FORTRA™

# What Six Cybersecurity Pros Think of Zero Trust Today

Zero trust isn't a new model, but its influence on the cybersecurity industry has grown over time. Coined by computer scientist Stephen Paul Marsh in 1994 and widely popularized by Forrester analyst John Kindervag from 2010 onward, the zero trust model — sometimes called zero trust architecture — promotes the rigorous validation of information.[1] Implicit trust in any devices or users is discouraged.

Zero trust became especially top-of-mind a decade later when remote work and cloud services took off, prompting organizational leaders to rethink the way they enforced cybersecurity controls in an increasingly perimeter-less world.

Is zero trust just another cybersecurity buzzword? What does zero trust look like in practice when implemented successfully? What are its challenges and limits?

**To answer these questions and more, Fortra surveyed six top cybersecurity professionals to weigh in with their insights on zero trust.**

## WHAT IS ZERO TRUST?

*A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.*[2]

— National Institute of Standards and Technology (NIST)

# MEET THE EXPERTS

**ANGUS MACRAE**
**Head of Cyber Security**
*King's Service Center*

**HUNTER SEKARA**
**Cybersecurity Engineer**
*CACI International*

**ANTONIO SANCHEZ**
**Principal Evangelist**
*Fortra*

**JOHN GRANCARICH**
**Chief Strategy Officer**
*Fortra*

**GARY HIBBERD**
**Professor of Communicating Cyber**
*Consultants Like Us*

**KURT THOMAS**
**Senior System Engineer**
*Fortra*

# IS THE HYPE AROUND ZERO TRUST JUSTIFIED?

## ANTONIO SANCHEZ

Zero trust is a mindset of guiding principles that has been around long before the world was forced into remote working. The technology that surfaced for me in recent years was user behavior anomaly detection (UBAD). As part of a zero trust strategy, users have to authenticate — most likely with multi-factor authentication — in order to access their organization's network. However, just because a person was able to successfully authenticate doesn't mean they should be completely trusted. UBAD creates a baseline of activity for each user, and once the user deviates from the baseline, that anomaly is surfaced for further inspection.

A common example would be an executive that normally logs in from Canada suddenly logging in from Japan. That's an anomaly, but not necessarily something malicious, as the executive may be traveling for business. If, however, the executive logs in from Spain just a few moments later, the UBAD solution will determine this anomaly to be malicious due to the impossibility of legitimate travel time, and the user credentials would then be disabled.

## ANGUS MACRAE

Yes and no. The pandemic most certainly accelerated the journeys of change and digital transformation already underway in most organizations: in particular, the adoption and now reliance upon public cloud and remote working. The old-world security perimeters were already little more than an illusion and the mass switch to remote working and cloud just helped to emphasize that.

But whilst most organizations should hopefully be using at least some elements and components of zero trust in their remote working solutions, remote working in and of itself does not of course equal a zero trust architecture.

## KURT THOMAS

The move to hybrid work meant a big shift for many organizations, which for various sociological, cultural, and technological reasons had their employees work primarily from company premises. The effect of the Covid-19 pandemic was that so that many organizations had to increase their capability to support remote work drastically, and in a short time.

Those organizations owe a lot to their IT teams, who in many cases designed and implemented massive changes to IT in months, or even weeks. To the degree that a zero trust approach had already been taken, their work was simplified. In other cases, zero trust allowed those organizations to preserve security even where it was not possible to establish or to readjust VPN connectivity in the short time available.

## GARY HIBBERD

In a word, yes. When organizations moved to remote working, for many it was a cultural shift that caused a strain on technology and people. People who had traditionally been given a mobile device because their position demanded it had to learn how to log in from home. VPN and network bandwidth was strained, along with the lack of available devices. For people management, we pushed people, data, and technology so far away from a central locus of control that it put people, data, and organizations at risk.

# *WHAT ARE SOME OF THE BIGGEST CHALLENGES IN ZERO TRUST, AND HOW DO YOU OVERCOME THEM?*

## HUNTER SEKARA

The greatest challenge with zero trust is understanding what it means to the organization, why we should pursue it, and how it fits into the mission or business processes. Foundational security principles influencing trust, such as least privilege, least functionality, and complete mediation, have existed for decades. In an industry known for adopting and promoting the latest buzzwords, organizations should exercise caution before spending six to seven figures on potential solutions for a problem that may or may not exist.

