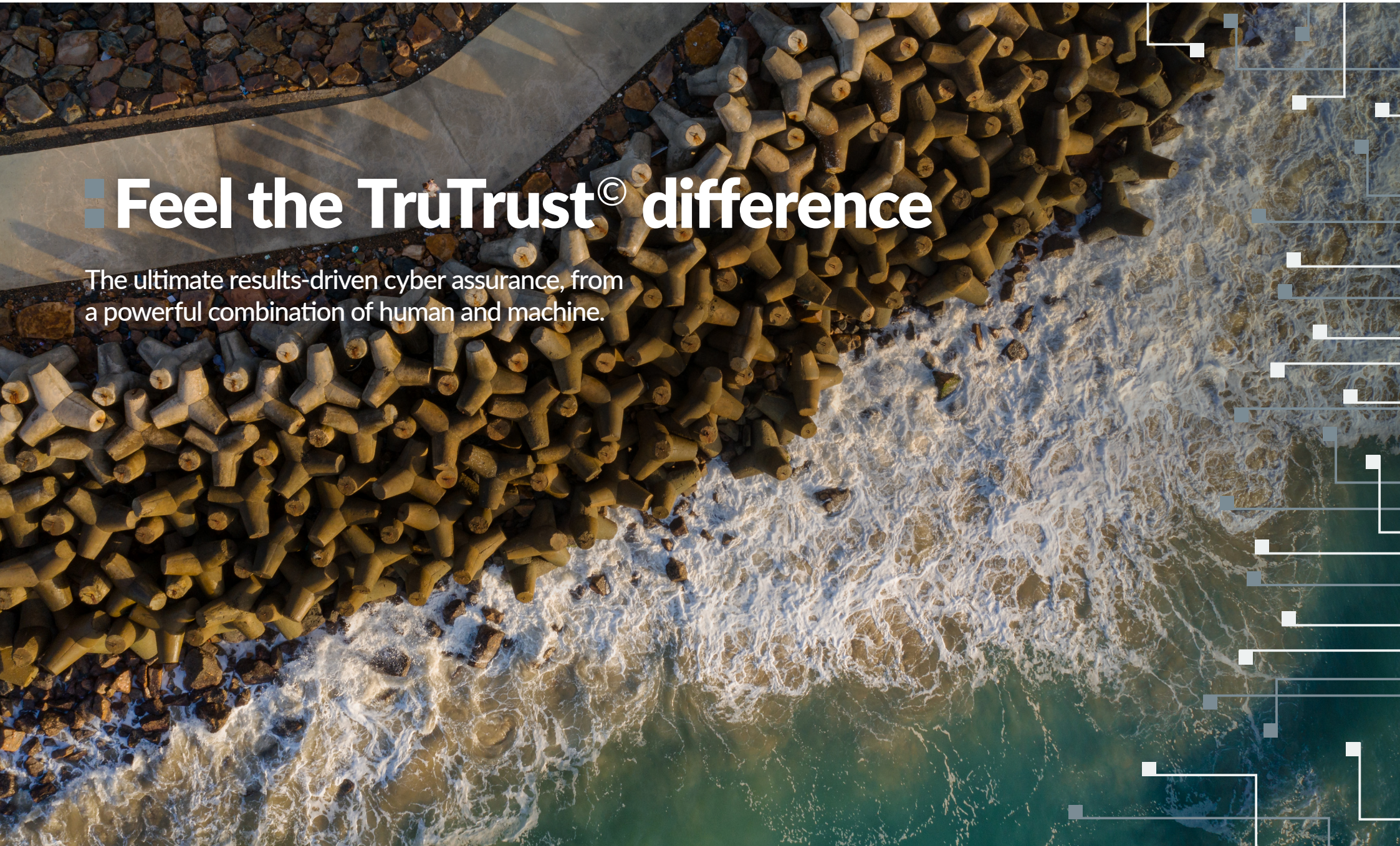
zepko



Feel the TruTrust© difference

The ultimate results-driven cyber assurance, from a powerful combination of human and machine.

Cyber threat reality outstrips correct response

Businesses are facing an increased level of cyber risk, and it isn't just the volume and frequency of attack that is rising. Cybercriminals are armed with a wealth of sophisticated attack methods that extend the breadth and depth of their exploits, placing every organisation at higher risk.

