Wilson Perumal & Company

OFFERING INTRODUCTION

HIGH RELIABILITY ZTNA

CYBERSECURITY IN A COMPLEX WORLD

Executive Summary

- Despite continued investment and huge market, political, and strategic emphasis—cybersecurity breaches are increasingly common and catastrophic
- A myriad of technology-based cybersecurity solutions and consultants have flooded the market—but **human errors still cause 95% of all cybersecurity incidents**
- In reaction to continued cybersecurity gaps, ZTNA (Zero Trust Network Access) has been heralded as the new solution to mitigate cybersecurity risk
  - If implemented as intended, **ZTNA significantly increases complexity**
  - This additional complexity increases both cyber risk and operational friction
- A holistic, practical, complexity-based ZTNA approach is needed to enhance cybersecurity without over-burdening IT operations and end users
  - **Each ZTNA deployment must be custom-designed** and optimized to fit the unique business strategy, risk tolerance, and operational constraints of each business
  - **ZTNA deployment must be paired with improved human performance within IT operations** to maintain, adapt, and continuously improve new cybersecurity mechanisms
  - **End users are the most common failure point for any cybersecurity approach—ZTNA deployments must focus on end users to ensure they do not bypass policies**
- WP&C is a leader in developing effective strategies that reduce complexity and improve human performance in high-risk enterprise environments

WP&C has deep experience helping companies address critical complexity and strategy issues

INDEPENDENT ADVISORS

Technology vendors and re-sellers make their money from implementation projects

WP&C is not a software reseller or implementer, offering an independent perspective

WP&C acts as a thought-partner to clients, shaping cybersecurity and vendor strategy with an unbiased perspective

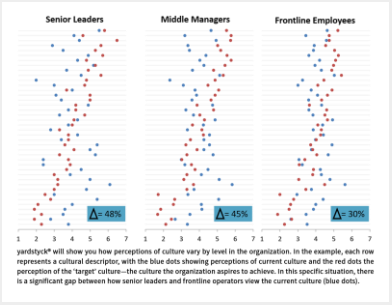
WP&C's Focus on Complexity

We partner with clients to help them better **compete in a complex world**, improving the customer experience, growth and profitability

Experienced Practitioners & Industry Expertise

We wrote the book on complexity and bring more cycles of experience

Industry-Proven Methods & Frameworks



WP&C's yardstyck® is a tool to **measure organizational culture**

OUR COMPLEXITY LENS CAN MITIGATE TECHNOLOGY RISKS

Technology connects processes and data—tech inherently adds complexity

Although technology naturally generates complexity, tech deployment offers an opportunity to vastly simplify process & data complexity

A complexity lens is required to mitigate increasing operational friction created by new technology

Increased investment in cybersecurity has not solved the problem of increasing cyber threats

INDUSTRY TREND #1

IT ecosystems are increasingly complicated

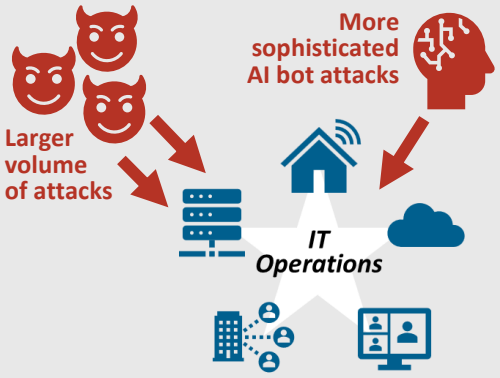
- Technology has become a key strategy enabler, resulting in businesses adding more software and IT infrastructure
- IT operations must manage increasingly complicated IT ecosystems
- There is a direct correlation between increasingly complicated IT operations and an increase in human errors

INTERNAL COMPLEXITY ↑

INDUSTRY TREND #2

Cyber threats require new security techniques

- Teleworking and the use of cloud-based software have created more potential points of attack
- Traditional perimeter-based security no longer protects a firm
- Businesses turn to ZTNA (Zero Trust Network Access) to reduce the risk that a bad actor could move freely within internal networks



