



Report:

How Recorded Future Drives ROI for Cybersecurity Teams

How do Recorded Future customers benefit from comprehensive threat intelligence?

This report quantifies their results and ROI and shares their real-time use cases.



How Recorded Future customers are improving visibility, building better threat detection, and delivering time and cost savings

Research conducted and verified by



UserEvidence

Table of Contents

Methodology	04
Key results for Recorded Future customers: What's the ROI?	05
Short-term and long-term ROI, and how customers measure it	06
1. Short-term productivity gains	06
2. Long-term risk reduction.....	08
Where customers see ROI through efficiency and productivity gains	10
Threat intelligence in practice: Before and after Recorded Future	11
Before: Manual processes amidst high urgency	11
After: Actionable intelligence and automation	12
The results Recorded Future customers achieve.....	13
Alert triage, investigation, and response	13
Threat analysis, hunting, and reporting	14
Brand abuse mitigation.....	15
Vendor evaluation	16
Digital footprint analysis	17
Threat landscape analysis.....	17
Senior analyst efficiency	18
Where customers see business impact and overall risk reduction	19
Threat intelligence in practice: Before and after Recorded Future	20
Before: Innovation bottlenecks and risks with lasting impact	20
After: A resilient, agile, and more secure business.....	21
The results Recorded Future customers achieve.....	22
Brand reputation impact.....	23
Cyber insurance premiums	24
Downtime avoidance.....	24
Fraud losses.....	25
Get Started: Assess and address the threats your business faces.....	26

The modern threat landscape is unpredictable. Threat actors grow more sophisticated all the time, as do the tools they use to wreak havoc on organizations spanning all industries and sizes. This makes [the role of CISOs](#) and cybersecurity leaders all-important and incredibly challenging.

Recorded Future CISO Jason Steer sums it up this way:

“The job of threat intelligence and security is about managing, accepting, and reducing risk.”

It *sounds* simple — but we all know it’s not. When the risk is tied to millions of dollars in lost revenue due to a [ransomware](#) attack or reputational damage caused by a customer data breach, threat intelligence takes on a whole new weight.

Security teams need tools that can advance the maturity of their threat intelligence programs, and Recorded Future delivers. Recorded Future reduces customers’ risk and delivers tangible ROI in the face of threat analysis challenges.

Recorded Future customers see ROI on two main fronts as they look to increase confidence and trust from leadership and stakeholders:

1. Productivity across the team and processes

2. Risk reduction across the business, from reducing downtime to mitigating brand reputation impact

This report explores the tangible ways Recorded Future customers realize that value and allows you to calculate the potential ROI of the platform for short-term and long-term results.



Methodology

We partnered with third-party research provider UserEvidence to collect quantitative ROI data and qualitative feedback on Recorded Future. They conducted two distinct surveys:

1. The first survey (from July 2024) captured details about 117 customers' threat intelligence programs and how Recorded Future contributed additional visibility, team capacity, time savings, and business impact.
2. The second value metrics survey (from November 2024) captured insights from over 170 customers. This research built on the first survey, capturing more in-depth quantitative details on customers' reported efficiency improvements, overall risk reduction, and brand impact.

Key results for Recorded Future customers: What's the ROI?

We *will* break down every metric, testimonial, and survey response we gathered—but this highlights the overall ROI of Recorded Future customers in any given year.

\$290,237

in savings due to productivity improvements.

That's a

141.9% ROI

in time and team savings alone.

\$371,263

in direct business impact, from fraud loss reduction to downtime avoidance.

That's a

209.4% ROI

when it comes to reducing business risk.

Altogether, Recorded Future customers see a total of

351.3% ROI in a year.

"Threat Intelligence allows us to see the unknown and stay proactive to emerging vulnerabilities. We're able to predict things easier with threat intelligence that our other security tools just don't have insight into."

