WHEN AI AND ZERO TRUST COLLIDE

RISE OF THE MACHINES

A *PROJECT ZERO TRUST* STORY

GEORGE FINNEY WITH ZACH VINDUSKA

FOREWORD BY JOHN KINDERVAG

WILEY

When AI and Zero Trust Collide

Rise of the Machines

A Project Zero Trust Story

George Finney with
Zach Vinduska

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@wiley.com.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2025906749

Paperback ISBN: 9781394303717
ePDF ISBN: 9781394303731
ePub ISBN: 9781394303724
oBook ISBN: 9781394352517

Cover images: Big data research and conversion process set. © Iconic Prototype/stock.adobe.com, Ai chatbot consultant concept vector flat style design illustration © Siberian Art/stock.adobe.com, Research center for artificial intelligence and robots. © YummyBuum/stock.adobe.com.

Cover design by Jon Boylan

Set in 10.5/13pt PalatinoLTStd-Roman by Lumina Datamatics

Contents

Foreword

Once again, I am honored to write the foreword to another book by my good friend George Finney. This novel, *Rise of the Machines: A Project Zero Trust Story*, is a sequel to *Project Zero Trust*, a landmark cybersecurity novel now properly ensconced in the Cybersecurity Cannon Hall of Fame.

Rise of the Machines focuses on the intersection of Zero Trust and artificial intelligence. It does this with amazing simplicity. While AI is a complex topic that means so many different things in different contexts, George does a masterful job of making every aspect of AI understandable to individuals who are not experts in the nuances of all of the acronyms and buzzwords. We throw around TLAs (Three-Letter Acronyms) like candy: GAI, LLM, ML (yeah, it's two letters, but you get the point). George demystifies all of these terms for the rest of us and then tells us specifically how to begin the journey of protecting these critical systems using a Zero Trust strategy.

This novel is not a dry, technical read. It creates characters that resonate with each of us. It also provides an eye-opening context for the AI discussion about our perceptions of AI. One of my favorite scenes in the novel occurs early in Chapter 2 (not a spoiler, I promise), when one of the characters asks, "When anyone talks about AI, why do we always make them evil?"

What a great question. George then goes on a litany of all of the evil AI characters we've seen in movies and TV. In fact, I've often thought that most of what the general public understands about any technology is primarily shaped by the mass media. In cybersecurity writ large, most of this perception is inaccurate. In AI, the doomsday predictions are loud and boisterous, but the reality remains to be revealed.

From my numerous conversations and BBQ Lunches (we live near each other) with George over the past few years, I know he has thrown his entire being into AI research to provide you, the reader, with as much accurate information as possible. This is done with finesse inside of an engaging story. He is educating us without the typical didacticism and boredom that comes from academia.

George is also a true Zero Trust expert. This is not just because he wrote a book about it, but because he's implemented it in real life. Zero Trust is experiential, not academic. It's this experience that George has been able to put on paper so well.

This experience gives *Rise of the Machines* such punch. A favorite quote in the book comes early in Chapter 1: "We're still in the early stages of extending Zero Trust to AI. We don't have a lot of specifics yet, but even if you can't spell *AI*, you probably know you need a lot of data. And Zero Trust is all about protecting data." What a great line. Simple. Intuitive. Unfortunately, this message often eludes practitioners. Folks think in products, not data. The first question you ask in Zero Trust is, "What are you trying to protect?" Of course, in AI, it is the data. The rise of AI will make this truth rise to the top.

Rise of the Machines isn't a long book. You can read it in a single sitting. It doesn't waste your time. It doesn't talk down to you. It's not preachy or pedantic. George hasn't padded it out to make it feel weighty. He's surgically dissected a convergence of two complex topics, AI and Zero Trust, and articulated them in such an engaging way that it makes the reader want to achieve George's objective: understanding that Zero Trust is simpler than you thought and that it's a perfect strategy to protect all the various aspects that comprise what we generically call artificial intelligence (AI).