EXTERNAL THREATS ↑

INDUSTRY TREND #3

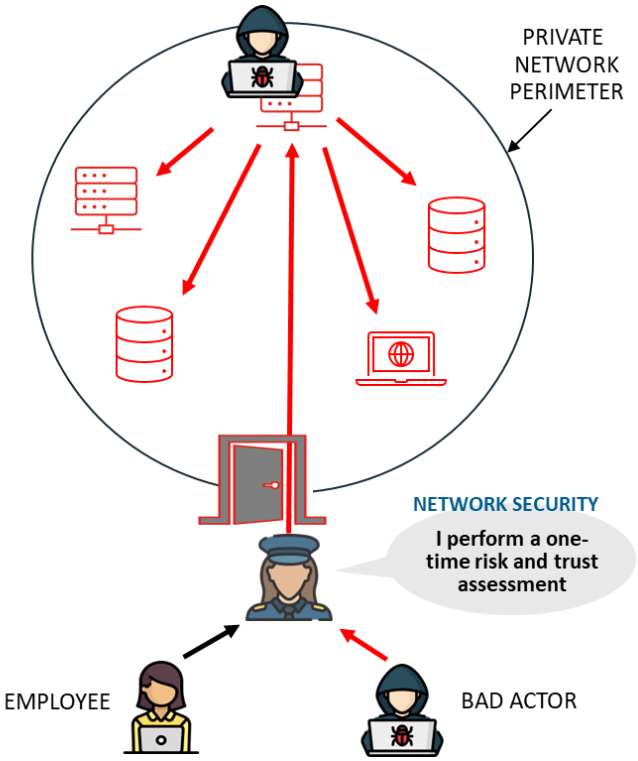
Human error is still the core gap in cybersecurity

- With more complicated IT operations and increasing threats, human error has become the leading cause of cybersecurity incidents
- This is further exacerbated by an industry-wide shortage of skilled cybersecurity professionals

ORG CAPABILITY ↓

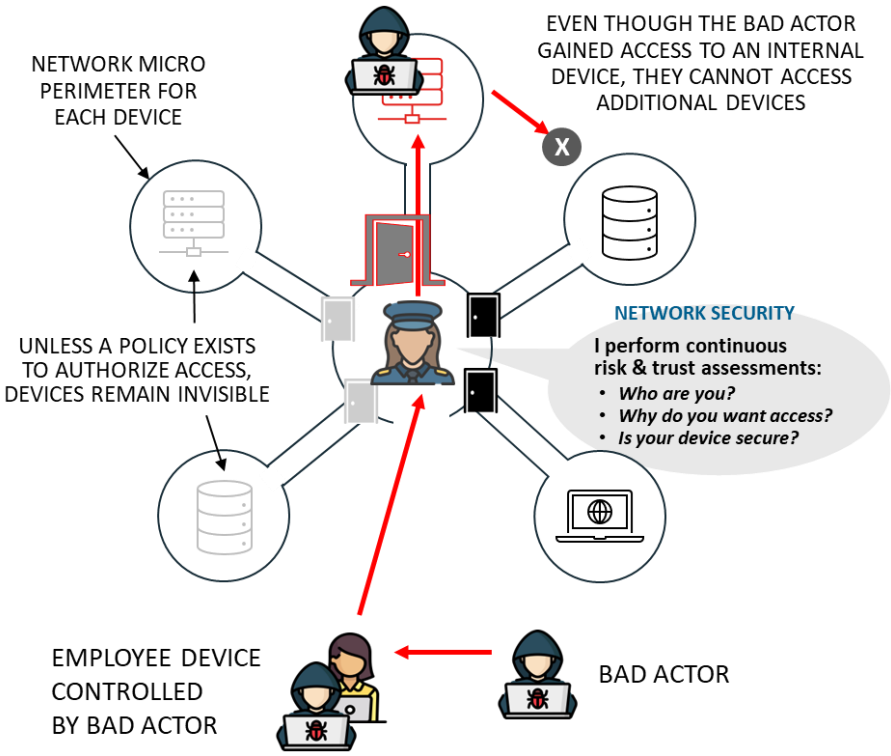
ZTNA is the newest cybersecurity strategy and it fundamentally changes the way firms manage cyber risk