Nathalie Salisbury

Strategic Threat Intelligence Analyst, Novavax



Short-term and long-term ROI, and how customers measure it

Recorded Future customers see tangible ROI from the platform, saving the business significant time and money and reducing risk. First, let's unpack the two key areas of ROI and how our research measured them.

1. Short-term productivity gains

Across the board, organizations are asking their cybersecurity teams to “do more with less,” cutting security budgets and leaving leaders under pressure to limit the strain on already-stretched teams. As Recorded Future CISO Jason Steer explains, “Finding ways to automate and save time are helpful to reduce the burden. Anything that can help teams operate more efficiently is a huge win.”

More mature security teams are more productive teams. Efficiency via threat intelligence automation and streamlined workflows from Recorded Future allows them to be more productive *and* proactive.

When Recorded Future enables faster threat detection and analysis, analysts can respond sooner to protect brand reputation and support business operations without becoming overwhelmed, creating a more mature security team.

“Threat intelligence will always improve your visibility. The important part is to do it without overburdening your team. How can we add new threat intelligence use cases without creating a whole load of extra work and alerts to deal with?”

Jason Steer

CISO, Recorded Future

We surveyed Recorded Future customers to learn how much time they saved across:

- Alert triage, investigation, and response
- Threat analysis, hunting, and reporting
- Brand abuse mitigation
- Third-party vendor evaluation
- Threat landscape analysis
- Digital footprint analysis
- Senior analyst efficiency

Using salary and company benchmark data, we also mapped their reported results to tangible financial value to the business.

“Recorded Future was a game-changer for us, transforming how our team managed threats and stayed proactive. With their platform, we automated repetitive reporting tasks, which allowed us to move key resources onto critical issues, tightening our focus on real threats. This shift didn’t just streamline our workflows; it gave us back nearly 50% in efficiency — significant when you’re dealing with a constant flow of new data.”

Jack Edens

IT Security Analyst, Dupaco Credit Union

2. Long-term risk reduction

Recorded Future customers unlock far-reaching business impacts through risk reduction. Comprehensive threat intelligence increases visibility and efficiency for better and faster threat detection and response. In turn, these workflows uphold brand image and reputation, prevent financial losses, and protect the business as a whole.

Recorded Future provides customers with the tools to make better decisions and streamlines responses for a stronger, more resilient business. The platform also equips security teams to prove the value of threat intelligence, answer questions from other teams, and enable innovation rather than blocking it due to concerns about risk.

“Recorded Future provides actionable data and context to make decisions with confidence and automate workflows that you might not otherwise feel quite so confident about.”

Jason Steer

CISO, Recorded Future

We surveyed Recorded Future customers to understand the ROI their organization receives from risk reduction across these areas:

- Prevention of domain impersonation and typosquatting
- Lower cyber insurance premiums
- Downtime avoidance
- Prevention of fraud losses

Using industry benchmark data, we also mapped their reported results to trackable business value.

“Recorded Future allows us to shift our mindset from being more reactive in nature to being more proactive and responsive to threats that went unnoticed in the past. This, in turn, has facilitated the development of new processes that have enhanced the overall security posture of the business.”

Lead Cyber Defense Engineer

Food & Staples Retailing Company



Where customers see ROI through efficiency and productivity gains

Mature threat intelligence programs don't just *react* to threats. They prevent breaches by proactively understanding the landscape and their digital footprint. They identify threats and mitigate them before they turn into attacks on their environment and respond to incidents before they impact the business.

To embrace this approach, they need a threat intelligence solution that offers comprehensive external visibility and supports efficiency so analysts can spend their time strategically.

Threat intelligence in practice: Before and after Recorded Future

How does Recorded Future transform threat intelligence? Next, we'll paint a picture of the night-and-day difference when enterprises adopt our platform.