1 in 2 firms are now targeted by cyber attacks every year[1], and the impacts are significant. The median cost of a successful breach has doubled in the last 12 months[1]. In response, businesses are taking immediate steps to increase their level of protection.

The knee-jerk reaction is to deploy additional technology. But while these solutions help to detect threats, misidentified risks create unwanted noise that overwhelms internal IT teams. This impacts their ability to properly detect and investigate live threats, extending resolution time and escalating business fallout.

Even with the new tools in place, protective monitoring and incident response is often restricted to business hours only. Many businesses believe they do not need 24/7 hour protection, yet recent data indicates that 25% of attacks occur outside of business hours. Therefore, failing to ensure around the clock defence is like leaving your front door open and unlocked while you sleep. Logic dictates this cannot be acceptable to any business, so the question you're facing is simple – **are you really doing enough to stay secure?**

AI: Panacea or predicament? Only a part of the solution

Businesses are buying into the promises of Artificial Intelligence (AI) to reinforce defences without needing the human touch. But while AI is a valuable weapon in the cybersecurity armoury, it is no silver bullet. In fact, it can foster a false sense of security.

- Overreliance on AI can expose your business to targeted attacks.
- Misidentified threats create additional operational overheads and extend business disruption.
- AI commonly learns from limited technologies or data out of context, undermining its ability to make good judgements.
- Hyper-responsive AI struggles to differentiate between genuine and malicious actions, inadvertently blocking legitimate activity.
- Persistent cyber threats are incorrectly baselined as normal network behaviour and thereby excluded from future analysis.
- New additions to your security stack trigger false alerts that add to the noise, causing IT teams to "over-tune" which limits effective response.

While there's little doubt that AI is useful, its true value can only be realised in conjunction with expert, timely and relevant interventions as well as constant tuning from skilled cyber teams.

TruTrust©- Game-changing peace of mind across your IT estate

The only way to ensure true cyber assurance is with the real-time correlation of information and rigorous investigative processes across your IT estate. TruTrust© from Zepko delivers a perfect balance of human and machine-learning that ensures 24x7 resilience against the latest cyber threats challenging your business – from detection through to trackable, reported remediation.

Leveraging technology-derived insights, our specialist team provide expert interrogation and human intellect to deliver extraordinary threat detection beyond human scale. Founded in a result-driven approach, our laser-focused ITM (Incidents that Matter) process model, and macro reporting on the Metrics that Matter, provide valuable full context and genuine transparency over the efficacy of your defences.

TruTrust© leverages 3 pillars of defence to ensure that your SOC can detect and track-and-trace the latest MITRE ATT&CK tactics, techniques and procedures (TTP).

Proactive defence

Powered by Global Threat Intelligence Network (GTIN)

Our cyber threat intelligence system provides advanced warning of cyber threats targeting your organisation or sector; coupled with vulnerability management insights, we aim to harden your organisational defences ahead of an attack.

Reactive defence

Automated

Our industry-leading security services protect your users and systems in real time by blocking network and malware threats, as well as data theft and exfiltration attempts.

Reactive defence

Incident response playbooks

Automated threat hunting, coupled with expert analysis enables the SOC team to rapidly identify indicators of compromise (IoCs) in your network and trigger incident response processes to halt attacks in progress.

TruTrust© delivers:

- Ultimate assurance and accurate resolution of cyber incidents 24x7x365.
- Sub-second incident responses.
- Community-based risk reduction benefit.
- Reduced false positives and unnecessary fire drills.
- Single pane of glass visibility of the active threats impacting your IT estate.
- Incident response play books that fuse AI with human intellect.
- Key Risks and Remediations (KRR) reporting, providing business context with the 'Metrics that Matter' dashboards.
- The TruTrust© Universal Connector connects with every IT data-source and security-relevant dataset to leverage what you have today.

