Thoropass™

Health

State of Health Security 2025

RESEARCH AND TRENDS

Contents

Introduction

The purpose of this report is to look back at research and news from the past year in order to identify key data points and trends that will be useful in driving healthcare security in the coming year. Healthcare leaders can use the data here to start conversations, build arguments, and develop strategy.

Compiled by Thoropass, this report is meta-research that looks across multiple studies about a particular theme (in this case cybersecurity in healthcare) and pulls threads in order to point toward what will be most salient to healthcare organizations in the coming year. The research comes from a variety of government entities, journalists, and industry leaders, some reporting directly on security in healthcare and some on related topics over the last two years.

Thoropass is a compliance and audit solution that eliminates the friction of infosec security so that organizations of every size and industry can attain scalable security across their systems. Thoropass Health—with the help of our Health Advisory Board—is a practice within Thoropass that works with healthcare-related organizations on compliance frameworks (such as HIPAA, HITRUST, and SOC 2), penetration testing, and the ethical use of AI (through ISO 42001, DDQs, etc.)

Key Findings

The amount and cost of cybersecurity events in healthcare-related organizations makes healthcare a unique industry. Only the financial (including FinTech) industry comes close to the breadth and depth of attacks faced. Despite (over)confidence of security leaders in healthcare, the data shows increasing need for vigilance.

97%

of healthcare workers believe in their org's ability to defend against cyber attacks [1]

24%

of all cyber events in first half of 2024 were healthcare-related [2]

⚠ 10 years

YoY increases in healthcare security breaches [3]

$1.47 million

average cost of a cyberattack [4]

10 x

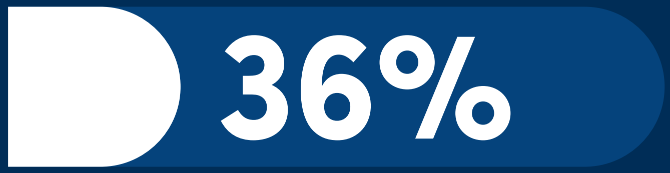
stolen healthcare data is 10 x more valuable than credit card data [5]

37%

of cyber events are email compromises, the most of any source [1]

100,000,000

people affected by a single breach at Change Healthcare [6]



36%

of the world's data will be healthcare related by end of 2025 [7]

AI use
IS GROWING

Artificial intelligence (AI) and Maching Learning (ML) have seen explosive growth since 2023. This will only continue into 2025 as healthcare orgs balance the data threats that come with it versus the automation efficiencies it can provide to overtaxed workforces and budgets.

#1 **AI seen as most popular tech for managing increased risk**[8]

63% say keeping org's data safe on AI is difficult[4]

59% see a reduction in their risk workforce due to AI automation[8]

Data
NEEDS STRUCTURE

Data creation and usage continues its exponential climb, yet most of it is unstructured (e.g. handwritten, siloed, not tagged, etc.) Many healthcare orgs are trying to catch up by addressing this trend internally, while many others see AI as a solution.

90% **of healthcare data is unstructured**[9]

1281% jump in direct tagging to healthcare data over the last year in a sample cohort[10]

78% use AI and ML to automate data analysis[8]

Controlling access

IS KEY

Access control is the biggest threat to a healthcare organization's security. In addition to threats from third parties and supply chain issues, organizations are beginning to see legacy systems and siloed teams as a threat that needs to be consolidated.

#1

credential access is biggest fear for healthcare orgs [1]

45+

average number of security tools used in enterprises [11]

71%

of CROs believe integrated systems make for safer orgs [8]

68%

reported 4 or more attacks on their supply chain in last 2 years [4]

Need to react

QUICKLY

Urgency is the number one issue facing healthcare organizations' responses to cyber threats. Bad actors are moving faster, and regulatory acts are asking for near real-time response and notification.

62 minutes

average time it takes an adversary to move from initial host to another once in a system [11]

72 hours

amount of time US government wants health orgs to report cyber events [12]

53%

of healthcare orgs have documented plans to address vulnerabilities [13]

28%

of orgs are only set up to monitor (not react) to cyber vulnerabilities [1]

Thoropass™

Rise of AI as a Solution

Every new phone, computer, and medical device is likely to be embedded with AI or machine learning capabilities in 2025. While the gains in automation are promising, the threats to data privacy and friction between new and legacy systems can't be overlooked. For now, healthcare orgs seem more excited than nervous about new AI technology.