Before: Manual processes amidst high urgency

Without automated threat intelligence and context, cybersecurity teams shoulder the burden of time-consuming and tedious manual workflows like this:

1. Find relevant data sources, including open-source intelligence feeds, blogs, news outlets, social media, and forums.
2. Collect unstructured and complex data from all relevant sources.
3. Sift through the collected data to separate relevant insights from noise and normalize data, if needed.
4. Analyze the data to identify potential threats, patterns, and correlation data.
5. Compile a report with findings.
6. Distribute the report.

These processes — along with manual alert triage, investigation, and response — aren't just frustratingly manual for team members. They also delay or slow down organizations' response times.

Security teams are inundated with alerts, some of which are noise and some of which are relevant and urgent. If they don't have actionable threat intelligence, they can't efficiently gain an understanding of the priority or criticality of each. And when it comes to addressing a security threat, time is of the essence.

After: Actionable intelligence and automation

Recorded Future helps teams efficiently capture, compile, and analyze threat data, turning it into actionable intelligence that teams would otherwise need to triage, investigate, and respond to manually. This frees the security team to focus their energy on responding to high-priority threats and hunting new ones. Rather than struggling to address everything that *seems* important, they can think strategically about protecting their organization.

In turn, by boosting productivity, automation decreases investigation *and* response times:

- Many Recorded Future customers use risk lists and integrations to implement automated workflows. These functionalities let organizations enrich alerts from other tools with threat intelligence and lower investigation times.
- To drive down response times, users can designate in Recorded Future that they'll only look at alerts with a risk score above a certain number — all other alerts will be autoremediated. In many cases, automated alert response reduces response time to seconds instead of hours or more.

"We use Recorded Future's risk lists to block malicious IPs with a risk score of 65 or higher. As a result, we automatically make an average of approximately 5 million blocks per day and have made more than 150 million blocks in the last 30 days, resulting in a time savings of about 40 hours per month for our team. We rarely need to allowlist something."

Information Security Specialist

Industrial Conglomerates Company

Enhanced productivity builds a more proactive, mature, and resilient business across all of the security team's activities.

The results Recorded Future customers achieve

Recorded Future customers achieve a more proactive, productive, and mature threat intelligence program, saving hundreds of thousands of dollars in productivity along the way.

Here are the activities where they save time and money and improve their processes.

Activity/Area	Weekly Time Savings
Alert triage, investigation, & response	11 hrs
Threat analysis, hunting, & reporting	11 hrs
Brand abuse mitigation	8 hrs
Vendor evaluation	7 hrs
Digital footprint analysis	8 hrs
Threat landscape analysis	10 hrs
Senior analyst efficiency	50 hrs

Alert triage, investigation, and response

Before using Recorded Future, teams spent an average of 34 hours per week on alert triage, investigation, and response. They reported saving nearly 11 hours each week with Recorded Future.

Customers save an average of
11 hours
per week on alert triage,
investigation, and response efforts.

Automation is a hallmark of more mature threat intelligence programs — with automated investigation, security teams can streamline threat detection and move straight to responding to relevant alerts more quickly.

What's more, Recorded Future customers also receive those alerts *sooner* to ensure timely action — 1 in 2 said that Recorded Future often delivers important alerts hours or days earlier than other vendors.

"Recorded Future has significantly improved our organization's security operations. We automated 70% of manual workflows, cutting investigation times by 50%. This led to a 40% increase in threat detection efficiency and a 30% reduction in response times, enhancing our overall security posture."

Senior SOC Analyst & Threat Intelligence Analyst

Air Freight & Logistics Company

90% of the work of [uab Medicine's](#) SOC moved from event response to threat hunting.

Threat analysis, hunting, and reporting

Before using Recorded Future, customers spent an average of 32 hours per week on threat analysis, hunting, and reporting. With Recorded Future, they reported saving an average of 11 hours each week.

Recorded Future customers save
11 hours
per week on threat analysis, hunting, and reporting.