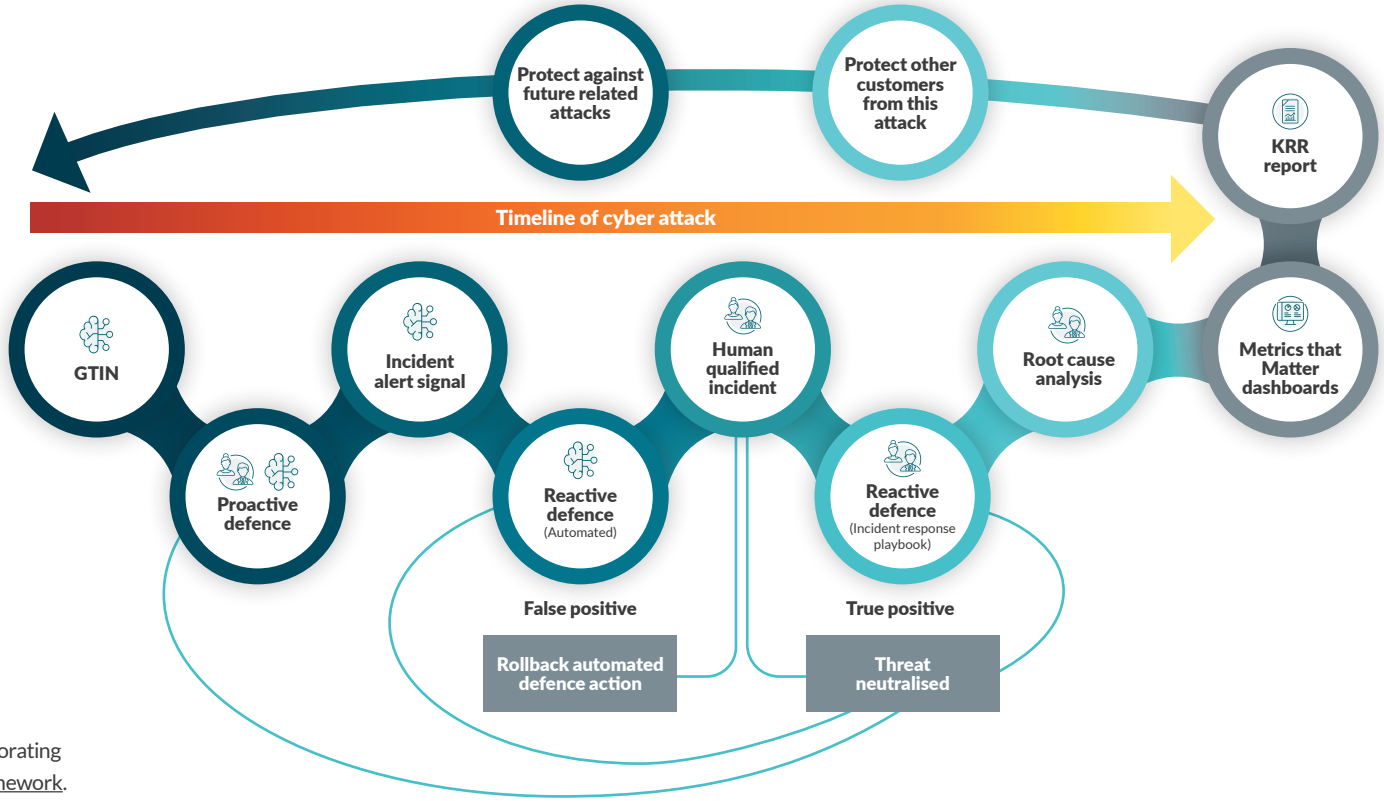
TruTrust© closes the cyber security loop

Traditional cybersecurity processes and incident responses are limited, and lack the insights and context needed to inform fast and accurate response-to-remediation. It's a reactive process that sees threats identified after-the-fact, often once significant damage has been done.

TruTrust© closes the loop to deliver an informative process that combines human insights and learned context to ensure responsive and reliable 24x7 security assurance. Incident post-mortem reporting is standard, with subsequent learnings used to refine and reinforce future defence postures.

With this approach, containment is no longer seen as the end of an attack, with appropriate follow-up actions in place to deliver robust resolutions that inform future response and provide reassurance that every incident is truly owned from beginning to end.

Cyber security assurance loop:



Derived from and incorporating the MITRE ATT&CK framework.