The legacy perimeter-based security model assumes that all devices inside a firm's network can be trusted



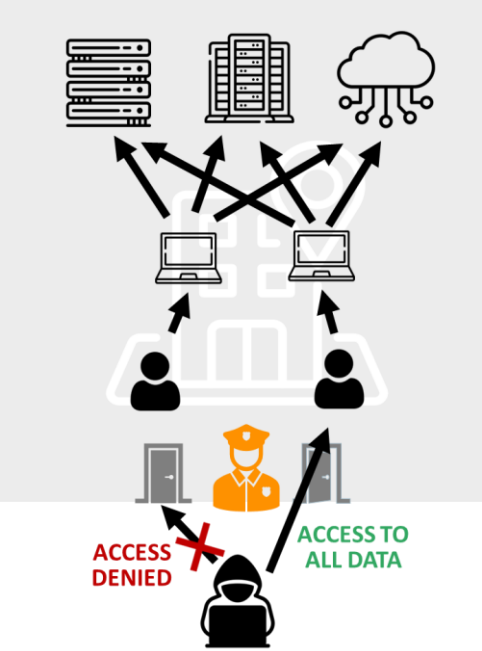
No matter how strong your security is, if a bad actor gets in through an external door, they can spread out laterally and vertically

Zero Trust Network Access (ZTNA) assumes no devices can be trusted and checks every device before it's granted access to another device



ZTNA assumes the bad actor has already gained access to the network and does not allow freedom of movement across devices

While ZTNA promises improved security, it is impossible to implement ZTNA without adding complexity



Data Point: *More than 60% of IT leaders that have implemented ZTNA believe it adds "moderate" or "significant" complexity to an organization**

ZTNA implementation activities	Friction and complexity are introduced
Design custom ZTNA policies that align with your business strategy & risk tolerance	A vendor recommends a "one size fits all" solution which does not fit your risk tolerance or tech strategy
Implement ZTNA policies, train users, and adapt business processes	New ZTNA policies and processes slow existing business processes, creating friction
Enforce ZTNA policies, deter end-user workarounds, and continuously adapt policies to changing business needs	Increased complexity causes human errors within IT ops and across the business

You must find the right equilibrium for your business which balances **Cyber Risk Reduction** and **Operational Complexity**

*According to a 2023 ZTNA complexity survey conducted by WP&C

A technology-led ZTNA strategy can result in increased business friction and even higher cybersecurity risks