#1

AI seen as the most popular tech for managing increased risk [8]

$156 billion

to be saved in healthcare automation through 2026 [10]

54%

have embedded AI in cybersecurity and patient care [4]

57%

think AI is very effective in improving organizations' cybersecurity posture [4]

55%

think AI-based security tools will increase productivity for IT security personnel [4]

41%

planning to spend more than half of their risk management budget on technology in the next 12 months [8]

63%

think keeping org's data safe on AI is difficult [4]

59%

see a reduction in their risk workforce due to AI automation [8]

Working Alongside AI

Bunny Ellerin

Bunny Ellerin is the co-founder and CEO of Digital Health New York (DHNY). She also serves on Thoropass' Health Advisory Board.

New can be scary. And in any industry other than technology, AI–its use and regulation–is still very much new. Health industry observers would be right to be careful (if not skeptical) of AI's use in our highly regulated industry. But as the data in this report shows, instead of running away from AI, many insiders are running toward it for one really good reason: its ability to help the health industry take control of its data.

According to RBC Capital Markets, an estimated 36% of the world's data will be health-related by the end of 2025[7]. But lots of that data–up to 90%--is unstructured. All of the handwritten reports, untagged fields, and information shared between new and legacy systems could be left behind, as good as useless.

This is why so many executives are seeing AI (and closely related machine learning) as a solution to help them keep up. At a time where health data is rising (and attackers are seeing it as 10x as valuable as credit card data), the industry is also seeing more mergers and acquisitions, more third parties entering the supply chain, and more legacy systems working alongside the most cutting edge Internet of Things medical devices.

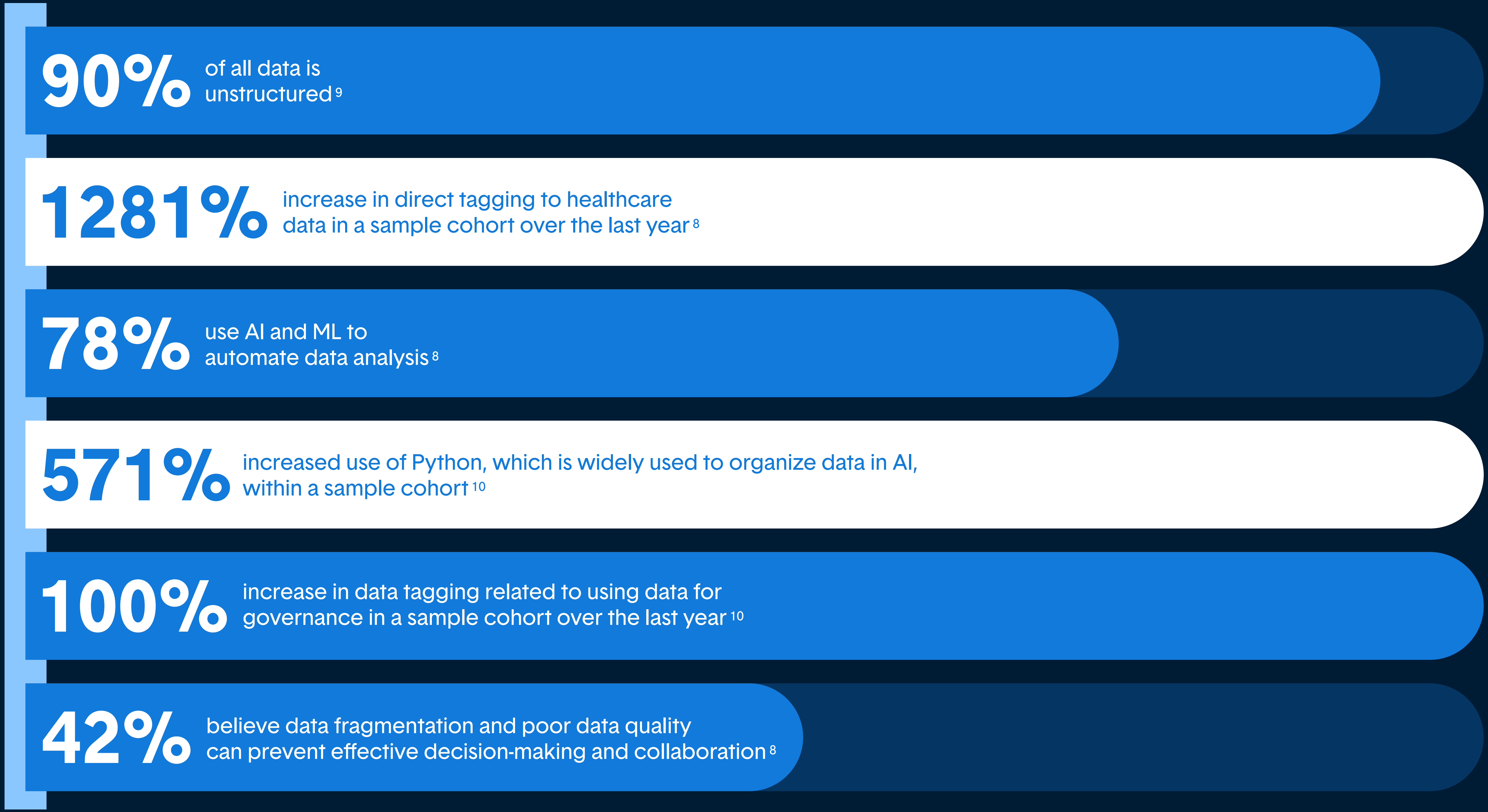
Yes, health leaders should be careful in protecting propriety and patient data that is entered into LLMs. Frameworks like HIPAA and NIST are as important as ever for protecting PHI. But as health-related companies face projected budgeting and staffing limitations (especially in rural or aging settings), AI is rightfully stepping in to automate some of the most burdensome data-related work needed for companies to keep up.

