the I.T. insider

# 6 Top Tips for Zero Trust Success

In a world where cybercrime is now being offered as a service, organisations are adopting a new approach to security, where the golden rule is to 'trust nothing, verify everything' – whether that's a device, an employee or even the supply chain.

If you're unsure about how to go about implementing a zero trust approach, here are some tried-and-tested tips and best practices to help get you started.

## Tip 1: Create your Zero Trust Business Plan

The first thing you need to do is align zero trust to your business initiatives:

- Map out your existing investments
- Prioritise projects and integrations
- Set clearly defined goals and outcomes
- Measure risks in financial terms

To have the best chance of success, make sure your business leaders are fully aware of the benefits of adopting a zero trust model and the risks involved if they don't. Having everyone on board and on the same page will make it that much easier when you set goals, align IT and security teams, and allocate budgets down the line.

## Tip 2: Build a Strong Foundation

Incorporating zero trust into your current security architecture should be a top priority. You can achieve this by:

**Increasing visibility** – apply advanced analytics to constantly monitor network communications and endpoint devices for suspicious activity, weak spots, and policy violations.

**Implementing a data loss prevention (DLP) policy** – helps prevent employees or third-party users from sending sensitive or business- critical information outside your core network.

**Treating your IT and security operations as a single estate** – embrace DevSecOps for a more holistic approach, where responsibility for security is shared.

Doing all of this will also help you get more insights into how data flows across your network and increase your ability to quickly recognise and mitigate any threats or vulnerabilities.

## Tip 3: SIEM, SOAR & SOC

Implementing a zero trust strategy doesn't have to break the bank. You can reduce security capital and operational cost and make budgets stretch even further by leveraging security incident and event management (SIEM) solutions like IBM Security QRadar XDR and security orchestration, automation, and response (SOAR) solutions like IBM Cloud Paks.

You can also make operations more robust by:

- Establishing an ecosystem-wide security operations centre (SOC)
- Implementing a single cloud-agnostic platform with visibility across providers
- Applying AI-enabled security intelligence to detect any abnormal behaviour

This allows for centralised management, streamlined operations, and collaboration across teams; ultimately putting you back in control of your network and giving you greater visibility into your ever-expanding cloud attack surface.

## Tip 4: Integrate Zero Trust Controls

IBM research has found that organisations with successful zero trust strategies use a combination of security telemetry, real-time traffic analysis, and automation and orchestration capabilities to achieve greater insights into user behaviour, the previously invisible and often unprotected devices connecting to their corporate network, as well as data and business-critical workloads across multiple cloud and storage locations.

Being able to provide more actionable insights for your security team is invaluable for your overall defence posture and is completely achievable when you integrate zero trust controls into your existing security operations.

## Tip 5: Build a Zero Trust Dream Team

If like many businesses at the moment, you're struggling to recruit and retain employees who have the necessary skills to help your zero trust vision succeed, take a more intuitive and flexible approach when hiring new talent:

- Offer skill development programmes to promising candidates
- Assess behaviour and competency, rather than just experience
- Apply cyber aptitude tests to identify a candidate's latent potential
- Foster a culture where continuous learning is encouraged and rewarded

Do this and you'll be on the fast track to having a modern and adaptive cyber talent management system.

## Tip 6: Measure your Zero Trust Progress

Implementing a zero trust strategy can take several years to achieve. Be sure to keep track of where you are in terms of your original business plan. Do any specific areas need revisiting and tweaking to fit with your evolving business needs? Has the user experience improved? Have the number of cyber events significantly reduced? Are your Dev, Sec and Ops teams working together as well as they could? These are just some of the questions you should be regularly asking, so you can catch any issues quickly and keep your zero trust journey on track.

## Key Takeaways

So remember, to get started on the road to implementing a zero trust security strategy:

- Treat your IT and security operations as a single estate
- Collaborate internally and externally to manage cybersecurity risk
- Modernise your security operations and integrate zero trust controls
- Apply cloud, AI-driven analytics, and automation extensively
- Start building and investing in your very own zero trust dream team