CISO MAG

beyond cybersecurity

Volume 5 | Issue 12 | December 2021

## To Evolve Zero Trust, We Need to Adopt It and Deploy It

John Kindervag

Senior Vice President Cybersecurity Strategy

**ON2IT and ON2IT Global Fellow**

UNDER THE SPOTLIGHT

32

# 2021 A Moonshot Year for Adversaries

CISO MAG

beyond cybersecurity

# EDITORIAL ADVISORY BOARD

CISO MAG established an **Editorial Advisory Board** with the foremost innovators and thought leaders in the cybersecurity space. Board members offer the CISO MAG editors advice regarding the magazine as well as suggest the strategic direction it should follow. It includes shaping our editorial content, identifying important topics and special issues, moderating discussions, vetting technical content, and updating the magazine's presence by creating and implementing different initiatives.

The Advisory Board members are "**active**" participants and contribute to CISO MAG regularly. They contribute in either of the following ways:

- Editorial strategy
- Writing articles
- Exclusive quotes for editorial stories
- Vetting surveys and technical content
- Podcasts, webinars, video, and text interviews

## Carolyn Crandall

Chief Security Advocate
**Attivo Networks**

Carolyn Crandall is the Chief Security Advocate at Attivo Networks, the leader in preventing identity privilege escalation and detecting lateral movement attacks. She has worked in high-tech for over 30 years and has been recognized as a top 100 women in cybersecurity, a guest on Fox News, and profiled in the Mercury News. She is an active speaker on security innovation at CISO forums, industry events, and technology education webinars. Carolyn also co-authored the book *Deception-Based Threat Detection: Shifting Power to the Defenders.*

## Vandana Verma

Security Relations Leader
**Snyk**

Vandana is a Security Relations Leader at Snyk with a current focus on DevSecOps. She has extensive experience in Application Security, Vulnerability Management, SOC, Infrastructure Security and Cloud Security. Vandana is a seasoned speaker and trainer. She presented at various public events ranging from Global OWASP AppSec events to BlackHat events, to regional events such as BSides events in India. She is on the OWASP Global Board of directors (Vice-Chair). She also works in various communities towards diversity initiatives such as InfosecGirls, InfosecKids and WoSec. She is a recipient of multiple awards and is listed as one of the top women leaders in technology and cybersecurity in India by Instasafe.

## Favour Femi-Oyewole

Global Chief Information Security Officer (CISO)
**Access Bank Plc.**

Favour Femi-Oyewole has over 23 years of experience managing all aspects of Information Technology with vast knowledge in Enterprise IT Security, Information Technology, IT Governance, Information Security best practices, Cyber Security, Business Continuity, and Risk Management, especially in dynamic, demanding large scale environments. She is also regarded as the first female COBIT 5 Assessor certified in Africa, the first female in Africa to be a Blockchain Certified Professional, and the first woman to win the Global Certified CISO (C|CISO) of the Year 2017. She is a Certified ISO 27001:2013 Lead Implementer Trainer and an Alumni of Harvard Kennedy School (HKS) - Harvard University and Massachusetts Institute of Technology (MIT). She is a member of the Cybercrime Advisory Council in Nigeria with the Mandate of implementing Cybersecurity for all sectors in Nigeria and the pioneer Chair of the Standard and Evaluations Committee. She is a Fellow of the British Computer Society (BCS), The Chartered Institute for IT. She serves as a member of the Global C|CISO Advisory Board and the Information Security woman of the Year 2021 in Nigeria.

## Dr. Charlotte M. Farmer

Independent Director

Charlotte is an experienced Director and Board Member with proven value creation across blue chip companies and top-tier general management consulting firms. Over the last 25 years, she has served as Board Chair, Committee Chair, or Board Advisor to 16 non-governmental organization (NGO) boards. Currently, she serves as Board Chair of a tech start-up and advisor to a private equity company in The Carlyle Group portfolio. Her board expertise includes strategy, governance, and turnaround with proven results building high-performing, growth organizations. Her leadership roles in high-tech manufacturing, global operations, finance, and digital transformation would also be an asset to companies eager to expand their footprint or companies in need of turnaround guidance.