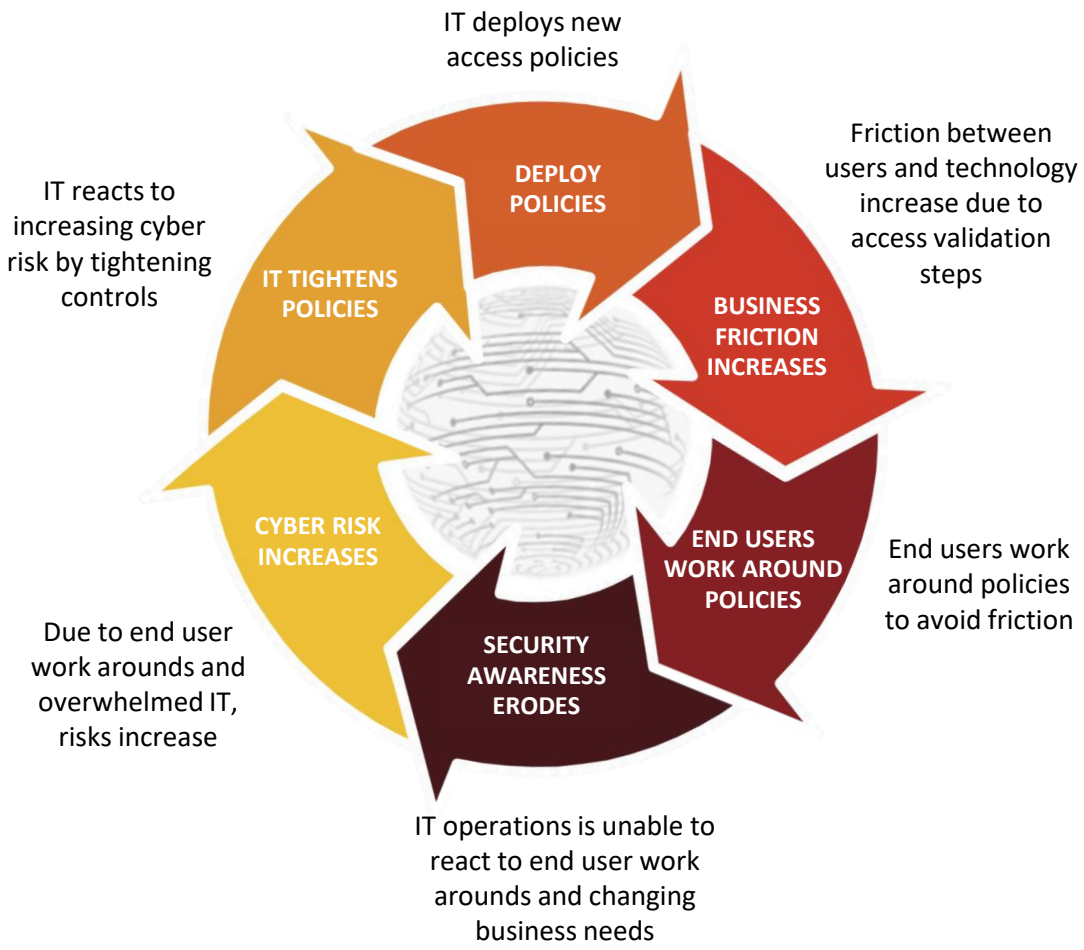
COMMON PITFALLS

1 After learning how ZTNA works, firms **refuse to adopt ZTNA** because they can't manage the complexity

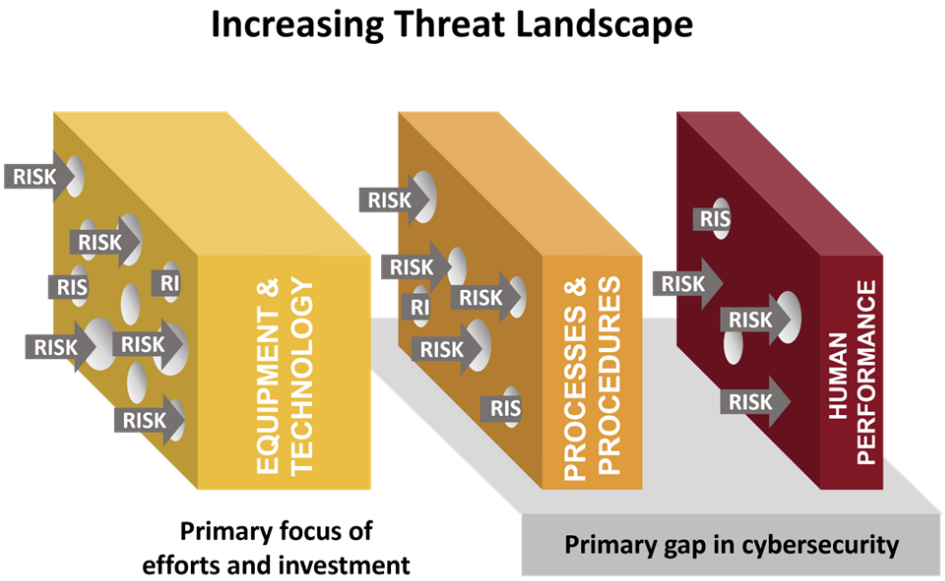
2 Firms never fully understand ZTNA but **implement off-the-shelf ZTNA technology from a vendor and assume they're more secure**—the false sense of security leads to more relaxed behavior and **cybersecurity risks increase**