With the relevant insights that threat intelligence provides, this process becomes much more simple. Analysts can confidently identify and prioritize the most relevant threats using information from Recorded Future. On average, customers reported being able to identify new threats 65% faster with Recorded Future, which means they can more effectively mitigate potential damage from cyber attacks.

Customers detected new threats

65%

faster with Recorded Future.

"Thanks to valuable and actionable data, we cut our intelligence hunting, reporting, an analysis by 80%."

Valentin Vanlaeys

Threat Intelligence Lead,
Proximus Ada

"Recorded Future has allowed us to take a more proactive approach to security, in particular with assessing threats to our tech landscape and setting priorities for eligible threat-hunting activities. Additionally, it has provided us visibility into spaces that we otherwise would be unable to attain such as dark web marketplaces for credential leaks."

Threat Intelligence Analyst

Construction & Engineering
Company

Brand abuse mitigation

Actionable threat intelligence streamlines the security team's efforts to protect brand assets from violations and abuse by malicious actors. Without Recorded Future, customers spent an average of 24 hours each week on brand abuse mitigation.

Now, they cite that Recorded Future drove greater efficiency, saving analyst teams 8 hours every week.

Recorded Future helps the security teams not only save time but also more effectively protect the company and prevent the loss of value that occurs with brand abuse.

On average, customers save

8 hours

weekly on brand abuse mitigation.

"We have coverage on hundreds of IPs and assets. Automating scanning of brand assets helped us provide better brand protection. As a trust-and-safety manager, I can mitigate reports of various brand violations including dark web coverage."

Joe Azzouggagh

Manager of Trust and Safety, ruby

Vendor evaluation

Enterprise security teams are tasked with assessing the associated risks of third-party vendors and contractors. Without threat intelligence, this process is time-consuming and not always effective. Not to mention: it's difficult to keep an eye on vendors continuously, rather than just at the point you're determining if you want to bring them on board. We would want to know if a third party vendor has been breached to mitigate the impact — wouldn't you?

Customers spent an average of 21 hours weekly on vendor evaluation before using Recorded Future. With the platform, they reported saving 7 hours per week. By offering visibility into third parties' risk landscape, Recorded Future helps teams prioritize key risks and identify security gaps, which reduces the time analysts spend on risk assessment.

Recorded Future customers save

7 hours

weekly on vendor evaluation.

"When presented with a new vendor, we use Recorded Future to do an initial analysis of the vendor. This has helped us remove potentially risky vendors before we do business with them, saving countless hours during drawn-out vendor security assessments on unqualified vendors."

Brian Dickerson

IT Security Manager, HumanGood

Digital footprint analysis

Security teams that deeply understand their organization's digital footprint can take the steps to proactively protect their company's digital assets and properties.

Recorded Future customers save
8 hours
per week on digital footprint analysis.

Without Recorded Future, customers spent an average of 24 hours each week on digital footprint analysis. They reported saving 8 hours per week thanks to Recorded Future.

Threat landscape analysis

Before Recorded Future, our customers spent an average of 28 hours each week on threat landscape analysis. The platform enables them to conduct this analysis with greater efficiency, saving over 10 hours each week.

Customers cite saving
10 hours
on threat landscape analysis weekly.

When you understand the threat landscape around your organization, your security team can ensure that necessary controls are in place *before* a threat impacts your organization.

"We are able to spend less time searching for daily news, and we're also able to save about an hour or so per threat hunt kicked off."

Senior Cybersecurity Specialist

Electrical Equipment Company

Senior analyst efficiency

Customers save an average of

\$70K

per year by improving senior analyst efficiency and transitioning tasks to junior analysts.

Customers reported that with Recorded Future, their teams have been able to shift a significant portion of work away from senior analysts to junior analysts. Based on observable data for the average team at a billion-dollar company, this shift equates to

over 50 hours of senior analyst time saved per week — or nearly \$70,000 per year, given the difference in salary.

This is critical efficiency for skilled analysts because it allows them to focus their energy and time on the kinds of strategic decisions and proactive defensive work that only a human can focus on, maturing the program overall.