## Tari Schreider

C|CISO, CRISC, MCRP, ITILF – Cybersecurity Architect, Author & C|CISO Instructor **EC-Council**

Tari Schreider - C|CISO, CRISC, MCRP, ITILf – is a Cybersecurity Architect, Author, Researcher, C|CISO Instructor at EC-Council, and Strategic Advisor at Aite-Novarica Group covering the cybersecurity industry. He is the author of two Amazon top sellers Building an Effective Cybersecurity Program and Cybersecurity Law, Standards and Regulations. He is also a cybersecurity strategist and C|CISO Master Course instructor passionate about making CISOs the smartest people in the room. Tari consults with organizations to guide the transformation of their cybersecurity programs to obtain regulatory compliance and stave off cyberattacks.

## Stan Meirzwa

M.S., CISSP, Director
**Kean University Center for Cybersecurity**

Stanley Mierzwa is the Director of, Center for Cybersecurity at Kean University in the United States. He lectures at Kean University on Cybersecurity Risk Management, Cyber Policy, Digital Crime and Terrorism, and Foundations in Cybersecurity. Stan has over 15 published research publications and is a peer reviewer for the International Journal of Cybersecurity Intelligence and Cybercrime, Online Journal of Public Health Informatics and an Editorial Review Board member for the International Association for Computer Information Systems. He is a Certified Information Systems Security Professional (CISSP) and member of several associations, including the FBI Infragard, IEEE, and (ISC)². He is a board member (Chief Technology Officer) of the global pharmacy education non-profit, Vennue Foundation. Stan holds an MS in Management with a specialization in Information Systems from the New Jersey Institute of Technology and a BS in Electrical Engineering Technology from Fairleigh Dickinson University.

## John Kindervag

Senior Vice President Cybersecurity Strategy
**ON2IT and ON2IT Global Fellow**

John Kindervag joined ON2IT in March of 2021 as Senior Vice President Cybersecurity Strategy and ON2IT Global Fellow. He spent the previous four years at Palo Alto Networks as Field CTO. Before Palo Alto Networks, John spent eight and one-half years at Forrester Research as a Vice President and Principal Analyst on the Security and Risk Team. John is considered one of the world's foremost cybersecurity experts. He is best known for creating the revolutionary Zero Trust Model of Cybersecurity.

## Zachery Mitcham

MSA, CCISO, CSIH, VP and Chief Information Security Officer, **SURGE Professional Services-Group**

Zachery S. Mitcham is a 20-year veteran of the United States Army where he retired as a Major. He earned his BBA in Business Administration from Mercer University Eugene W. Stetson School of Business and Economics. He also earned an MSA in Administration from Central Michigan University. Zachery graduated from the United States Army School of Information Technology where he earned a diploma with a concentration in systems automation. He completed a graduate studies professional development program earning a Strategic Management Graduate Certificate at Harvard University extension school. Mr. Mitcham holds several computer security certificates from various institutions of higher education to include Stanford, Villanova, Carnegie-Mellon Universities, and the University of Central Florida. He is certified as a Chief Information Security Officer by the EC-Council and a Certified Computer Security Incident Handler from the Software Engineering Institute at Carnegie Mellon University. Zachery received his Information Systems Security Management credentials as an Information Systems Security Officer from the Department of Defense Intelligence Information Systems Accreditations Course in Kaiserslautern, Germany.

## Muhammad Tariq Ahmed Khan

Head of Information Security Audit,
Internal Audit Department, **Riyad Bank, KSA.**

Muhammad Tariq Ahmed Khan is Head of Information Security Audit, Internal Audit Division, Riyad Bank, KSA. He has over 21 years of experience in the Banking industry, in areas such as Information Technology, Cyber & Information Security, Business Continuity Management & Disaster Recovery and related Audits. He has a solid understanding and application of Risk-Based Audit methodology, ISMS (ISO 27001), ISO 22301, NIST and COBIT, IT & Information Security regulatory compliance.

He is a double Graduate (Finance and Computer Science) with one Master's Degree in Computer Science. In addition, he holds a number of professional certifications such as CISA, CISM, CRISC, CDPSE, CISSP, PMP, CEH, ISO 27001 ISMS Lead Implementer & ISO 22301 BCMS.

Tariq has published articles on different topics of Cyber & Information Security and IT Audit and also spoken at regional and international seminars and conferences.

