing innovation.

All of these are reasonable. None of them are wrong. **But if you start evaluating vendors before you agree on priorities, every demo becomes a debate.** One stakeholder loves the vendor because it solves their problem. Another one hates it because it does not solve theirs.

What to do before you talk to any vendor

Get the key stakeholders in one room (or one call) and answer three questions together.

1

Who will use this platform day to day, and what do they need it to do?

Not what would be nice to have. What do they actually need to do their jobs?

2

What are the non-negotiable requirements?

These are the things that will eliminate a vendor immediately if they cannot do them. Examples: multi-entity support, on-premises deployment, AI governance capabilities, specific framework coverage.

3

What does success look like in 12 months?

If you buy this platform and implement it, what should be different one year from now? Write it down. If people cannot agree on the answer, you are not ready to buy yet.

Six Questions Your Buying Committee Should Be Able to Answer Before Talking to Any Vendor

01 Can you define the business problem you are solving in two sentences, naming who owns it and what measurable success looks like?

02 If your organization has used a GRC tool before, have you fully diagnosed why it did not deliver, not just acknowledged that it did not?

03 Do you have a named executive sponsor who will stay actively involved through implementation, not just someone who approved the budget and moved on?

04 Do you have dedicated people assigned to this project, team members whose primary responsibility this will be, rather than people who will fit it in around existing full-time roles?

05 Are you prepared to redesign processes and accountability structures as part of this implementation, or are you expecting the technology to solve what may be organizational problems?

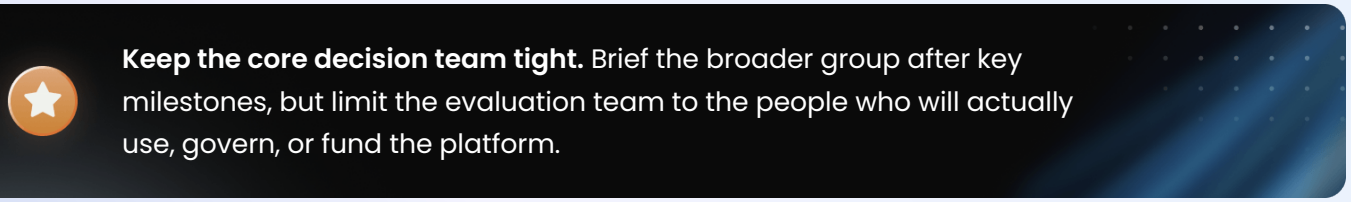
06 Can you define success in business outcomes that your leadership will still care about at contract renewal time, not just deployment milestones?

These are not evaluation questions. They are readiness questions. If the answer to any of these is "not yet," resolve it before your first vendor conversation.

Who should be in the room

At minimum, you need the CISO or head of security, the CRO or head of risk (if your organization has one), the senior compliance leader, the General Counsel or a senior legal representative, the head of internal audit, someone from IT or engineering who will own the technical integration, and someone with budget authority or a direct line to the CFO.

If AI governance is part of the requirement, you may also need the head of AI or the CTO.



CHAPTER 02

Define What You Actually Need

Many buyers skip this step. They go straight from “we need a GRC platform” to scheduling demos. Then they spend weeks watching demos without a clear way to compare what they saw.

Before you talk to any vendor, get clear on your requirements. Not a 50-page RFP. A simple, honest list organized around six categories. Here is what each one covers and why it matters.

Scope & Coverage

Which departments, jurisdictions, and frameworks does the platform need to support? This is the category that separates enterprise platforms from departmental tools. If you only define scope around IT and cyber, you will end up with a compliance tool. Define scope around your entire organization and you will evaluate very differently.

Organizational Structure

How complex is your organization? Multi-entity, multi-business unit, and multi-jurisdiction support sounds like a checkbox on an RFP, but it is one of the hardest things for a platform to do well. If your organization operates across multiple entities or geographies, test this early. It is the requirement most likely to eliminate vendors from your shortlist.

Risk & Governance Depth

This is where you find out whether a platform delivers real governance and risk management or just compliance with a GRC label. Formal risk registers, risk quantification in financial terms, policy lifecycle management, and separation of lines of defense are the capabilities that distinguish a platform from a tool. If these are important to you, make them non-negotiable.

Operational Requirements

How will the platform connect to your existing infrastructure? Do you need continuous assurance (real-time control monitoring) or is periodic evidence collection sufficient? Do you have non-negotiable data residency requirements that mandate private VPC or on-premises deployment? Or no data residency concerns, so SaaS deployment is fine? The answers drive both the shortlist and the total cost.