As you read *Rise of the Machines*, look for all the Easter eggs George has hidden in the novel. George is not only a CISO, cyber expert, and a newly minted AI guru, but he's also a lawyer, novelist, and painter. And he's a pop-culture aficionado. I wouldn't want to play Trivial Pursuit against him. So keep an eye out for the cultural references sprinkled throughout.

Rise of the Machines is a must-read for anyone involved in cybersecurity and /or AI. The convergence of these two topics is accelerating at an unprecedented rate. This will drive the adoption of Zero Trust as the strategic way to protect all of the data and assets that interact with AI-adjacent systems.

I am forever indebted to my good friend George Finney for supporting me in telling the Zero Trust story truthfully and simply. This book is a synthesis of a practitioner and a thinker. In less than 200 pages, George gives us a blueprint for building a Zero Trust environment for our AI systems. That is a laudatory accomplishment. I learned a ton about AI from reading this book and was given a different lens to view the topic.

Thank you, George, for finding new and innovative ways to enlighten us on things others deliberately obfuscate. You make difficult topics accessible. I can't wait for the next book in the Project Zero Trust Novelistic Universe!

John Kindervag
Denton, TX
January 2025

About the Authors

George Finney is a Chief Information Security Officer who believes that people are the key to solving our cybersecurity challenges. George is the CISO for the University of Texas System and was the recipient of the Malcolm Baldrige Award for Cybersecurity Leadership in 2024, was recognized in 2023 as one of the top 100 CISOs in the world, and in 2022 as University Technology Leader of the Year. George is the bestselling author of several cybersecurity books, including the Cybersecurity Cannon Hall of Fame–winning *Project Zero Trust* and the Book of the Year Award–winning *Well Aware: Master the Nine Cybersecurity Habits to Protect Your Future*. George has worked in cybersecurity for over 20 years helping startups, global corporations, governments, and nonprofits improve their security posture. George received his Juris Doctorate from SMU, where he was the CISO, and is a licensed attorney. In his spare time, he creates spray-paint pop-art robots.

Zach Vinduska is a cybersecurity leader that is passionate about protecting people and organizations from cybercriminals. He is the Chief Information Security Officer for Credera and manages the Security and Privacy practice and has more than twenty years' experience leading security and technology teams of all sizes, from start-ups to the Fortune 500. He has led several transformative efforts as well as certification efforts such as SOX, ISO27001 and SOC for both publicly traded and privately held organizations. Zach is an advocate for the education of his fellow CISOs and speaks on the topic at conferences and multiple podcasts including a regular seat on Technically Minded podcast. He serves on multiple security related boards and councils.

Acknowledgments

I couldn't have written this book without you, dear reader. This book wouldn't have been possible without the massive outpouring of support from people all over the world who loved the first book, *Project Zero Trust*. Thank you for your kind words and your generosity. I'm so excited to be able to continue the story of Dylan and the whole team at MarchFit.

Your support allowed me to make this book even more fun with cool pop-culture references and nerdy humor. But it also gave me the courage to address my own imposter syndrome through the character Dylan. Rather than drive the narrative through the conflict with a threat actor like in the first part of *Project Zero Trust*, much of the conflict in this book comes through some of the interpersonal challenges that we all face when working together in a team.

When I talked to my publisher, Jim Minatel, about doing a sequel, he gave me that encouraging push that unleashed my creativity. I'm indebted to his guidance and the team of editors and designers and marketers for helping make this second book possible.

John Kindervag may think that I'm crazy, but he's had my back for years no matter what. He's not just the father of Zero Trust, he's an incredible mentor, not just for me, but I've heard from many people how much he's done to help them in their own lives, both personally and professionally. He's truly a national treasure.

For those of you who don't know my coauthor, Zach Vinduska, he's been a CISO for years and helped me workshop ideas for the last book. It only made sense to bring him in to help play an even bigger role in the sequel.