## Narendra Sahoo

Founder and Director, **VISTA InfoSec**

Narendra Sahoo (PCI QSA, PCI QPA, PCI SSFA, CISSP, CISA, CRISC and CEH) is the Founder and Director of VISTA InfoSec, a global Information Security Consulting firm, based in the U.S., UK, Singapore & India. Mr. Sahoo holds more than 25 years of experience in the IT Industry, with expertise in CyberSecurity Risk Consulting, Assessment, and Compliance services. VISTA InfoSec specializes in Cyber Security audit, consulting, and certification services which include PCI DSS Compliance & Audit, PCI PIN, PCI SSF, SOC1/2, GDPR Compliance and Audit, HIPAA, CCPA, NESA, MAS-TRM, PDPA, PDPB to name a few. The company has for years (since 2004) worked with organizations across the globe to address the Regulatory and Information Security challenges in their industry. VISTA InfoSec has been instrumental in helping top multinational companies achieve compliance and secure their IT infrastructure.

## Sunil Varkey

VP
**Forescout**

Sunil Varkey has over 26 years of Security leadership experience, with large global corporates in banking, telecoms, ITES, software, and manufacturing. At Forescout he is involved in security strategy, innovation, and stakeholder engagements, prior to this he led Cyber Security Assessment and Testing for HSBC, he also worked with Symantec as CTO and Strategist, Wipro as Global CISO and Fellow, as Head of Security and Privacy at Idea Cellular, and in GE, Barclays and SABB.

## AJ Yawn

Founder and CEO
**ByteChek**

AJ Yawn is a seasoned cloud security professional that possesses over a decade of senior information security experience with extensive experience managing a wide range of cybersecurity compliance assessments (SOC 2, ISO 27001, HIPAA, etc.) for a variety of SaaS, IaaS, and PaaS providers. AJ is a SANS Institute instructor and currently teaches the SEC557: Continuous Automation for Enterprise and Cloud Compliance.

AJ is a Founding Board member of the National Association of Black Compliance and Risk Management professions, regularly speaks on information security podcasts, events, and he contributes blogs and articles to the information security community including publications such as CISOMag, InfosecMag, HackerNoon, and (ISC)².

## Dick Wilkinson

Chief Technology Officer
**Proof Labs**

Dick Wilkinson is the Chief Technology Officer at Proof Labs. He also served as the CTO on staff with the Supreme Court of New Mexico. He is a retired Army Warrant Officer with 20 years of experience in the intelligence and cybersecurity field. He has led diverse technical missions ranging from satellite operations, combat field digital forensics, enterprise cybersecurity as well as cyber research for the Secretary of Defense.

## Christina Gagnier

Shareholder
**Carlton Fields' Los Angeles office**

Christina Gagnier, a shareholder in Carlton Fields' Los Angeles office, is an experienced technology lawyer whose practice focuses on cybersecurity and privacy, blockchain technology, international regulatory affairs, technology transactions, and intellectual property. She advises clients on digital strategy to help them navigate uncharted legal territory, and guides a variety of technology companies and consumer brands through emerging legal and policy issues such as digital currency, the sharing economy, network neutrality, and the ever-changing area of consumer privacy law.

Christina has served on notable committees and task forces, including the Federal Communication Commission's Consumer Advisory Committee and the California attorney general's Cyber Exploitation Task Force. Outside her practice, Christina is an adjunct professor at the University of California, Irvine School of Law, where she serves as clinical faculty for the Intellectual Property, Arts, and Technology Clinic.

EC-Council

# CAPTURE THE FLAG

## Get CodeRed's Bestselling Learning Bundle for Just $29.99

With Capture the Flag (CTF) courses on CodeRed, EC-Council's continuous learning platform, you will learn with a walkthrough how to footprint a target, enumerate the target for possible vulnerabilities, analyze the vulnerabilities, and exploit the target to gain root access.