People & Capacity

How many people will use the platform, and how skilled do they need to be? Some platforms require dedicated GRC specialists to operate. Others are built so that general practitioners across departments can use them. The difference affects not just usability but ongoing operating cost. Moreover, some platforms charge by seat, which penalizes adoption; other platforms charge a flat rate so you can expand usage at no additional cost. Major difference.

Timeline & Migration

When do you need to be live, and are you replacing an existing platform? If you are migrating from a legacy GRC platform or from a compliance tool, you need to know whether you can run both systems in parallel. Your timeline and migration plan will shape the entire evaluation.

We have included a printable Requirements Worksheet in the Appendix at the end of this guide. Fill it out with your buying committee before your first demo. It will keep every vendor conversation focused on what matters to your organization.

See the Appendix for the full Requirements Worksheet. Print it. Fill it out as a team. Bring it to every demo. It will keep every vendor conversation focused on what matters to your organization.

CHAPTER 03

Running the Evaluation

How to structure demos, POCs, and reference calls so you learn what matters.

You have your requirements. You have your shortlist. Now you need to evaluate the vendors without wasting weeks on demos that all look the same.

Structuring the Demo

Tell the vendor your requirements before the demo. Send them the worksheet from the Appendix. A good vendor will tailor the demo to your needs. A mediocre vendor will run their standard pitch regardless of what you sent them. That difference is itself a signal.

During the demo, watch for three things:

1. **Can they show your use cases, not just their best use cases?**
   If you need multi-entity risk aggregation and they only show single-entity compliance dashboards, that tells you something.

2. **Who is driving the demo?**
   If it is only a sales engineer and no one from the product team can answer your deeper questions, that tells you something too.

3. **How do they handle questions they cannot answer?**
   "That is on our roadmap" is not the same as "that is in production today."

Running a Proof of Concept

A demo shows you what the vendor wants you to see. A POC shows you what the platform actually does with your data, your frameworks, and your workflows.

If a vendor resists doing a POC, ask why. If the answer is that it takes too long to set up, that tells you something about implementation complexity. If the answer is that they only do POCs for committed buyers, that is reasonable, but make sure you understand the terms.

During the POC, test the hard things, not the easy things. Every platform can show you a dashboard. Test whether it can handle your multi-entity structure. Test whether the framework mapping actually works across the standards you need. Test whether the reporting gives your board what they asked for.

Reference Calls

Ask for references in your industry and at your scale. A reference from a 500-person SaaS company is not relevant if you are a 10,000-person regulated enterprise.

On the call, ask (at least) these three questions:

1. **Can they show your use cases, not just their best use cases?**
2. **How many people does it take to run the platform day to day?**
3. **Would you buy it again?**