3 Firms try to determine the right ZTNA strategy but never understand the interdependencies between process and systems and inadvertently **build friction into existing processes—users complain and work around new ZTNA policies**

A vicious cycle leads to increasing cybersecurity incidents



Technology-only solutions alone do nothing to address the 95% of cyber attacks caused by human error



Organizations that have already implemented ZTNA were 50% more likely to cite improved process discipline as the most important IT investment, as compared to firms that have not implemented ZTNA*

The gap in cybersecurity performance is due to poor operational discipline, which is **doing the right thing, the right way, every time.**

When IT operations lack effective mechanisms to detect failures in human performance, companies easily succumb to cyberattacks.

Process automation does not resolve human error, it simply moves the potential for human error to those designing, building and deploying the automation.

Cybersecurity strategies today rely too heavily on technology solutions with the belief they can "automate away problems"

*According to a 2023 ZTNA complexity survey conducted by WP&C

Complex processes cannot be made failure-proof, but HRO practices make them highly resilient and less likely to fail

High Reliability Organizations (HROs) operate in complex socio-technical environments and exhibit very low rates of catastrophic failures

1950s

HRO principles evolved after World War II from the U.S. Navy's program to develop and deploy mobile nuclear reactors to power ships and submarines

1960s – 1970s

HRO principles then spread across high-risk, and highly-complex sectors

1980s

Researchers at Berkeley and University of Michigan study the U.S. Navy, FAA, and a Commercial Power Plants to understand how these organizations operate

1990s – 2010s

Most recently, HRO principles have been deployed in other environments such as chemical manufacturing and emergency care

TODAY

IT HROs are the needed revolution in cybersecurity—Cyber HRO's will maximize human capability to prevent catastrophic cybersecurity failures