**Grab this Learning Bundle for $29.99**

## Courses in This Learning Bundle

Ethical Hacking -
Capture the Flag Walkthroughs – v1

Ethical Hacking -
Capture the Flag Walkthroughs – v2

Ethical Hacking -
Capture the Flag Walkthroughs – v3

## What You'll Learn

- Scanning, footprinting, and recon
- Enumeration and gaining access
- Exploitation and privilege escalation
- Cover tracks and plant backdoors
- SQL Injection to Shell
- Learn about CTF exercises
- Build your own virtual lab environment
- Learn basic to advance level Pentesting
- Capture the Flags using various tools

**Get Started Now for Just $29.99**

Cyber Talks

EC-Council

# Best Threat Hunting Practices for Security Operations Centers

WEDNESDAY
DECEMBER 8, 2021

9:00 AM CST / 8:00 AM MST /
10:00 AM EST / 8:30 PM IST

**Mike Miller**
vCISO - Chief Information Security Officer
**Cyber Protection Group**

**Joshua Copeland**
SOC Director
**ATT**

**Lee Thomas**
Sr. Director of Cybersecurity Operations
**L2 Cyber Security**

REGISTER NOW

Cyber Talks

EC-Council

# Can Current Security Awareness Programs Help Mitigate Vulnerabilities Caused by Human Factors?

THURSDAY
DECEMBER 9, 2021

9:00 AM EST / 3:00 PM CET /
7:30 PM IST

**Sachin Jain**
CEO & CTO
**Cognyse**

REGISTER NOW

Cyber Talks

EC-Council

Join us for the webinar on

# How Modernizing Incident Response Processes Can Help Stop Cybercrime

**Friday,**
JANUARY 21, 2022

**10:00 AM EST / 4:00 PM CET / 7:30 PM IST**

SPEAKER
**Paul Caron**
Senior Director,
Incident Response
**Arete Incident Response**

**Register Now**

Cyber Talks

EC-Council

# What Makes SOCaaS Essential in the Current Cyber Threat Landscape?

SPEAKER

**Reagan Short**
Security Operations Technical Director
**BlueVoyant**

THURSDAY
JANUARY 27, 2022

9:00 AM CST / 4:00 PM CET /
8:30 PM IST

SPEAKER

**Christopher Russell**
CISO
**tZERO Group**

**REGISTER NOW**

CISO MAG
Cybersecurity Person of the Year

Every December, CISO MAG acknowledges and honors those who made significant contributions to the industry. These are individuals who have, over the years, been committed to bringing awareness into the realm of cybersecurity – to whom the information security industry is profoundly indebted.

The selection parameters include experience, contribution to industry, spreading cybersecurity awareness, authorship, speaking roles, awards & recognitions, innovations, influencer status, and patents.

The Cybersecurity Person of the Year is decided through an internal voting process involving CISO MAG editors.

This year we decided to have only one recognition. We did not have a list of nominees and other finalists.

We are proud to announce that **John Kindervag** is the **CISO MAG Cybersecurity Person of the Year (2021)**.

# JOHN KINDERVAG

John Kindervag is Senior Vice President Cybersecurity Strategy, ON2IT, and ON2IT Global Fellow. He is  considered one of the world's foremost cybersecurity experts. Kindervag is best known for creating the revolutionary **Zero-Trust Model** of Cybersecurity.

Before ON2IT, he spent the previous four years at Palo Alto Networks as Field CTO. Before Palo Alto Networks, John spent eight and a half years at Forrester Research as a Vice President and Principal Analyst on the Security and Risk Team.

He is also on the U.S. President's NSTAC Zero-Trust and Trusted Identity Management Subcommittee (National Security Telecommunications Advisory Committee).

Kindervag devised the term Zero Trust in the fall of 2008 while at Forrester. Two years later, he moved to Palo Alto Research and completed a paper on zero trust titled, "*No More Chewy Centers: Introducing The Zero Trust Model Of Information Security.*" His blogs on this topic are widely read. He spoke about zero trust at many security conventions and meetups, and then it became an industry term.

Zero trust gained more significance when the pandemic came along, as everyone began to work from outside the organization.

We think Zero Trust was the biggest industry buzzword of 2021. The term is mentioned in most security conversations today; security practitioners speak about it at conferences, and  it is frequently mentioned in Board room discussions.

In May 2021, President Biden passed an Executive Order to improve the nation's cybersecurity. The order mandates that the Federal Government develop a plan to implement Zero-Trust Architecture (ZTA), which is mentioned in multiple sections within the Executive Order.

ZTA has changed how the world views cybersecurity today, and the credit for this goes to **John Kindervag**.

Kindervag has a practitioner background, having served as a security consultant, penetration tester, and security architect. He has been interviewed by numerous publications, including *The Wall Street Journal, Forbes, Bloomberg, and The New York Times*. He has also appeared on television networks such as *CNBC, Fox News, PBS, and Bloomberg*, discussing information security topics. John has spoken at many security conferences and events, including RSA, SXSW, ToorCon, ShmoCon, InfoSec Europe, and InfoSec World. Kindervag has a Bachelor of Arts degree in communications from the University of Iowa and lives in Dallas, TX.