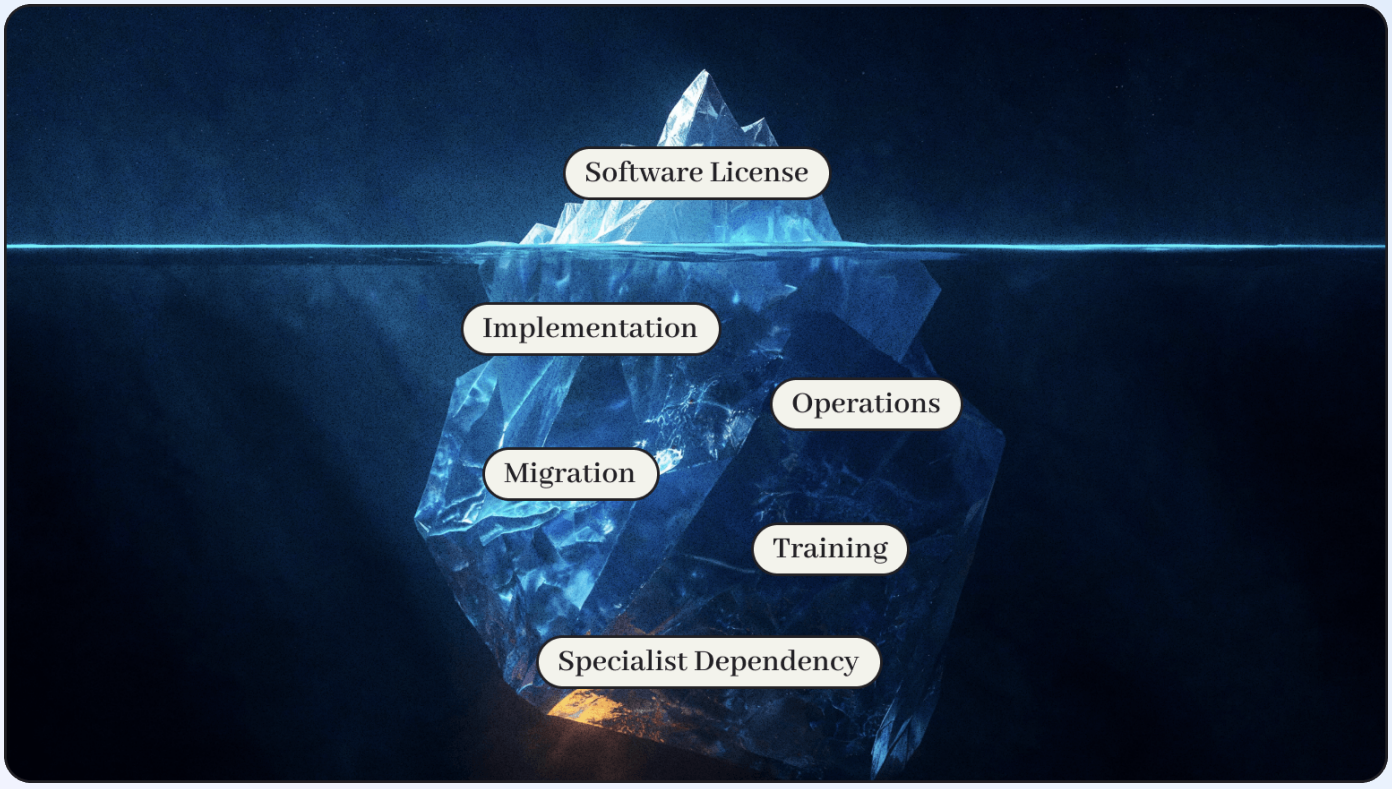
See the Appendix for the full Requirements Worksheet. Print it. Fill it out as a team. Bring it to every demo. It will keep every vendor conversation focused on what matters to your organization.

CHAPTER 04

The Real Cost of a GRC Platform

Software is just the starting line. Here is where the real money goes.

Every vendor will show you a software price. Very few will help you understand the total cost of ownership. **That is because the software license is often the smallest part of the bill.**



What you need to account for:

Software License

The annual or multi-year fee for the platform itself. Ask whether this is per-user, per-entity, per-module, or flat rate. Ask what happens to the price when you add entities, users, or frameworks. Ask whether AI capabilities, continuous assurance, and AI governance modules are included or priced separately. Remember that per-user pricing penalizes adoption, and per-module pricing penalizes the scope. Platforms priced on entity count or flat rate allow you to expand usage without renegotiating every quarter.

Implementation

How long does it take to go live? Who does the implementation work: your team, the vendor's team, or a third-party consulting firm? What does that cost? Implementation consulting in legacy platforms often runs $200K to $500K and takes 12 to 18 months before you see the first dashboard goes live. Modern platforms, with pre-built framework libraries, native integrations, and configurable workflows go live in weeks to a few months with the vendor's own team, not a third-party consulting firm. The difference in total cost and in time to value is enormous.

Ongoing Operations

How many people will you need to run the platform once it is live? If the system requires two or three dedicated specialists who are the only people who understand it, the salary cost of those specialists is part of your GRC platform cost. If the platform is built so that general practitioners can use it, that cost is lower.

Migration & Co-habitation

If you are replacing an existing platform, can you run both systems in parallel during the transition? Or do you need to rip and replace on day one? Running two systems has a cost. But a failed migration has a much bigger one.

Cost of Inaction

This is the number most buyers forget to calculate. What does it cost to stay on your current setup for another 12 to 24 months? More manual effort. More audit prep time. More spreadsheets. More gaps that surface at the wrong moment. Potentially more fines for incompliance. More tools you need to buy separately (AI governance, continuous monitoring, cyber compliance) because your current platform cannot do them. Add it up. That number is your baseline for comparison.

Build a simple TCO comparison: current state (including all the gaps and manual work) vs. new platform (including all implementation and operating costs). Present both numbers to the CFO. Let the math make the case.

CHAPTER 05

Implementation & Migration Reality

How to Pressure-Test Any Vendor's Implementation Claims.