For all the books I write, I do a massive amount of research, which includes talking to people who are much smarter than myself to get their perspectives and insights. I'm humbled to have so much support from legends and luminaries in the cybersecurity world.

First, I want to thank Malcolm Harkins, whom I've known for nearly a decade. He and his team at HiddenLayer were instrumental in helping me get to the heart of understanding the details of how to protect AI from cybercriminals.

I'd also like to thank Jim Reavis and Illena Armstrong at the Cloud Security Alliance. This book wouldn't be possible without their support through their AI Safety Initiative and their generous introductions to so many people in the AI security community. One of the very first conversations I had after writing the book was with Caleb Sima, who helped me understand the big picture of AI and Security and is tireless in his commitment to build up the security community through his passionate work with the CSA.

Security gets better through a community, so I'm incredibly thankful that so many security leaders were willing to pitch in, like the prolific author and founder Ken Huang, who has been working with AI security for years. I'm thankful to Steve Grobman, CTO for McAfee, for his insights and colorful wisdom, really stretching my understanding of AI security. Jason Clinton, CISO for Anthropic, was incredibly thoughtful about where AI is going and what the security implications of this will be. And to Justin "Hutch" Hutchins for his early work on AI and social engineering, you should definitely check out his book, *The Language of Deception* (Wiley, 2023). And to Dutch Schwartz for providing tons of valuable feedback on early versions of this book.

Finally, I'd like to send a shout-out to Rick Howard for his incredible insights and support for many years. He's a legend in the security community and makes everyone around him better.

There are so many other people out there that I'm grateful to for your support over the years. If I've left you out of this list, please know that my heart is full of gratitude for being a part of my journey.

I love security. I love security so much that my wife, Amanda, is a little jealous. Thank you, Amanda, for all of your support over the years while I pursued my dream of being a writer and making a difference in the world.

Introduction

An ounce of prevention is worth a pound of cure. When it comes to cybersecurity, prevention is the most effective way of protecting our organizations. And when people inside an organization begin to work together, they need a strategy to follow to align the unique needs of the business with the goal of preventing breaches. Zero Trust is the strategy for prevention in cybersecurity and this is what makes Zero Trust one of the most successful cybersecurity strategies. It focuses on prevention for the thing that cybercriminals target most: trust.

According to a study by Statista in 2024, 43 percent of professionals surveyed worldwide indicate that their organizations have already adopted Zero Trust while another 46 percent of organizations have begun the process of adopting Zero Trust. That means almost 90 percent of all organizations are at some point on their Zero Trust journey. But in just the last two years, almost every organization in the world has also started adopting artificial intelligence (AI), and AI requires that we revisit our Zero Trust posture to ensure our organizations remain protected.

Rise of the Machines is the second book in the *Project Zero Trust* series. It applies the lessons learned from Zero Trust in the first book to the challenge of protecting organizations that are adopting AI. The *Project Zero Trust* series uses a fictional case study of a company called MarchFit to show how organizations can adopt a strategy of Zero Trust. More importantly, readers can see how the different roles inside an organization will play a part in the overall Zero Trust effort.

If you haven't read *Project Zero Trust* yet, don't panic! *Rise of the Machines* can be read as a stand-alone book to understand the challenges of securing AI systems. To get a deeper dive into the Zero Trust principles and design methodology, you can go back and read *Project Zero Trust*.

Preventing something from happening means that you have some knowledge about what you're trying to prevent. The pace of change around AI makes prevention a challenge because we can't always predict what new attacks or exploits will be around the corner. Like many other technology innovations over the last 50 years, AI has been largely developed without security in mind. And, in fact, the way most AI tools have been designed is with one hundred percent trust, meaning they trust all the data and inputs at every level in order to do what they do.

Zero Trust is the most effective strategy we have for securing AI precisely because of AI's reliance on trust.

