Building a Modern Security Strategy

A Practical Approach

Lee Roebig | *Customer CISO*

sekuro

Who is Lee Roebig ?

- Customer CISO for Sekuro
- Director of Strategy & Architecture practice
- Completed numerous strategies across legal, health, insurance, construction, manufacturing, leisure, ASX listed companies.
- 17+ years in Technology, 10+ in Cyber Security
- Held previous cyber security leadership roles in Australian multi-national organisations

Agenda

- CHALLENGES IN THE MODERN ENTERPRISE
- WHY WE NEED TO CHANGE
- HOW TO BUILD A MODERN, PRAGMATIC STRATEGY WITH KEY INGREDIENTS
- 3 KEY STRATEGIC INNOVATIONS THAT ACTUALLY WORK

Challenges in the modern enterprise

Things were simpler in the past

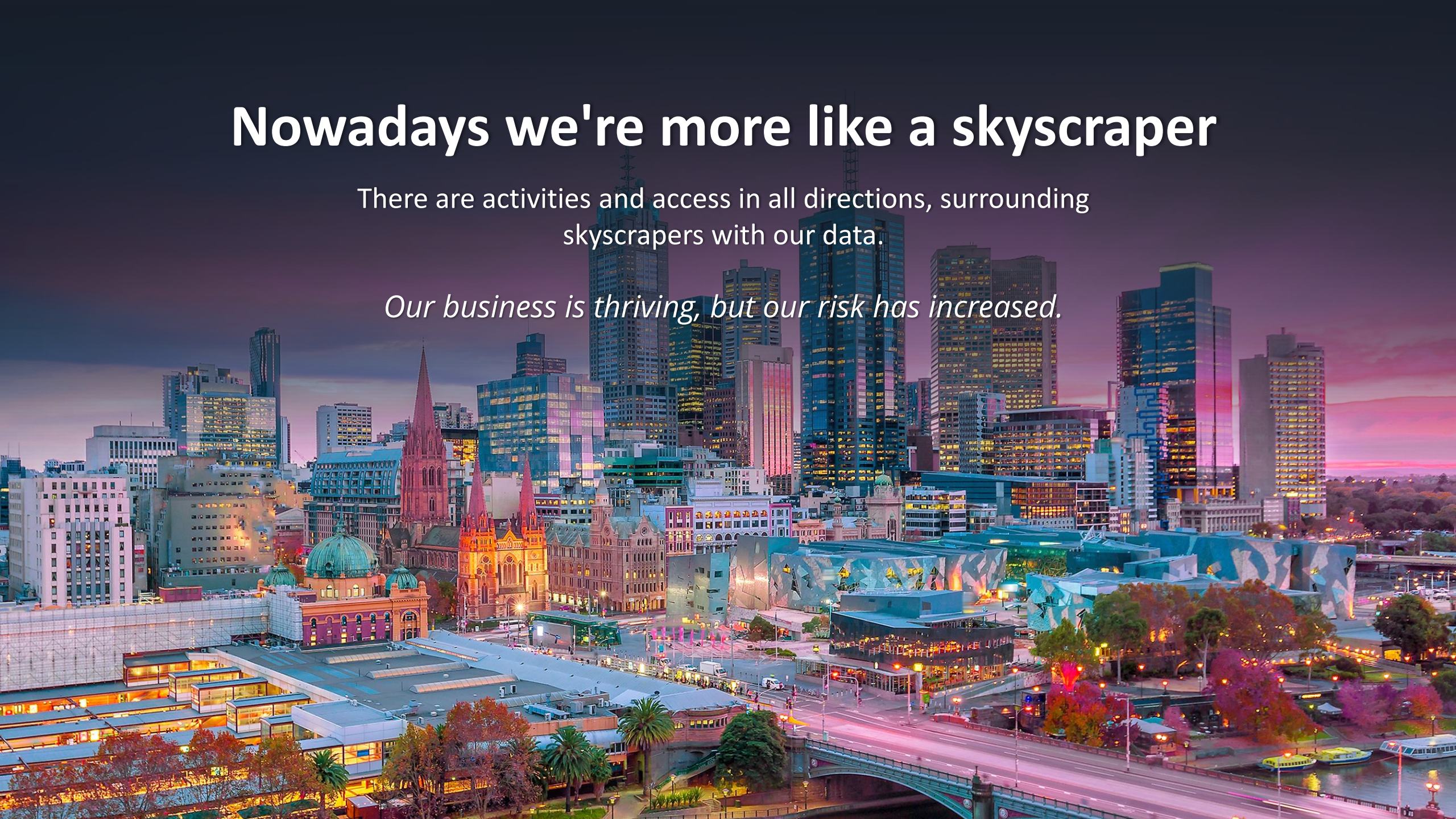
Our organisation and assets were like a castle. There was one bridge in, and huge walls around anything of value inside.