Every GRC vendor will tell you implementation is fast and easy. The problem is that "fast" depends entirely on your complexity and what "live" actually means. **Don't compare timelines. Compare answers to these four questions.**

1	**What does 'live' mean in your timeline?**	Some vendors mean "the platform is turned on." Others mean "your frameworks are mapped, your controls are loaded, and your team is using it for real work." Make sure you agree on the definition before you compare.
2	**How much work falls on our team?**	A fast implementation that requires three of your people full-time for a month is not actually fast. It just shifted the effort to you. Get clarity on what the vendor does vs. what your team does.
3	**What is included, and what costs extra?**	Some vendors include implementation support in the license. Others charge separately for onboarding, configuration, migration, and training. A low license price with a $200K consulting fee is not a good deal.
4	**Can I speak with a customer in a similar industry or with similar complexity?**	Not a case study on the website. A real conversation with someone who implemented the platform in an environment similar to yours. Their experience will tell you more than any vendor slide deck.

If You Are Migrating from an Existing Platform

Can you run both systems in parallel? If yes, migration becomes a gradual transition instead of a risky cutover. If the vendor does not support co-habitation, ask why and ask what their alternative looks like. And ask for references from customers who migrated from the same platform you are currently on.

Implementation timelines are only meaningful when you agree on **what 'live' means, who does the work, and what is included in the price.**

CHAPTER 06

Ten Mistakes That Derail GRC Purchases

These are the patterns we see repeatedly. Every one of them is avoidable.

1 Evaluating features instead of outcomes.

Most GRC evaluations are organized around feature checklists. Does it support this framework? Does it have that dashboard? Does it integrate with this tool? These are reasonable questions, but they are the wrong starting point.

The right question is not "does it have this feature?" Rather, it is "will it reduce our SOC 2 audit prep from six weeks to two weeks, and can you show us evidence of that before we sign?"

Buyers who lead with features may select a platform that scores well in a demo and even passes a thorough vendor evaluation, but is never implemented in a way that produces measurable results. Nobody can say at renewal whether the investment worked.

Before evaluating any vendor, define the two or three business outcomes that will determine whether this purchase succeeded. Make those outcomes the first filter, not the last.

2 Buying for today's requirements only.

The GRC market is shifting fast. AI governance, continuous assurance, and cyber compliance are no longer future requirements. They are current ones. If the platform you choose today cannot handle these, you will be back in the market within 12 to 24 months buying additional tools or starting over.

3 Letting one department choose a tool the rest of the organization cannot use.

If the CISO picks a cyber compliance tool and calls it "our GRC platform," finance, legal, operations, and the rest of the organization are left out. You end up with a departmental tool, not an enterprise GRC platform. Refer back to Chapter 1: get alignment first.

4 Choosing a brand name instead of evaluating fit.

A well-known vendor is not automatically the right vendor for your organization. Some of the largest names in GRC have the lowest ease-of-implementation scores. Evaluate fit, not familiarity.

5 **Skipping the POC.**

A demo is a performance. A POC is a test. If you buy based only on demos, you are buying based on the vendor's best-case scenario, not your reality.

6 **Comparing initial license prices instead of total cost.**

Some pricing models punish you for growing. Per-user pricing penalizes adoption. Per-module pricing penalizes scope. Look for pricing that lets your program expand without triggering a new negotiation every quarter. Also remember that license cost is just part of the picture. Implementation support, consulting fees, training, specialist dependency, and the ongoing cost of operating the platform all add up. Compare total cost of ownership, not initial license cost.

7 **Ignoring deployment flexibility.**

If your organization operates in regulated industries or jurisdictions with data residency requirements, SaaS-only platforms may not be an option. Ask about private VPC and on-premises deployment before you fall in love with the demo.

8 **Signing a long contract before proving value.**

A three-year deal with upfront commitment may offer a discount, but it locks you in before you know whether the platform works for your organization. Negotiate a shorter initial term or build in exit clauses tied to implementation milestones.

9 **Buying a platform your team will not use.**

The most powerful platform fails if your team avoids logging in. Ask how many people at existing customers actually use it day to day, not just how many have licenses. If the interface looks like it was designed for specialists, it will stay with specialists.

10 **Assuming every vendor's 'AI' claim means AI governance.**

Almost every GRC vendor now puts "AI" on their website. This is not a future risk: the 2026 Verizon Data Breach Investigations Report found that shadow AI, meaning employees accessing AI tools outside corporate governance controls, was already the third most common insider threat action, up fourfold in a single year.

Most vendors who put "AI" on their website mean they use AI to speed up tasks like control mapping or policy drafting. That is not AI governance. AI governance means discovering shadow AI, protecting AI applications at runtime, governing agentic AI, and mapping controls to frameworks like the EU AI Act and NIST AI RMF. Ask the vendor to show you those capabilities specifically.