Read our interview with John Kindervag in **Under the Spotlight** on page 32.

CISO MAG
beyond cybersecurity

Volume 5 | Issue 12
December 2021

President & CEO
**Jay Bavisi**

### Editorial

Director, Content & Editorial
**Cynthia Constantino***
cynthia.constantino@eccouncil.org

Editor-in-Chief
**Brian Pereira***
brian.p@eccouncil.org

Editorial Consultant
**Minu Sirsalewala**
minu.sirsalewala.ctr@eccouncil.org

Sub Editor
**Pooja Tikekar**
pooja.v@eccouncil.org

Sr. Feature Writer
**Rudra Srinivas**
rudra.s@eccouncil.org

Sr. Technical Writer
**Dr. Anuradha Nair**
anuradha.nair@eccouncil.org

### Management

Senior Vice President
**Karan Henrik**
karan.henrik@eccouncil.org

Director, Digital Marketing
**Mayur Prasad**
mayur.prasad@eccouncil.org

Senior Director
**Raj Kumar Vishwakarma**
rajkumar@eccouncil.org

Publishing Sales Manager
**Taruna Bose**
taruna.b@eccouncil.org

Asst. Manager Visualizer cum Graphic Designer
**Jeevana Rao Jinaga**
jeevana.r@eccouncil.org

Manager – Marketing and Operations
**Munazza Khan**
munazza.k@eccouncil.org

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,

The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & may not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.

EDITOR'S NOTE

# 'TIS THE SEASON TO BE PRUDENT

Brian Pereira

Editor-in-Chief

Another year draws to a close, and everyone is preparing for the holidays and the Christmas season. It is also the time to reflect on what happened during the year. In the same breath, I urge everyone to be extra cautious and not let their guard down. For 'tis is also the season for threat actors and hacking too!

This year, the attacks on users continue unabated, with phishing attacks getting sneakier and more sophisticated. We saw government and financial institutions being impacted by data breaches. Even industries such as manufacturing, health care, and education that were once not considered "lucrative" targets have now come within the crosshairs of adversaries.

Last year around December, there were many ransomware attacks on U.S. health care institutions. Health care and supply chain security are among the lowest-ranked domains for the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) conformance. But there could also be attacks on financial institutions and critical infrastructure, as we saw in the first quarter this year.

The CISO MAG editorial team tracked these events and incidents throughout the year. We report daily on breaches, attacks, and other trends. This time, every year, our editors pick the biggest stories in Cybersecurity, and you can read our selection in the **Cover Story** on page 62.

**CYBERSECURITY PERSON OF THE YEAR**

At the end of the year, we also acknowledge individuals in the cybersecurity industry. These are individuals who have, over the years, been committed to bringing awareness into the realm of cybersecurity – to whom the information security industry is profoundly indebted.

I am thrilled to announce that **John Kindervag** is the **CISO MAG Cybersecurity Person of the Year (2021)**. He is best known for creating the revolutionary **Zero-Trust Model** of Cybersecurity. Kindervag is Senior Vice President Cybersecurity Strategy, ON2IT, and ON2IT Global Fellow.