The key to addressing these concerns before making a zero trust decision is understanding the "how, what, why, and when." How is this different from our existing security measures in place? What are the benefits to the organization? If we are not already implementing these security controls, why? Lastly, when do we believe the organization is mature enough for proper implementation? Techniques such as a business impact analysis, risk assessment, and gap analysis can help facilitate informed decision-making for a zero trust expenditure.

## GARY HIBBERD

There are three aspects of information security that I always talk about: people, process, and technology. The biggest challenge with zero trust touches all of them. Zero trust requires changes to existing security infrastructure, including investing in new security infrastructure such as identity and access management (IAM) solutions, cloud security posture management (CSPM) solutions, and network segmentation tools. Business changes may also be impacted, as zero trust may change how personnel access data and applications. Therefore, it impacts those personnel and how they use systems.

I have overcome these challenges by being very clear on what we mean by zero trust and ensuring we have a clear project in place with senior leadership support and buy-in. This is then communicated to personnel with a clear test project in mind. This becomes the proof of concept, which is then rolled out across the rest of the organization.

## ANGUS MACRAE

The challenges will be multiple, ranging from cultural and organizational to financial and technological. The biggest mistake will be rushing to some major technology change without a true understanding of all the digital assets, as well as evaluating existing complex infrastructure and business data flow. Technology-wise, one of the biggest challenges will be legacy systems and business processes that were built in a different era and are not able to be replaced easily. A good approach will be to plan stages in alignment with the NIST Risk Management Framework.

One of the first real challenges, however, is ensuring people actually understand what zero trust is and what it isn't. For this, I refer you to NIST SP 800-207 which states: "*Zero trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different — or no more trustworthy — than any non enterprise-owned environment. In this new paradigm, an enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks.*"

# *WHAT KIND OF TECHNOLOGY HAS HELPED YOU ON YOUR JOURNEY TO ZERO TRUST, AND WHAT IMPORTANT INSIGHTS CAN YOU SHARE REGARDING IMPLEMENTING SUCCESSFUL PROCESSES?*

## ANGUS MACRAE

Technologies that genuinely leverage the vital components of a zero trust architecture, i.e., those that have a policy engine, a policy administrator, and policy enforcement points. All data sources and computing services must now be considered resources, and all communication must be secured regardless of network location. This will likely require multiple levels of technology to get right across large and complex organizations. True telemetry across the layers becomes more important than ever in getting the right data to execute the right policy decisions.

At the end of the day, it's not about a product simply marketed as zero trust; it's about leveraging good technology stacks to create the building blocks of enhanced identity governance, micro-segmentation, and ultimately software-defined perimeters. Processes have to be constantly reviewed and security models need to move to a more dynamic state of 'never trust — always verify, explicitly,' and operate under the assumption of a data breach.

Not all enterprise resources will reside on enterprise-owned infrastructure and devices on 'the network' may no longer be owned or configurable by the organization. Every asset must therefore have its security posture evaluated at the time of request by a policy enforcement point.

## GARY HIBBERD

Not wishing to call out one system over another, I would simply say identity and access management (IAM) solutions help organizations manage who has access to what resources and under what conditions. This is essential for zero trust, as it allows organizations to control who can access their systems and data, even if they are already inside the network. Data loss prevention (DLP) tools are important to help organizations prevent sensitive data from being exfiltrated from their networks. This is important for zero trust, as it helps to protect sensitive data from unauthorized access.

# *WHAT DOES THE FUTURE OF ZERO TRUST LOOK LIKE? WHERE DO WE GO NEXT AS AN INDUSTRY?*

## JOHN GRANCARICH

The future of zero trust — what it should become — I think looks relatively straightforward; users are authenticating and being authorized with every connection they make in order to limit an attacker's lateral movement in the event of a successful breach. What's less obvious is how we are going to achieve this not just across identity and networks, but also across devices, applications, and data.

This is part of the key to systematically implementing zero trust over time: Organizations need to start by understanding which specific assets they most want to protect and why, which asset category they fall into, and then what specific zero trust controls and monitoring solutions need to be implemented to achieve that across those selected asset classes. A well-designed, phased approach to this should increase internal communication and alignment across the three key constituencies: business, IT, and security.