While we use terms like AI or machine learning in this book, AI isn't just one thing. There are many different flavors of AI. This book will examine many of the different use cases of AI today, from LLMs and GPTs, to building your own AI models, to adversarial AI, AI in the SOC, and chatbots or digital avatars. We will use the Zero Trust design methodology to examine each one in turn, providing a case study into how to apply the Zero Trust principles and design methodology to all the different aspects of AI.

This second book also provided an opportunity to elaborate on several topics that we didn't have time to cover in the first book. *Rise of the Machines* will also examine how Zero Trust can play a role in critical issues like mergers and acquisitions, business continuity and disaster recovery, endpoint protections, regulation and compliance, ethics, certifications, and culture. All of these issues will also be impacted by AI as time goes on.

We are still in the early days of AI, and we should expect changes to occur at an exponential rate. This makes getting security right for AI systems right today is critical in order to secure our collective future.

Rise of the Machines: A Project Zero Trust Story is an essential read for professionals who are new to technology, as well as seasoned IT leaders, executives, and cybersecurity practitioners who need to understand how to protect their organizations while adopting AI to help their organizations remain competitive. *Rise of the Machines* demonstrates how Zero Trust can be integrated into any organization adopting AI using easy-to-understand examples, bridging the gap between technical reference guides, vendor marketing, and organizational strategy.

CHAPTER

1

AI-pocalypse Now

The alarm for Dylan's smartphone went off again. He had snoozed it several times already, but this time, he dismissed it altogether. He only had 60 seconds before he was supposed to go to the biggest interview of his life. The Cloud Security Alliance was hosting its annual conference for chief information security officers (CISOs). And the keynote speech this year would be a fireside chat with Dylan, CISO for MarchFit. Dylan had successfully led MarchFit's initial implementation of Zero Trust after a ransomware incident and then became their CISO.

From backstage, Dylan could see the crowd of about 200 CISOs in a ballroom that could have contained the entire MarchFit headquarters. The first rows were filled with couches for the VIPs, then rows and rows of chairs filled with some of the most successful CISOs in the world, with hundreds of years of experience collectively. At the back of the conference were even more security leaders standing up.

Dylan hadn't been a CISO for very long. He had been in technology for years but had unexpectedly found himself doing security for his company, MarchFit. His team hadn't just implemented Zero Trust—they helped foil a cybercriminal from getting back into their network after the breach.

From Dylan's perspective, none of that explained how he was about to give the biggest presentation of his life. He finally understood why everyone says their number-one fear is public speaking. But he had seen firsthand how much of a difference Zero Trust had made, so he hoped he could help make things easier for someone else.

Backstage, there was a monitor that allowed Dylan to see the stage from the audience's perspective. There were two leather wingback chairs and a table between them, with two bottles of water on the main stage next to a plexiglass podium. Behind the chairs was a giant video screen displaying a loop of an ornate fireplace with a roaring fire.

The conference emcee had silently walked up behind Dylan and patted him on the shoulder. He was startled until he recognized her. She was the reporter who had interviewed his boss, MarchFit's founder, Olivia Reynolds, at the Consumer Electronics Show two years ago. He remembered her because afterward she had spent an hour grilling Dylan about cybersecurity as she had been working on an investigative piece around a group of nation-state actors and several large Bitcoin transactions. She nodded and gave Dylan a thumbs-up as she walked out to the lights on the stage.

"Hi, I'm Monica Stewart, and I'm a journalist," she began, pausing after some laughter among the crowd. "I know security people get nervous around reporters. But don't worry, I'm off duty, but if you have any leads on a good story, you can always reach me . . ." Again, she paused as the rest of the audience joined in the laughter. "When one of my security friends found out I was emceeing the event, they said, 'Monica, don't even bring your cell phone. It will get hacked.' But then the conference organizers require you to have the app to register, so I had to go back to my room to get it!" She paused, and a roar of laughter came from the crowd; she let the noise die back down before she continued.