Business impact assessment

Scenario 1 | Self-managed security posture – 9am-5pm

30%
The percentage of alerts ignored or not investigated due to alert fatigue.[2]

277 days
The average time taken to identify and resolve a data breach.[3]

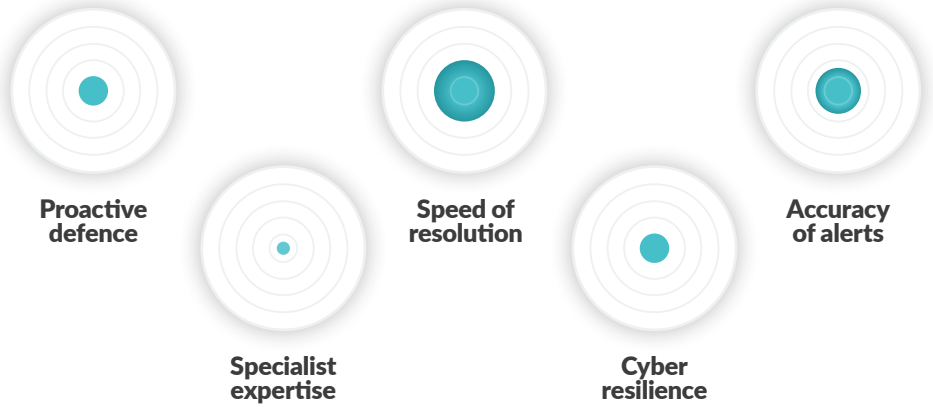
Situation

- Business operates with some basic protections, including firewall, anti-virus and web-proxy.
- This is managed on an ad-hoc basis during business hours only.
- Multi-vendor estate with little to no cyber integration.
- Managed by generalist internal IT resource, with no specialist cyber expertise.

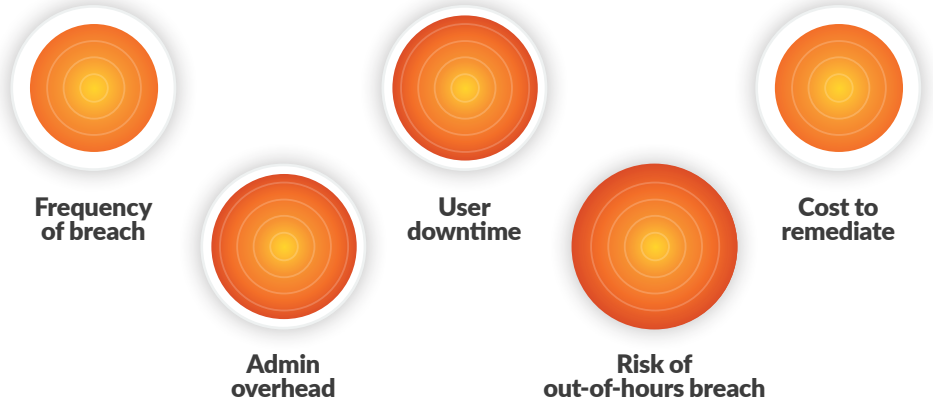
Impact

- Lack of cyber integration restricts context and visibility of the IT estate.
- Limited resources prevents any out-of-hours incident response capability.
- Lack of expertise and informed insights extends resolution times.
- Single system alerts with no wider context yield incomplete or incorrect threat assessments.
- No root-cause analysis to inform prevention of reoccurrence.

Cyber response



Business impact



Business impact assessment

Scenario 2 | Outsourced service from non-specialist MSP – 24x7

$5,600
The potential cost to a business for every minute of downtime.[4]

>10 mins
The average time spent investigating security alerts.[5]