## ANGUS MACRAE

Very few organizations I'm aware of yet run a true zero trust architecture end-to-end. Whilst many are in some state of transition toward that, for most of us it's going to be an evolution rather than a revolution.

Conceptually, it will also take a rethink in traditional risk management in that no organizational resource or area should be inherently trusted. There isn't a magic set of tools you can buy or a set of compliance metrics you follow that mean your organization can pride itself as secure. Instead, your security model now has to continually operate with the altogether more realistic assumption that an adversary already has a presence within your organization and that nothing should be implicitly trusted. Everything must be verified continually.

This is a more complex and, in some ways, far less comforting message to those who may not really understand the truer picture of security, threat, and zero trust. But to quote an old traditional maxim, "Take the world as it is, not as it ought to be."

## GARY HIBBERD

There will be an increased adoption of cloud-based security solutions, as they can be easily scaled and updated to meet the changing needs of organizations. It is almost impossible to escape the rise of AI and machine learning, as these will be used to improve the effectiveness of zero trust deployments and to identify and respond to threats more quickly and accurately.

# CAN ZERO TRUST MEAN CONFIDENCE?

## KURT THOMAS

Zero trust can mean different things. Used in the widest sense of the term, it is a re-establishment of the old 'least privilege' approach. This is the best approach that you can take for security because it minimizes the attack surface, and what's not to like in that? The only reason that approach was not adopted more widely in the past is a sense of inertia, of sticking one's head in the sand. Well, we don't live in a world anymore where that kind of approach would be sustainable. An organization that allows everyone and every process to do everything is an organization asking for disaster. It's like leaving the door to the safe open.

The least privilege approach originated in the military, which has been used to dealing with adversaries for a long, long time. The military had processes in place to secure the confidentiality, integrity, and availability of information and physical goods. I am not saying they were perfect processes, but something was in place. This was zero trust before computers, when secrets existed primarily on paper or in spoken conversations.

When computers came along, a lot of their use was in academia and related to specialists, and that created a natural protection for them. Few people had a reason to mess with computers, and even fewer would have known how to do it. That has changed drastically, and now the kind of approaches to security that were prevalent in the military are being applied to the world of computers. In that sense of the term, zero trust isn't going away, because the underlying requirement to protect data in a hostile environment is here to stay. Does zero trust equal confidence? No, but I would argue that zero trust in the broad sense of the term is a condition for confidence.

## GARY HIBBERD

I don't believe that it can. In fact, the idea of zero trust may lull us into a false sense of security. There is a saying, "In screen we trust," meaning that we will trust what is presented on the screen. Can we ever have full confidence in technology and say with absolute certainty that we can trust it? I don't think so. This is why I prefer the 'trust, but verify' principle.

Ultimately, zero trust is about creating a security posture that is based on trust, not perimeters. By continuously verifying the identity of users and devices, and by granting access only on a need-to-know basis, organizations can significantly reduce their risk of cyberattacks.

## ANGUS MACRAE

In a word, no, but for context on this question, again, I refer back to a Voltaire quote I used in a 2020 Tripwire blog: "Doubt is an unpleasant condition, but certainty is an absurd one." That is, if you have some complete, and implicit confidence in zero trust, or a perimeter-based model or any other security implementation for that matter, then you are missing the point. By the very metamorphic nature of security and threat itself, you may soon find yourself sadly deluded. A properly developed and maintained zero trust architecture will, however, reduce overall cyber risk and protect against common threats.

***"Doubt is an unpleasant condition, but certainty is an absurd one."***

— Voltaire

## WHAT'S NEXT?

There is no consensus in the cybersecurity community on a single, definite route to implementing zero trust. However, its underlying tenets are generally agreed on, and the zero trust model is evolving as a major component of successful cybersecurity strategies.

Have you implemented the zero trust model in your own organization? Whether your implementation is just getting started or already well on its way, you can trust Fortra as your relentless ally through every step of your cybersecurity journey.

**Learn how Fortra can help you with your zero trust strategy at fortra.com.**

**Sources**

1. https://venturebeat.com/security/zero-trust-architecture/
2. https://csrc.nist.gov/glossary/term/zero_trust

FORTRA™

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.



fta-tw-gd-1123-r1-hm