"I know you're all probably tired of hearing about AI. So up next, we've got a fireside chat to talk about the second biggest buzzword in all of technology: Zero Trust." The crowd applauded with a hoot as the clapping started to fade.

"You can find the info for the guest Wi-Fi network on each of the tables in front of you. We'd like to ask that you please refrain from hacking the Wi-Fi network." She gave the audience a moment to allow the cheers to die down. "But seriously, we want to get invited back for this conference next year. And for the other half of our fireside chat," she continued, "we'd like to welcome Dylan Thomas, chief information security officer for MarchFit, to talk about their Zero Trust journey."

Dylan walked in from the opposite side of the stage as the crowd and joined Monica. They sat down across from each other.

"Thanks, Monica," Dylan said. "I got a Faraday cage for my phone just for this event." The crowd cheered at this.

Monica smiled and steepled her fingertips. "Dylan," she began as a hush went over the crowd, "you've come into some notoriety lately for how your company was able to stop a cybercriminal by using a technique called Zero Trust. Some of the people here might not know what that is. How would you explain that to someone who has never used a computer?"

Dylan cleared his throat nervously, attempting to smile back at Monica, but it probably looked like he needed to sneeze. This wasn't one of the questions they had prepared for.

Dylan thought back to a conversation he had with one of his colleagues, Rose, a few weeks ago. She was the person who helped bring down the cybercriminal

Encore, aka Richard Greyson. Greyson thought he could intimidate her into giving him access into MarchFit's network after they had launched their Zero Trust project. He didn't realize she was a Brazilian jiu-jitsu practitioner and wasn't going to be intimidated by anyone.

"Zero Trust is like kung fu," Dylan began. "Before we get into a debate about whether Brazilian jiu-jitsu or Krav Maga is better, I'm just using 'kung fu' as a general term for the personal discipline involved in mastering a martial art. Zero Trust is the discipline of protecting yourself and your community in the cyber world. The cybercriminals need trust to disrupt our businesses."

"Thanks, Dylan, that makes a lot of sense," Monica said. "I can see how there may be a lot of different definitions of Zero Trust. What's your technical definition?"

Dylan explained, "Zero Trust is a strategy for preventing or containing breaches by removing the trust relationships we have in digital systems. Every business leader knows that a strategy is critical for success in any part of the organization, and that's why Zero Trust resonates so much with them. We know from studying successful breaches that the thing the cybercriminals need to get in is trust. Hence the name, Zero Trust. And we need a strategy because everyone in our company needs to be on the same page about how we're going to accomplish that. Zero Trust is like a rallying cry, getting everyone moving in the same direction."

"Sounds expensive!" Monica said.

"It doesn't have to be!" Dylan laughed easily. He had heard that kind of criticism of cybersecurity over the years. "You've probably heard the old adage that an ounce of prevention is worth a pound of cure. Because we focus on preventing bad things from happening, we know that Zero Trust is the most cost-effective strategy for securing our organizations. It's much cheaper than paying millions in a ransomware incident or losing clients to a competitor because we didn't get security right. You don't necessarily need to go out and buy a bunch of new tools to make that happen. Sometimes you can even reduce the number of tools you use and simply deploy them more effectively with Zero Trust."

"But don't we need to trust our employees?" Monica asked.

"Our adversaries don't have the element of surprise anymore. We know what they're after: money, information, secrets. We also know how they get it. No matter what technology you use or what industry you're in or what role you may play in your organization, the one common denominator of the thing that attackers exploit is trust. We've evolved our defense to focus on trust relationships in digital systems. But Zero Trust is about removing trust relationships from digital systems. We need to trust our people to work together as a team to achieve our mission of Zero Trust."

"Thanks for clarifying that, Dylan," Monica said. "But so far at least, I'm not hearing a lot of specifics. Usually with a strategy like this, I'd expect to see some design principles."