One way to ensure that AI works ethically with current systems is to follow guidelines related to ISO 42001, an updated compliance framework specific to AI adoption and use. Likewise, regular pentesting (including pentesting specific to AI systems) can help ensure that data leakage and ethical best practices are in use.

What's become clear since ChatGPT took over the tech world's conversations in 2023 is that AI is not fading away any time soon. As our phones and cars utilize this world-changing technology, it's now inevitable that our health-related companies, too, will be altered forever. The opportunity for us all is to learn as quickly as possible how to harness them to make us even more efficient and effective.

More Data/Less Structure

The move to digitize healthcare data will not slow down in 2025. Healthcare orgs are looking to AI and ML to help them with this influx by converting unstructured data into usable data that can drive patient care and business decisions.



90% of all data is unstructured[9]

1281% increase in direct tagging to healthcare data in a sample cohort over the last year[8]

78% use AI and ML to automate data analysis[8]

571% increased use of Python, which is widely used to organize data in AI, within a sample cohort[10]

100% increase in data tagging related to using data for governance in a sample cohort over the last year[10]

42% believe data fragmentation and poor data quality can prevent effective decision-making and collaboration[8]

Issues of Access

Credential access was the biggest concern for healthcare orgs as they looked to 2025. The reason this threat outpaces ransomware, phishing, and email-related issues is that healthcare orgs face unique challenges in siloed information, third party vendors, supply chains, and multiple security solutions spanning new and legacy systems. Of the hundreds of healthcare orgs polled about access:

#1 credential access is the biggest fear for healthcare orgs[1]

45+ average number of security tools used in enterprises[11]

68% reported 4+ attacks on their supply chain in last 2 years[4]

71% of CROs believe integrated systems make for safer orgs[8]

49% of hospitals state they have adequate coverage in managing risks to supply chain risk management[13]

47% reported a ransomware attack; 46% of those stated it was caused by a third party[13]

50% of hospitals are considering risks to patient care in their evaluations of new suppliers' products[13]

Keeping Your Data Clean and Close

Katherine Kelton

Katherine Kelton is an executive, specializing in legal, human resources, and global compliance.
She also serves on Thoropass' Health Advisory Board.

Cleanliness is next to godliness, especially in health-related fields where our digital practices are still catching up to our physical ones. As pointed out elsewhere in this report, the volume of health-related data continues to rise even as areas of the industry experience consolidation. Our challenge, then, is to ensure that this data is as useful as possible while being as secure as possible.

The challenges to clean data aren't just for the sake of security. KPMG reports that 42% of survey respondents believe "data fragmentation and poor data quality can prevent effective decision making." In other words, having usable data is crucial for companies to make strategic business decisions. As this report has detailed, AI and automation technology is helping some companies to corral and maintain actionable data. For others, though, the first step in data hygiene is understanding who has access to data.

What Kroll finds in their study speaks to this point: of every industry surveyed, credential (user) access to data was their perceived least significant security threat. The one exception was healthcare, where it ranked #1 by a longshot.

