Zero Trust: A One-Page Brief for Busy Stakeholders

Why now?

Cyberattacks are in a new, more sophisticated era, regulators are raising the bar, and customers expect stronger protection.

Boards, investors, and compliance teams are asking the same question: how do we prove our security model is strong enough?

Different audiences, different needs

For Executives - Focus on reducing business risk, maintaining compliance, and protecting reputation.

For Staff - An inclusive approach that makes them feel part of the solution rather than part of the problem.

For Suppliers - Providing access to systems is controlled, and data is protected, so collaboration doesn't increase risk.

What's at Stake

- **Trust erosion**. Clients may quietly shift to competitors if they doubt your security.
- **Supply chain exposure.** One weak third-party link can undermine your whole system.
- **Financial strain.** Fines, fixes, and lost sales drain resources.
- **Investor confidence.** Uncertainty reduces backing from lenders and investors.

How Zero-Trust Helps Stakeholders

Reduce breach risk. Close insider gaps before they turn into headlines.

Support compliance. Stay aligned with GDPR, ISO 27001, and other key frameworks.

Give leaders oversight. Visibility of who's accessing what, when, and why.

Reassure stakeholders. Show customers, partners, and regulators that security is built in.

Key Points To Start

- Check that your company's most critical data, systems, and users are secure.
- Identify where implicit trust still exists.
- Phase Zero Trust controls into existing systems gradually.
- Involve staff, stakeholders and the Board.

Takeaway

Zero Trust isn't a product; it's an approach. The organisations that adopt it early build stronger security foundations, reduce risk, and improve confidence with customers and stakeholders.

Created by Sara Edlington. Cybersecurity content writer. Email: sara@sandsedlington.com