Impact of HROs

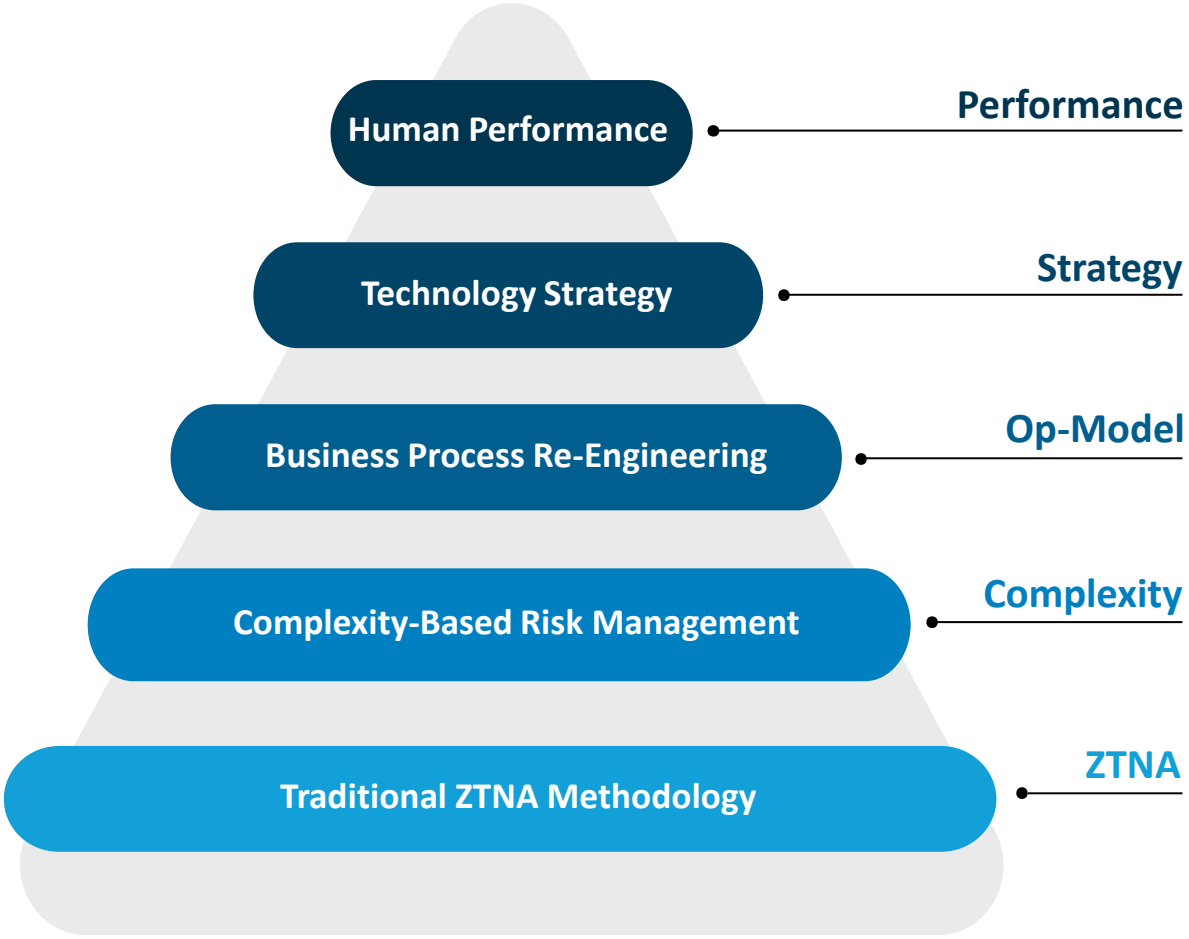
No nuclear incidents while operating 100+ Navy nuclear reactors for 60+ years

33x reduction in commercial aviation fatalities per million miles flown since 1973

100% decrease in incidents at Genesis Health System from 2009 to 2017

WP&C helps clients achieve the best security that ZTNA can offer without impairing the efficiency of the business

WP&C's High Reliability ZTNA Methodology



Performance — High-Reliability IT operations are required to maintain ZTNA

Strategy — Cybersecurity strategy must enable the desired tech vision

Op-Model — Business processes must be re-engineered to ensure ZTNA deployment does not increase friction

Complexity — Risk comes from complexity—understanding process-org-system interdependencies is the only way to understand true cyber risk

ZTNA — ZTNA as a methodology (instead of a rule) is the basis for a practical cybersecurity strategy

WP&C is experienced in helping organizations excel in each of the areas required for High Reliability ZTNA

	WP&C CASE STUDIES	IMPACT
Human Performance	• Assessed current-state culture with Yardstyck* • Established guiding HRO cultural principles • Prepared the org for change through training • Integrated behavior expectations into OEMS	• 50% reduction in lost opportunities, worth ~$200M in EBITDA • Improved culture reduced incidents by +70% • Nearly 5% improvement YOY in refinery utilization
Technology Strategy	• Developed high-level tech strategy • Deployed strategy through vendor selection, process re-engineering, and governance work	• Developed a tech strategy in 4 weeks • Selected 4 technology vendors • Instigated necessary governance
Business Process Re-Engineering	• In-depth assessment of process & organization • Developed a new operating model with an updated technology strategy • Collaborated with software vendors to implement changes	• Full-scale implementation within 60 days • Streamlined organization and process complexity through standardization • Transformed the organization's culture
Complexity-Based Risk Management	• Assessed architecture & organizational complexity by mapping system ecosystem • Conducted technology workshops to educate key stakeholders	• Full ERP modernization—with a focus on simplifying systems, improved integration between systems, and building capability for future system development