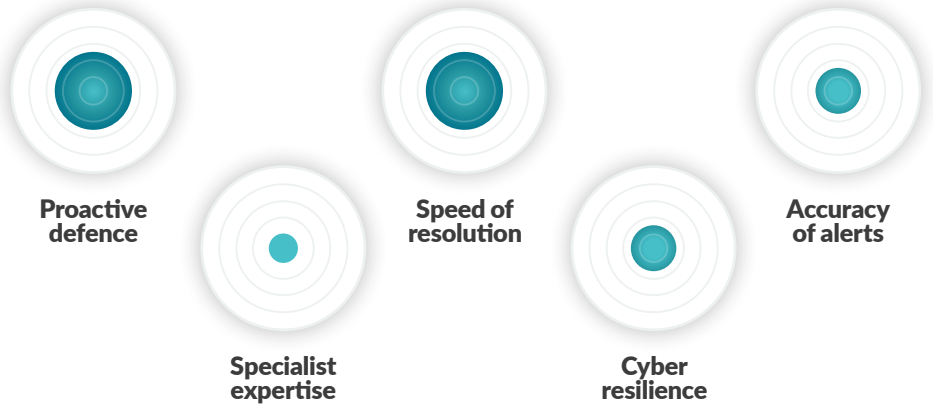
Situation

- Business operates with some dedicated internal IT resource, but also outsources to an IT generalist MSP.
- Multi-vendor estate with limited cyber integration.
- Over-reliance on AI platforms and automation to overcome gaps in expertise.
- Single-service alerts delivered from multiple protections to a non-specialist helpdesk.

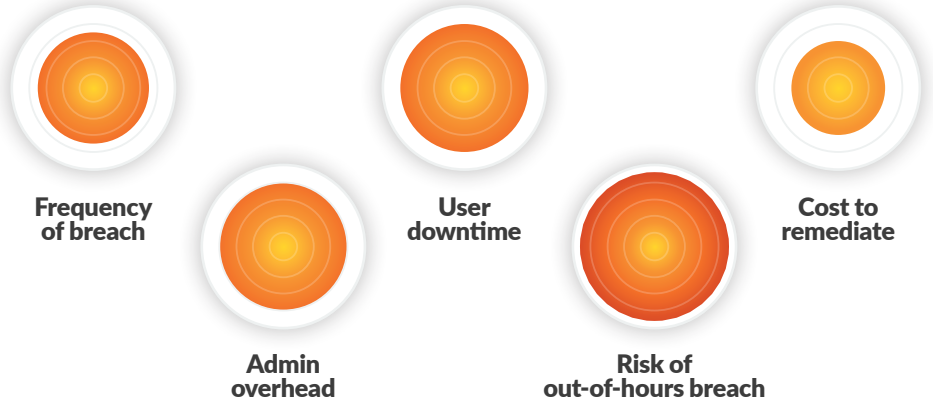
Impact

- AI tools limited to historical data and known patterns, so cannot adapt to new threats.
- Limited context sees AI systems frequently flag legitimate user activity, impeding productivity and damaging user experience.
- Limited integration prevents full visibility of IT estate.
- No root-cause analysis to inform prevention of recurrence.

Cyber response



Business impact



Business impact assessment

Scenario 3 | Comprehensive SOC with TruTrust© - 24x7

£2.4m
Saved for customers by TruTrust © between Jan - May 2023.