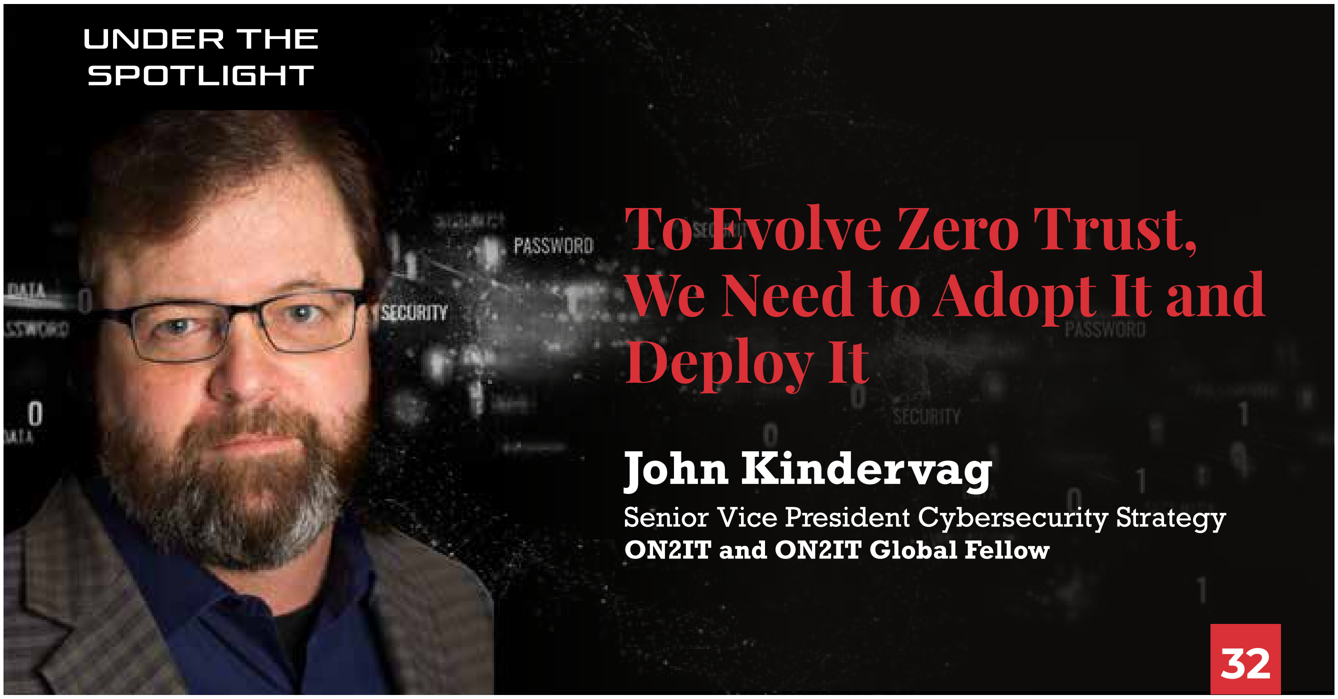
Zero-Trust Architecture has changed how the world views cybersecurity today, and the credit for this goes to Kindervag.

Read our interview with John Kindervag in **Under the Spotlight** on page 32.

I wish all our readers a Merry Christmas and a Happy New Year.