Mercury Financial estimated

2-4X

full-time employee headcount efficiency with Recorded Future.

So: what's the ROI?

Across all threat intelligence areas and including improvement to senior analyst efficiency, Recorded Future customers saved

100 hours weekly, or \$290K yearly.



Where customers see business impact and overall risk reduction

With a mature threat intelligence program, security teams reduce risk and drive positive financial and brand impacts for the business. Recorded Future provides actionable data and context that allows security teams to confidently make decisions and respond to threats, enabling long-term resilience and agility.

"The increased visibility allows our organization to approach threat intelligence in a more proactive manner and build defense logic based on adversarial TTPs targeting us and our affiliates."

Bryan Cassidy

Lead Cyber Defense Engineer, 7-Eleven

Threat intelligence in practice: Before and after Recorded Future

Robust threat intelligence can take cybersecurity from being viewed as a necessary evil to an enabler of innovation and a supporter of business goals. Here is how security teams function within the broader business without Recorded Future and with it.

Before: Innovation bottlenecks and risks with lasting impact

Without the right tools to support a mature threat intelligence program, the security team often lacks the information and context to effectively assess risks to the business *and* communicate those risks to other teams.

Instead of seeing how cybersecurity upholds the brand image and protects the business from financial losses through threats of multiple types, other teams and leaders view security as a roadblock to business initiatives. From mergers and acquisitions to expanding into a new region to buying a new tool, virtually all business initiatives require approval from security. But when security has to deny a request because of uncertain threats and risks (*without* tangible threat-related insights in hand) time and time again, security seems to other teams like a blocker rather than an enabler.

Risks to the business are relentless and constant, from downtime to fraud losses. Security teams need a full understanding of the threat landscape to answer leaders' questions about risks and stay one step ahead of the constant barrage of threats.

"Recorded Future helps us democratize intelligence and create a shared understanding of CyCrime and Nation State actors' behavioral patterns towards our services."

Espen Agnalt Johansen

CSO, Visma

After: A resilient, agile, and more secure business

The future of cybersecurity lies in businesses embracing the business value of threat intelligence. When cybersecurity leaders can show the substantial impact of threat intelligence, they enhance the reputation of their team and, ultimately, the business.

Recorded Future strengthens an organization's resilience to detect, respond to, and remediate the threats it will inevitably face — and remain agile over time.

1 in 2 survey respondents reported that Recorded Future has made their organization **significantly more resilient to cyber threats**.

Resiliency in the face of a changing threat landscape requires two key components: **planning** and **identification**.

By using our platform, Recorded Future customers understand their highest priorities so they can quickly identify and respond to threats. They can more effectively prevent loss of revenue due to downtime, typosquatting, and detriment to brand capital, improving the company's image with stakeholders from potential and current customers to insurers.

What's more, with Recorded Future, organizations can identify the gaps in their defenses — vulnerabilities, compromised credentials, unknown assets, and supply chain risks. They can begin shoring up weaknesses and mitigate these gaps before threat actors exploit them.

"We have improved brand protection by at least 100%. We can identify some risks and patterns in infancy stages, and we have been able to automate some brand scanning to eliminate hours of manual work. As we automate more coverage, we have saved hundreds of labor hours per quarter and improved efficiency."

Joe Azzouggagh

Manager of Trust and Safety, ruby

"Recorded Future gives me the information I need to be able to articulate threats to the rest of the organization. Whether there is a threat just to my industry or just something that was in the news, Recorded Future breaks things down so I can quickly get up to speed."

Information Security Director

Specialized Consumer
Services Company

At its best, threat intelligence allows security to influence the business and delivers insights that keep the organization secure, improves customer trust, and prevents compliance failures. In this way, security works to build an all-around stronger organization by empowering other teams to participate in safer, secure, and more strategic ways of doing business.