High Reliability ZTNA builds on Traditional ZTNA Methodology and Tools

*WP&C proprietary culture and Human Performance tools

WP&C's three-phase approach will guide you through a successful ZTNA journey

See the benefits from a ZTNA cyber strategy in just 3 months

PHASE 1: 5-Week ZTNA Readiness Assessment

WP&C's unique diagnostic tools and capabilities are used to rapidly understand the organization:

i. Current **Cybersecurity Capability Assessment**

ii. **Maturity Level Assessment** to evaluate org preparedness to adopt ZTNA

iii. **Business Process-IT Complexity Assessment** to understand high-risk processes and systems which require ZTNA policies

iv. Business Strategy understanding to ensure **ZTNA strategy enables tech vision**

v. Definition of **your unique balance** of ZTNA architecture, policy, and process

PHASE 3: Execution & Implementation

WP&C supports the execution to operationalize necessary changes, including vendor selection and program support as-needed

PHASE 0: Pre-Engagement Preparation Work

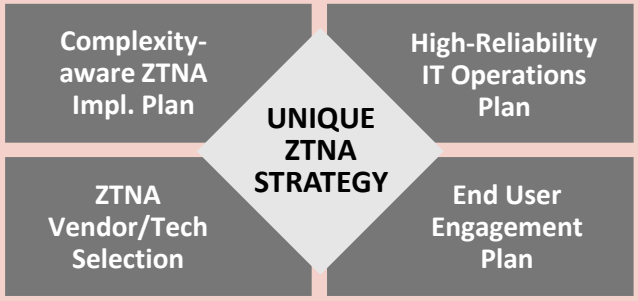
Align leadership & stakeholders

Stakeholder Survey

ZTNA Complexity Workshop

PHASE 2: ZTNA Strategy & Operating Model Development

WP&C works together with the client to design a bespoke ZTNA strategy



Note: WP&C is not a re-seller of technology or technology implementation services

Typical ZTNA engagements focus on ZTNA policy deployment without understanding underlying complexity

	OTHER CONSULTING FIRMS	WILSON PERUMAL & COMPANY
Core Capability	**Technology Deployment**	**Complexity Management**
Core ZTNA Services	• ZTNA policy creation • Deployment of ZTNA enforcement services or products	• Investigation of key systems and processes that have the biggest impact on cyber risk • Development of the right policies for these key processes and systems • IT operational capability to design, deploy, maintain, and continuously adapt policies
Tech Strategy	Promote their own technology products or partner vendors	Not affiliated with any vendor, we provide unbiased vendor selection recommendations
Working Style	Copy/paste approaches from previous clients, including 'off the shelf' tech	We have a collaborative working style and work with clients to help the find the best solution
Outcome	Generalized, comprehensive ZTNA policies are deployed indiscriminatingly without consideration for existing or added complexity, leading to: • Reduced effectiveness of ZTNA • Added friction in business operations • Increased cyber risks	• ZTNA policies are specific to the firm's unique balance of agility, strategy, and risk tolerance • ZTNA policies are deployed as-needed with a formally vetted 3rd party vendor • IT is upskilled and transformed into a High Reliability Organization that can maintain ZTNA policies and react to new threats

Conclusion & Getting Started

We help organizations of all sizes focus their cybersecurity efforts by:

Determining the key systems and processes that make the biggest impact on cyber risk (and enable their business strategy)

Defining the policies to secure these key systems and processes

Within 3-months you will be well along your ZTNA journey by:

Identifying what ZTNA policies and processes are the best fit for your organization (not just for your cyber targets but for your business strategy)

Improving human performance to ensure you're able to execute without the human errors that leave firms susceptible to cyber attacks

If you're concerned about cybersecurity risk—reach out to us
at contact@wilsonperumal.com to get started on your ZTNA journey

Wilson Perumal & Company

CONTACT US

wilsonperumal.com

contact@wilsonperumal.com