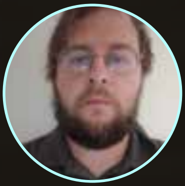
INDEX

# Contents



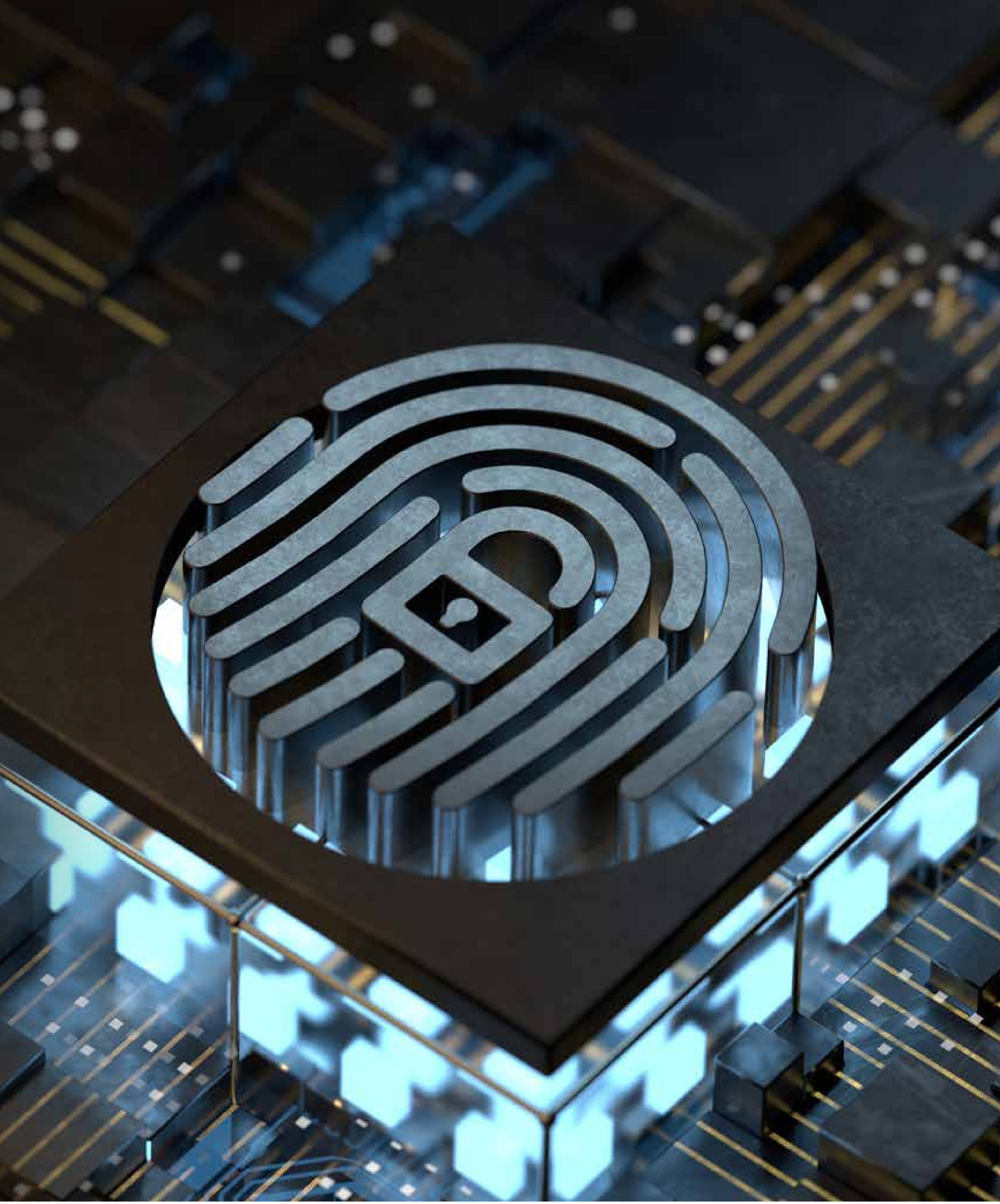
# ZTA - Don't Fear the Buzzword

**Dick Wilkinson**
Chief Technology Officer
**Proof Labs**



**Vincent Kelley**
Senior Cyber Transformation Architect
**Palo Alto Networks**

You can't attend a conference without seeing Zero-Trust Architecture (ZTA) mentioned in almost every presentation. Zero-Trust Architecture or ZTA has been around for quite a while but has finally captured the attention of the commercial IT sector. Zero trust has been promoted heavily by the U.S. National Security Agency. Recently, it has been established as the best way to secure the nation's infrastructure, both in the government and private sector[1]. This sudden popularity has created a profound buzzword status around the security architecture. It has sometimes led to a misunderstanding around what exactly ZTA is and how it can be deployed in your organization. As a CISO, we often bristle at buzzwords and fads and stick to our core competencies in security. Zero trust is more than just a buzzword and should not be seen as a sales gimmick. Every CISO needs to take a careful approach to analyze their risk and decide if a phased zero trust deployment makes sense. Here are some critical concepts to apply when thinking about your needs and if ZTA can improve your security posture.



## Critical Questions to Answer

Zero trust is set up as a series of five sequential steps. The ability to accurately and efficiently complete one step depends on the previous step's accuracy and completion. A good way to illustrate this is questions that should arise for each step in reverse order:

- How am I maintaining security for my critical resource(s)?
- What are the security products and capabilities that protect my critical resource(s)?
- Where are the security products located and, what should be the configuration for the capabilities?
- What are the transaction flows and elements of my critical resource(s) that need protection?
- What is the critical resource(s) I need to protect?

To answer these questions in order, you first would need to answer the question below it. For example, to know how you maintain security for a critical resource, you first need to determine what products and capabilities provide that security. Next, you must understand where these capabilities and security products are and how they should be configured. To answer this, you have to analyze the security and capabilities to protect your critical resource. Which leads to demanding the answer to the last question, "What is the critical resource I need to protect?"

## Five-Step Methodology

Zero trust, when approached as a sequential 5-step methodology, answers these questions in the correct order. This ensures the following step can be accomplished, then the one after, and so on. Until ultimately, you can answer definitively, "How am I maintaining security for my critical resource?"

### These five steps are:

*ry and Prioritization:* Define what
itical resource, identify what
n, and then prioritize
appropriate
med