"I think we have a slide prepared that might help with this," Dylan said. The fireplace behind Monica and Dylan was replaced with a black slide and a bulleted list:

Principles of Zero Trust

- Focus on business outcomes.
- Design from the inside out.
- Determine who or what needs access.
- Inspect and log all traffic.

Dylan took a sip of water and continued: "I love that Zero Trust starts with understanding the specific business you work for. Different companies or different risk appetites. They use technology in different ways. They have different ways of making money. The security industry has talked about aligning the businesses with security for years, and this was the first principle of Zero Trust from the beginning."

Monica was nodding along, so Dylan continued. "The next principle is that we need to architect our organizations like jawbreakers instead of M&Ms. We can't be crunchy on the outside and chewy in the middle. They should be hard all the way through, and the best way to do that is by starting from the middle, with your crown jewels, and working your way out from there. A lot of people correlate microsegmentation or deperimeterization with Zero Trust, and that falls under this principle."

"I love jawbreakers. But not everyone has the patience for them," Monica said, getting a chuckle from the crowd.

"Knowing how your business works means narrowly tailoring your security to the organization," Dylan continued, "so you need to know both the human and nonhuman identities and use least privilege to provide granular access to everything. And we'll regularly review if people still need access to that data or have expiration dates on certain privileges."

Monica was looking thoughtful, so Dylan paused, but when the reporter didn't ask a question, he continued. "We know the first thing that cybercriminals do when they get in is to cover their tracks. Since we assume we're going to be breached with Zero Trust, we know we'll need to capture everything so that we can be successful at containment. The worst question to get from a board member is 'How did this happen?' when you don't have the logs to be able to answer the question."

"I feel like I'm starting to understand cybersecurity, which is really scary," Monica admitted. "These principles are great, but how can the CISOs in the room go back to their organizations and actually take the first steps on their own Zero Trust projects?"

Dylan used that moment to take a deep breath. "I just happen to have a slide for that as well," he said, getting several laughs and a few claps from different parts of the audience. A second slide appeared behind them, this showing a new list that read:

Zero Trust Methodology

- Define your protect surface.
- Map transaction flows.
- Architect your environment.
- Create Zero Trust policies.
- Monitor and maintain.

"After John Kindervag coined the phrase Zero Trust, he spent the next decade and a half doing strategic security consulting for businesses all over the world. And he didn't want to just swoop in for a week and leave. He needed a repeatable methodology that covered all the different aspects of a Zero Trust initiative so that organizations could sustain their progress and measure their maturity. These five steps are his methodology."

"What's a protect surface?" Monica asked. "That sounds like a new dance move that's taking nightclubs by storm."

"Think of it like a safe you're putting your crown jewels into. You might have 10 or 20 different safes of different sizes. The safes might have better and better locks depending on how important the contents are. And typically, you'd put all your credit card numbers in one specific safe, not all of them. If someone breaks in, you've limited them to getting what's in just one of those safes."

"That makes sense," Monica said. "It's like that microsegmentation concept you mentioned earlier."

"Exactly. But starting with the protect surface, you'll build an interdisciplinary team of everyone who plays a role in securing that protect surface. Your firewall admin, your antivirus analyst, your server admins, your developers, and the identity team should all be engaged so that they can coordinate their efforts more effectively."

"Am I right that the ransomware gang hit on your first day?" Monica asked. "What are some surprising things you learned on the way?"

"Yes, it's true," Dylan replied. "It seems obvious to say this, but I think the most important thing I realized is that you can't be one click away from going out of business. With Zero Trust, instead of asking what went wrong after the fact and attempting to fix it, we ask what needs to go right for the business to succeed and then ensuring what must go right goes right. We're moving away from firefighting each incident toward problem management by asking what the root causes of those incidents are. There's no concept of unknown traffic. If something is unknown, it's blocked."

"I read a lot about Zero Trust architecture to prepare for this interview, so I'm surprised that you haven't talked about architecture at all," Monica said.