If fragmented data can inhibit decision making, it can also hinder collaboration. But clearly collaboration is not without its risks, according to Kroll. Because the healthcare industry can be both siloed and spread out by its very nature (not even considering the vast network of third party vendors on which most organizations rely), it's both understandable and unfortunate that this one particular threat is still fretted over, especially since email compromises continue to be the leading source of threat faced by healthcare organizations.

As a result, it's up to us in the industry to confront these two issues–data hygiene and data access–as one in 2025. Where AI and automation can help with data hygiene to a large degree, user access remains a unique cybersecurity concern that can be addressed through consolidated credentialing and monitoring. Maintaining your myriad regulatory and compliance frameworks through a single dashboard where you can also control user access at the employee level remains the gold standard for addressing data hygiene and access. Likewise, regular training and ensuring that any HIPAA security controls (such as use of MFA) are enforced consistently across systems and end users is more important than ever.

Healthcare is not unique in facing the growing importance of personal/patient data and working across dispersed teams. But given how valuable our data is, and how the frequency and severity of attacks are going up, it is more important than ever to look for technology solutions that enable secure, sustainable growth in 2025.

Responses to Regulation

Time is becoming a bigger factor in healthcare cybersecurity. While regulators are asking organizations to respond to breaches in days, bad actors are moving into systems in minutes. Most orgs are using immature security systems that monitor, but don't react, when attacks occur.

62 minutes

average time it takes an adversary to move from initial host to another once in a system [11]

72 hours

amount of time US government wants health orgs to report cyber events [12]

28%

of orgs are only set up to monitor (not react) to cyber vulnerabilities [1]

53%

of orgs have documented plans to address vulnerabilities [13]

68%

believe that integration and interconnection of risk management systems, domains, and processes had a significant enhancement to effectiveness over risk-related decision making [8]

89%

of hospitals that were conducting regular vulnerability scanning at least quarterly [13]

20%

go beyond scanning with use of penetration testing, red/blue teams, etc. [13]

96%

of small, medium, and large sized hospitals claim they were operating with end-of-life operating systems or software with known vulnerabilities [13]

Looking Ahead

The data and perspectives in this report offer insights and trends that are more reliable than mere predictions. As you and your organization prepare for, and move through, 2025 and beyond, the following themes should be considered through the frame of cybersecurity:

→ Technology:

As this report shows, the rewards outweigh the risks when investing in new technology, especially in AI. As automation and machine learning get faster and smarter, tech can save on headcount and make your company more secure.

→ M&A, TPRM, and Data Sharing:

Healthcare will continue its 30-year trend of consolidation, making it increasingly important that data is transportable across networks, and access controls are in place for data to be used by those who need it.

→ Global Risks:

Geopolitical and economic risks will have primary and secondary effects on the healthcare industry as leaders grapple with local and international regulations, rising costs and inflation, and threats from bad actors in light of global conflicts and governmental changes.

→ Compliance:

Basic frameworks like HIPAA, NIST, and HITRUST continue to evolve, requiring updating training, auditing, and (in some cases) pentesting. As AI becomes more wide-spread, compliance with frameworks like ISO 42001 become necessary.

→ Proactive Protection:

Basic monitoring and minimal preparations continue to be inefficient. An increased effort to be audit-ready with compliance and regulation, and to be ready with a reaction plan will be crucial to dealing with inevitable threats.

Endnotes

[1] **Kroll.** The State of Cyber Defense: Diagnosing Cyber Threats in Healthcare. (2024)

[2] **Amantha May. Tebra. The Intake.** The major cyberattacks that have affected healthcare systems in 2024. (2024)

[3] **Steve Alder. The HIPAA Journal.** Healthcare Data Breach Statistics. (2024)

[4] **Proofpoint.** Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care. (2024)

[5] **John Riggi. American Hospital Association.** The importance of cybersecurity in protecting patient safety. (2024)

[6] **U.S. Department of Health and Human Services.** Breach Portal. (2024)

[7] **RBC Capital Markets.** The healthcare data explosion. (2024)

[8] **KPMG.** Future of Risk. (2024)

[9] **IDC. Box.** The untapped value of unstructured data. (2023)

[10] **Snowflake.** Data Trends 2024: Healthcare and Life Sciences. (2024)

[11] **Crowdstrike.** Global Threat Report. (2024)

[12] **Cyber Incident Reporting for Critical Infrastructure Act of 2022.** (2022)

[13] **U.S. Department of Health and Human Services.** Hospital Cyber Resiliency Landscape Analysis. (2024)

Thoropass™