YOUR ACTION PLAN

Your Buying Checklist

Here is the short version of everything in this guide. **Use it to track your progress.**

- [ ] **Step 1:** Align your internal team on priorities and non-negotiables. — CH. 1
- [ ] **Step 2:** Fill out the requirements worksheet before your first demo. — CH. 2, Appendix
- [ ] **Step 3:** Structure demos around your use cases, not the vendor's. Run a POC. Check references. — CH. 3
- [ ] **Step 4:** Build a total cost picture that includes implementation, operations, and migration, not just the license. — CH. 4
- [ ] **Step 5:** Set realistic implementation expectations and plan for co-habitation if you are migrating. — CH. 5
- [ ] **Step 6:** Avoid the ten common mistakes. — CH. 6

Companion Guide

Want detailed evaluation criteria?

Download our companion guide for a 14-point comparison table and 15 vendor questions: "Enterprise GRC Platform or Compliance Tool? How to Tell the Difference."

www.lockthreat.ai/resources/ebooks →

GRC Requirements Worksheet

Print this worksheet and fill it out with your buying committee before your first vendor demo.

Section 1 – Scope & Coverage

- [ ] How many departments will use the platform? (list them)
- [ ] Which geographic jurisdictions does your organization operate in?
- [ ] Which regulatory frameworks are mandatory (not optional) for your organization? (List them)
- [ ] Which frameworks are important but not mandatory?
- [ ] Do you have AI governance requirements today, or expect to within the next 12 months?

Section 2 – Organizational Structure

- [ ] How many separate legal entities or subsidiaries need to be on the platform? (List them)
- [ ] Do different entities need different framework coverage?
- [ ] Do you need scoped controls with inheritance across entities?
- [ ] Do you need jurisdiction-specific regulatory mapping?

Section 3 – Risk & Governance Depth

- [ ] Do you need formal risk registers with inherent vs. residual scoring?
- [ ] Do you need risk quantification in financial terms (FAIR, Monte Carlo)?
- [ ] Do you need risk appetite thresholds and key risk indicators?
- [ ] Do you need full policy lifecycle management (creation, ownership, attestation, exceptions, effectiveness tracking) beyond storing documents?
- [ ] Do you need separation of first, second, and third lines of defense?
- [ ] Do you need board-ready risk reporting and enterprise-wide roll-ups?

Section 4 – Operational Requirements

- [ ] Do you need continuous assurance (real-time control monitoring)?
- [ ] Or is periodic evidence collection sufficient for now?
- [ ] Which cloud providers do you need to connect to? (AWS, Azure, GCP, Oracle Cloud, other)
- [ ] Which enterprise applications need to integrate? (ServiceNow, Jira, SAP, etc.)
- [ ] What is your deployment requirement: SaaS only, private VPC, on-premises, or flexible?
- [ ] Do you have data residency or sovereignty requirements? If yes, in which jurisdictions?

Section 5 – People & Capacity

- [ ] How many people will use the platform day to day?
- [ ] How many dedicated GRC specialists does your organization currently have?
- [ ] Can you support a platform that requires dedicated specialists to operate or to make any updates (like adding a new framework)?
- [ ] Or do you need something that general practitioners across departments can use and update?

Section 6 – Timeline & Migration

- [ ] When do you need the platform to be live and operational?
- [ ] Are you replacing an existing GRC platform? If yes, which one?
- [ ] If replacing, can you run both systems in parallel during the transition?
- [ ] Is there a contract renewal date on your current platform that creates a deadline?
- [ ] What is your available budget for software, implementation, and first-year operations?

Print this page. Fill it out with your buying committee. Bring the completed worksheet to every vendor demo. It will keep the conversation focused on what matters to you, not what matters to the vendor.

For detailed evaluation criteria and vendor questions, download the companion guide: 'Enterprise GRC Platform or Compliance Tool? How to Tell the Difference' at **www.lockthreat.ai/resources/ebooks**

LockThreat

Ready to Start Your Evaluation?

You have the requirements worksheet. You have the evaluation questions. You have the checklist. Now see how a platform answers all of them, for your organization. Bring your requirements worksheet. We will show you your use cases, not ours.

See It in Action →

About LockThreat

LockThreat is the enterprise GRC platform for the era of AI, three layers within one platform: Enterprise GRC, Cyber Compliance, and AI Governance and Security. A platform that combines a System of Record, with a System of Defense for AI. Full governance, risk, and compliance across your entire organization, not just IT and cyber. Deployed as SaaS, private VPC, or on-premises to meet data residency and sovereignty requirements. Serving enterprises in North America and the Middle East, including regulated industries and government.

Learn more at www.lockthreat.com