The results Recorded Future customers achieve

Risk reduction through threat intelligence saves money and prevents loss across numerous areas of business and brand impact, amounting to over \$371,000 annually.

Next, we'll unpack where this risk mitigation occurs within the business.

Area	\$ Value
Brand reputation impact	\$2,602/month
Cyber insurance premiums	\$2,497/month
Downtime avoidance	\$19,025/month
Fraud Losses	\$6,812/month

57% of customers say that using Recorded Future has **significantly reduced their organization's overall cyber risk.**

Brand reputation impact

Typosquats — illegitimate but similar-looking web domains — can result not just in lost web traffic and brand safety issues, but also increased phishing attacks. The faster security teams can take these domains down, the safer employees, partners, and customers are from disclosing personal, confidential, or financial information.

Customers report a

51%

increase in efficiency when removing typosquatting instances.

the actions they set out to accomplish by visiting your site. We see that as an increase in web traffic that we can quantify the value of with the help of research by the [University of Illinois](#).

An average billion-dollar business sees 2 million monthly web visits. At an average loss rate of 5.28% due to typosquatting, more efficient typosquat takedowns with Recorded Future would help them recover over 50,000 website visits each month — and an expected \$2,600 in value, according to research by the [University of Illinois](#).

Recorded Future customers reported that they are now 51% more efficient at taking down typosquatting instances. Swift typosquat mitigation not only helps combat phishing attempts, but it also enables your customers to seamlessly carry out

Exelon [reports](#) a

100%

hit rate on detecting typosquatting domains that were spun up for testing purposes.

“Recorded Future has notified us of multiple third-party data breaches such as our vendors being hit by ransomware. This has led us to find our data included in these breaches. We have been able to stop multiple typosquat domains before they could be weaponized against our company.”

[Chris Cafego](#)

Cybersecurity Engineer/Threat Analyst, EOG Resources

1. Source: <https://www.cs.uic.edu/~ckanich/papers/khan2015every.pdf>

Cyber insurance premiums

Premiums for cyber insurance vary widely, depending on how much confidential information a company holds, what cyber controls are in place, their approach to vetting third-party vendors, and other factors. What doesn't vary is the value of threat intelligence to drive down risk, which can position your organization more positively to insurers in the areas they cover.

Customers save an average of
\$2,497
on their monthly insurance premiums.

Based on observable market data and the average 2024 [cost of a breach](#) being \$4.88 million, a typical billion-dollar company likely pays a yearly premium of \$207,400, or \$35-50,000 per million of coverage. Reported reductions in average cyber insurance monthly premiums from Recorded Future's customers translate to a monthly savings of approximately \$2,497 for the business.

Cummins [reported](#) a **32%** year-over-year reduction in cyber insurance premiums with Recorded Future.

Downtime avoidance

Any downtime — no matter how short — can do lasting damage to public brand perception of your brand. On top of the inconvenience when service is delayed, downtime due to a security breach can foster a perception that your company is untrustworthy or unreliable — a substantial and lasting risk to your brand image.

By preventing disruptions with threat intelligence, you uphold the financials and reputation of your business. Our customers report that threat intelligence from Recorded Future helps minimize downtime, which for a billion-dollar organization translates to an

With Recorded Future, a billion-dollar organization could save

\$19,025

per month due to
downtime mitigation.

average revenue value of approximately \$19,025 per month. This doesn't include the added benefit of avoiding the reputational damage that could result from any security breach.

Fraud Losses

Fraud losses such as transaction fraud and billing schemes result in significant risks to the brand and financial losses for the business.

Recorded Future's threat intelligence helps customers reduce fraud losses. A billion-dollar business that loses \$500,000 annually to payment fraud losses would recover over \$6,812 per month through improved threat intelligence with Recorded Future. Outside of the payments themselves, fraud loss mitigation also contributes financially by strengthening the integrity and trustworthiness of your business.

A billion-dollar organization could save over

\$6,812

per month with Recorded Future.