106
The number of attacks prevented by TruTrust © between Jan – May 2023.

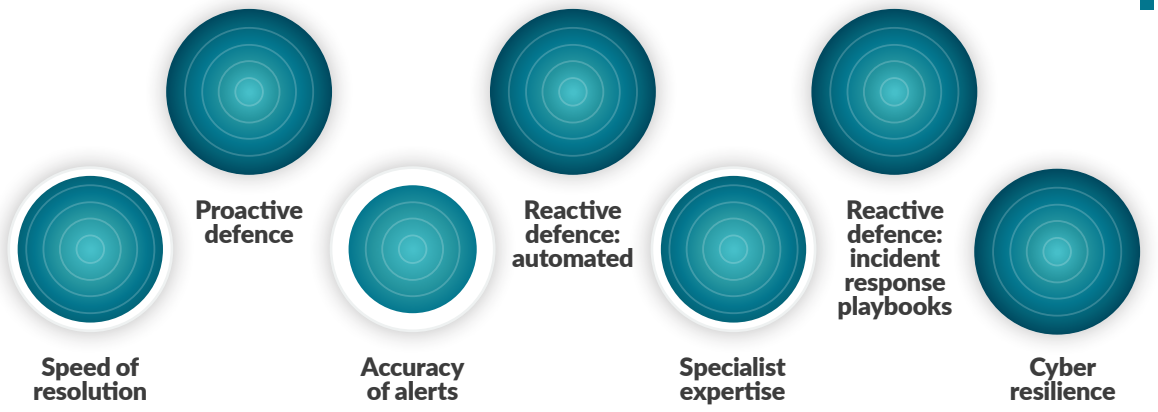
Situation

- Business operates with a combination of appropriate security protections, orchestrated and managed by a dedicated and expert SOC team.
- Multi-vendor estate integrated with TruTrust© Universal Connector.
- Eyes-on 24x7 threat protection from expert team.
- Unified insights delivered with context via Metrics that Matter dashboard.

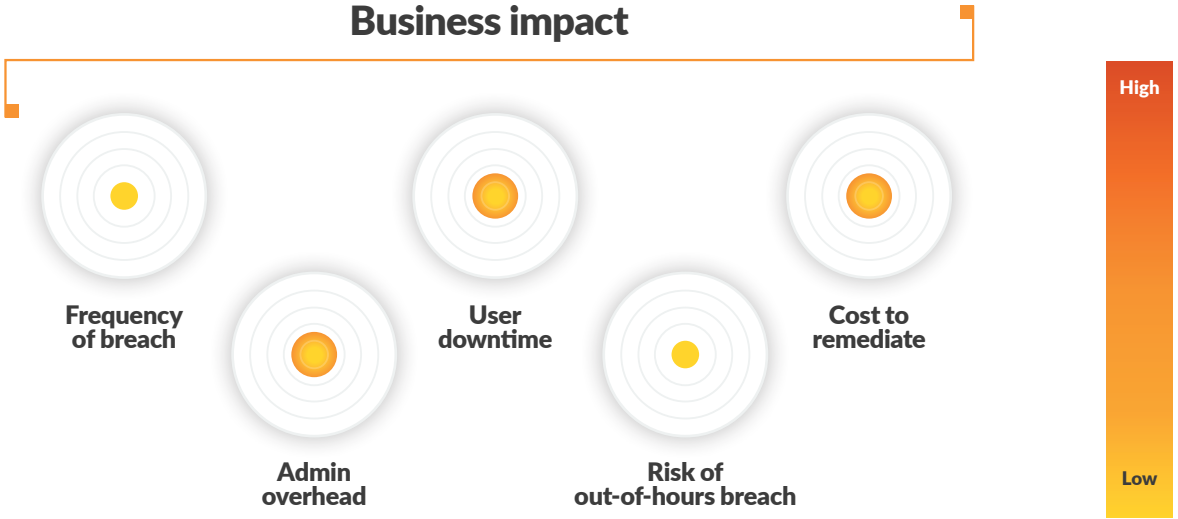
Impact

- Real-time visibility across entire IT estate provides a complete cybersecurity picture.
- Expert human intervention harnesses valuable AI insights with applied real-world context to arrest attacks whilst reducing false positives.
- Proactive defence, powered by GTIN delivers sub-second response times.
- Threat qualification and post-mortem root cause analysis informs ongoing protection.

Cyber response



Business impact



Why Zepko

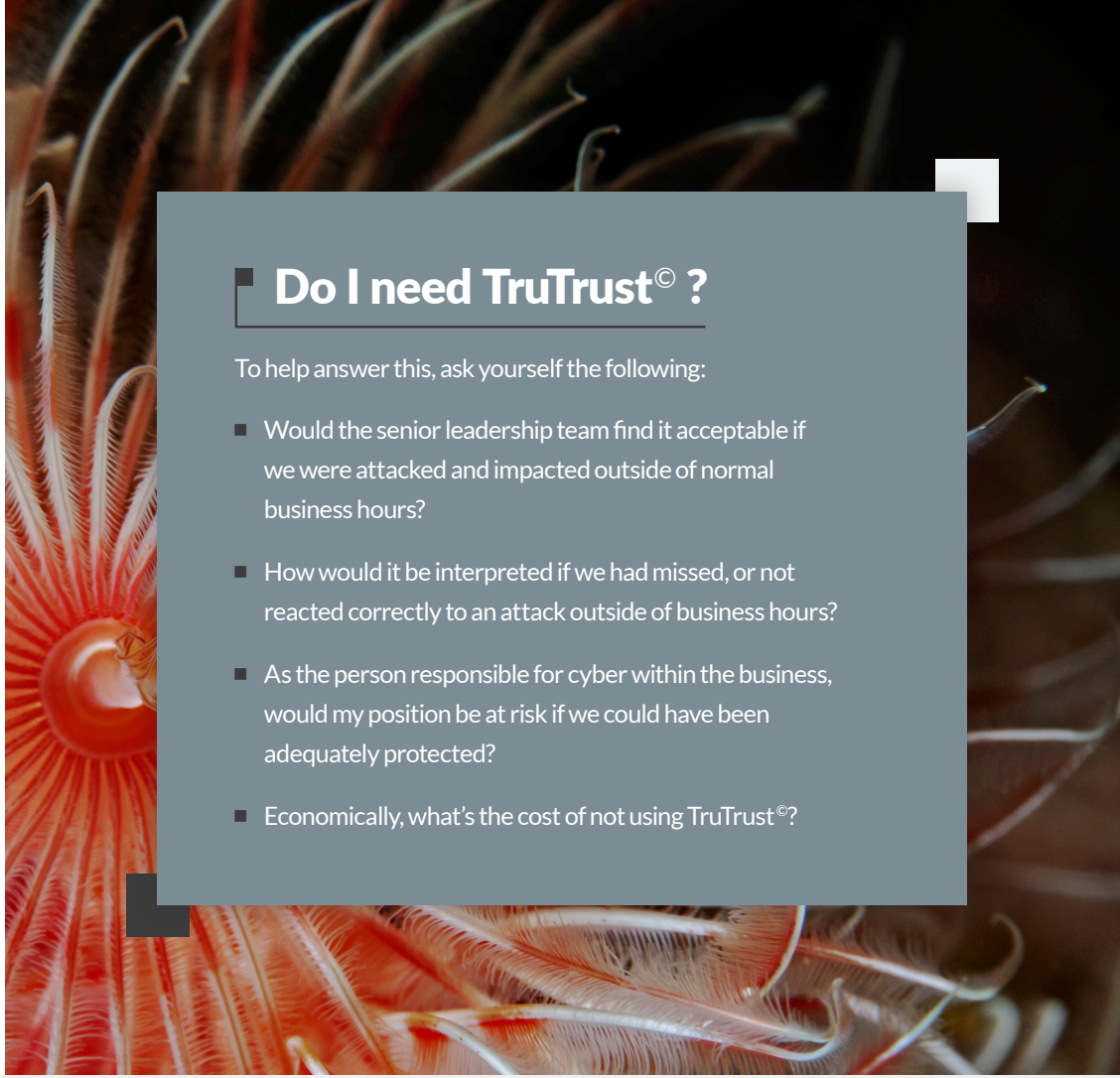
With two decades of real-world cyber incident management experience, we bring industry-leading skills, knowledge and instincts to protect you against the latest cybersecurity risks threatening your IT business.

Accredited to ISO 27001 and CE+, every member of our UK-based SOC teams is vetted to SC and NPPV3 and works as an extension of your team to deliver 24x7 tailored protection.

Our diverse portfolio of existing customers ensures a wealth of experience across organisations from every industry, leaving us uniquely positioned to understand the intricacies of your business and sector to deliver a SOC solution built around results that make a difference.

References:

1. Hiscox Cyber Readiness Report 2022
2. https://www.criticalstart.com/wp-content/uploads/2021/11/US48277521_TLWP.pdf
3. https://www.ibm.com/reports/data-breach
4. https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/
5. https://www.infosecurity-magazine.com/news/mssps-waste-hours-of-time-on-false/



Do I need TruTrust© ?

To help answer this, ask yourself the following:

- Would the senior leadership team find it acceptable if we were attacked and impacted outside of normal business hours?
- How would it be interpreted if we had missed, or not reacted correctly to an attack outside of business hours?
- As the person responsible for cyber within the business, would my position be at risk if we could have been adequately protected?
- Economically, what's the cost of not using TruTrust©?

zepko

+44 (0) 845 074 0790 | info@zepko.com