"We use Recorded Future's dark web intelligence to proactively stop attacks, reset weak passwords, or prevent bank card fraud. This has a potential savings of \$1,000-2,000 depending on the customer or situation."

Sergio Castrejon

Sr. Information Security Analyst,
Jefferson Bank

So: what's the ROI?

Across all risk reduction areas, Recorded Future customers can save

\$31K monthly
or **\$371K yearly.**



Get started: Assess and address the threats your business faces

Security teams have virtually countless potential vulnerabilities and risks to mitigate — while threat actors only have to succeed once, and their skill sets are advancing all the time thanks to AI. Leaders need to know which activities deliver the highest impact with the lightest lift.

If you're ready to improve your overall threat intelligence, here's how to get started:

- 1. Define your business's security priorities.** Work with security and business leadership to identify top concerns and the “crown jewels” that most need to be secured. Everything else you do should stem from these.
- 2. Assess threats in the context of risk to the business.** When everything is urgent, nothing is. Not all vulnerabilities will be exploited, and not all threat vectors pose an immediate risk. Focus first on responding to the threats that could actually harm your people, assets, and business.

Once you've decided what's most important to protect (and protect against), Recorded Future is here to help you respond to the threats that matter. With 96% of customers willing to recommend Recorded Future to a peer, the [return on investment](#) is clear.

Our comprehensive threat intelligence ensures that you can see all threats, see them first, and prioritize and act to remediate incidents before they impact your business. Give your team actionable insights and timely intelligence to get ahead of present and future attacks. Ask our team about the ROI that Recorded Future can bring to your unique business — [book a demo](#) with our team today.



UserEvidence Research Methodology

About UserEvidence

UserEvidence is a software company and independent research partner that helps B2B technology companies produce original research content from practitioners in their industry. All research completed by UserEvidence is verified and authentic according to their research principles: Identity verification, significance and representation, quality and independence, and transparency. All UserEvidence research is based on real user feedback without interference, bias, or spin from our clients.

UserEvidence Research Principles

These principles guide all research efforts at UserEvidence -whether working with a vendor's users for our Customer Evidence offering, or industry practitioners in a specific field for our Research Content offering. The goal of these principles is to give buyers trust and confidence that you are viewing authentic and verified research based on real user feedback, without interference, bias, and spin from the vendor.

Principle 1 - Identity Verification

In every study we conduct, UserEvidence independently verifies that a participant in our research study is a real user of a vendor (in the case of Customer Evidence) or an industry practitioner (in the case of Research Content). We use a variety of human and algorithmic verification mechanisms, including corporate email domain verification (ie so a vendor can't just create 17 gmail addresses that all give positive reviews).

Principle 2 - Significance and Representation

UserEvidence believes trust is built by showing an honest and complete representation of the success (or lack thereof) of users. We pursue statistical significance in our research, and substantiate our findings with a large and representative set of user responses to create more confidence in our analysis. We aim to canvas a diverse swatch of users across industries, seniorities, personas - to provide the whole picture of usage, and allow buyers to find relevant data from other users in their segment, not just a handful of vendor-curated happy customers.

Principle 3 - Quality and Independence

UserEvidence is committed to producing quality and independent research at all times. This starts at beginning of the research process with survey and questionnaire design to drive accurate and substantive responses. We aim to reduce bias in our study design, and use large sample sizes of respondents where possible. While UserEvidence is compensated by the vendor for conducting the research, trust is our business and our priority, and we do not allow vendors to change, influence, or misrepresent the results (even if they are unfavorable) at any time.

Principle 4 - Transparency

We believe research should not be done in a black box. For transparency, all UserEvidence research includes the statistical N (number of respondents), and buyers can explore the underlying blinded (de-identified) raw data and responses associated with any statistic, chart, or study. UserEvidence provides clear citation guidelines for clients when leveraging research that includes guidelines on sharing research methodology and sample size.