It's easier to stop an attacker when you know where they'll come in.

Nowadays we're more like a skyscraper

There are activities and access in all directions, surrounding skyscrapers with our data.

Our business is thriving, but our risk has increased.



2

Modernise our security program, compliment and accelerate the business securely. This is the correct approach.

1

Raise some risks, slow down digital transformation. Consequence: We get ignored and bypassed.

Industry Pitfalls of Security Strategy

Stuck in the past – suggesting old techniques to solve new problems. Who needs another firewall?

Unclear

High-level advice that doesn't properly articulate what good looks like

Unrealistic

Suggesting things that are **far beyond budget/capabilities**

Unbeneficial

Giving recommendations **'because that's what we do'** or **'box ticking'** instead of real benefit

Unactionable

Advice so non-prescriptive that we don't know what to do with it.

Two Extremes..

No more secure than before but having papers to say you are

Either lead by compliance/audit

…or lead by technology

Buying all the shiny new toys with no clear purpose

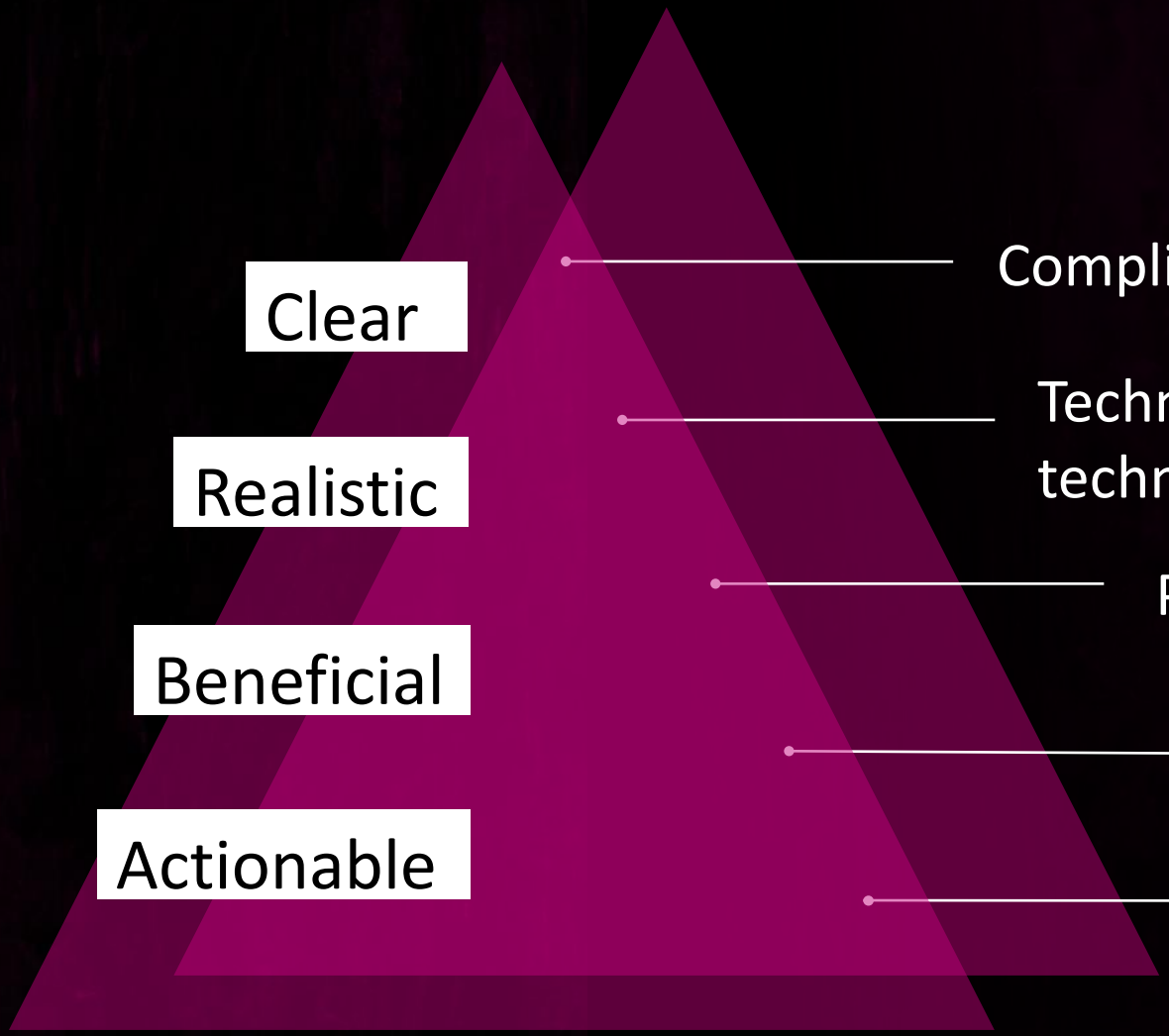
What we need:

A modern approach to security that still address our compliance, manages our risks and gives us a clear way to holistically defend against modern attacks.

But How?

By using key ingredients in our strategic recipe

The key principles to a successful strategy



Compliance considered, not compliance led

Technology agnostic, but technology considered

Prescriptive but not restrictive

Less pretty pictures, more real actions

Modern techniques

sekuro

Analytics

Real-time observation across all pillars to understand interactions, anomalies and threat visibility.

Governance & Risk

Manage risk, make strategic decisions within security to match business objectives.

Data

Store, manage and protect data from exfiltration & misuse.

Compliance & Privacy

Adhering to regulatory obligations, standards and laws.

Applications

Catalogue, assess, restrict access to and protect applications and APIs.

People

Foster a culture that creates awareness & resilience in our people whilst measuring its effectiveness.

Infrastructure

Protect key infrastructure from misconfiguration and unauthorised access.

Identities

Multi-step verification of users with automated, continuous provisioning and deprovisioning.

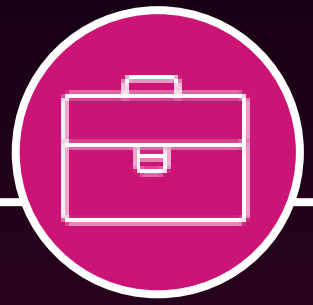
Networks

Segmenting and isolating networks to protect our valuable assets.

Endpoints

Protecting our devices, anywhere anytime.

Suggested Process



Map to your business goals

Work closely with your business, understand future plans, their concerns and how the security strategy can help then. **We're not always a cost centre!**

Get Technical with the Engineers

Don't stay high-level, get down into the weeds with engineers. Understand what's possible, what actually works and where true gaps lie.

Get prescriptive and innovative

Figure out what technologies exist that can creatively solve problems, design prescriptive outcomes that clearly articulate what good looks like.

Map to, but don’t stop at, compliance.

The final output

Current & Future State Initiatives

The details on what is(n't) working currently, and what good looks like in the future (including technologies required). Clearly articulate what needs to be achieved!

Prioritised Roadmap

Executive Engagement

The final output

Current & Future State Initiatives

Prioritised Roadmap

A detailed roadmap with prioritisation timelines for implementation of each target control. Start with Quick Wins.

Executive Engagement

The final output

Future State Initiatives

Prioritised Roadmap

Executive Engagement

Map your security objectives to business objectives – change security perception from cost centre to business enabler.

Innovation trends

3 Innovations

Zero Trust Network Access – Segmentation the Easy Way

Use Identity to dynamically drive network access. Remove inherent trust from networks – unify off-premises and on premises user experiences.

MFA and Authentication Policies – Better and Faster

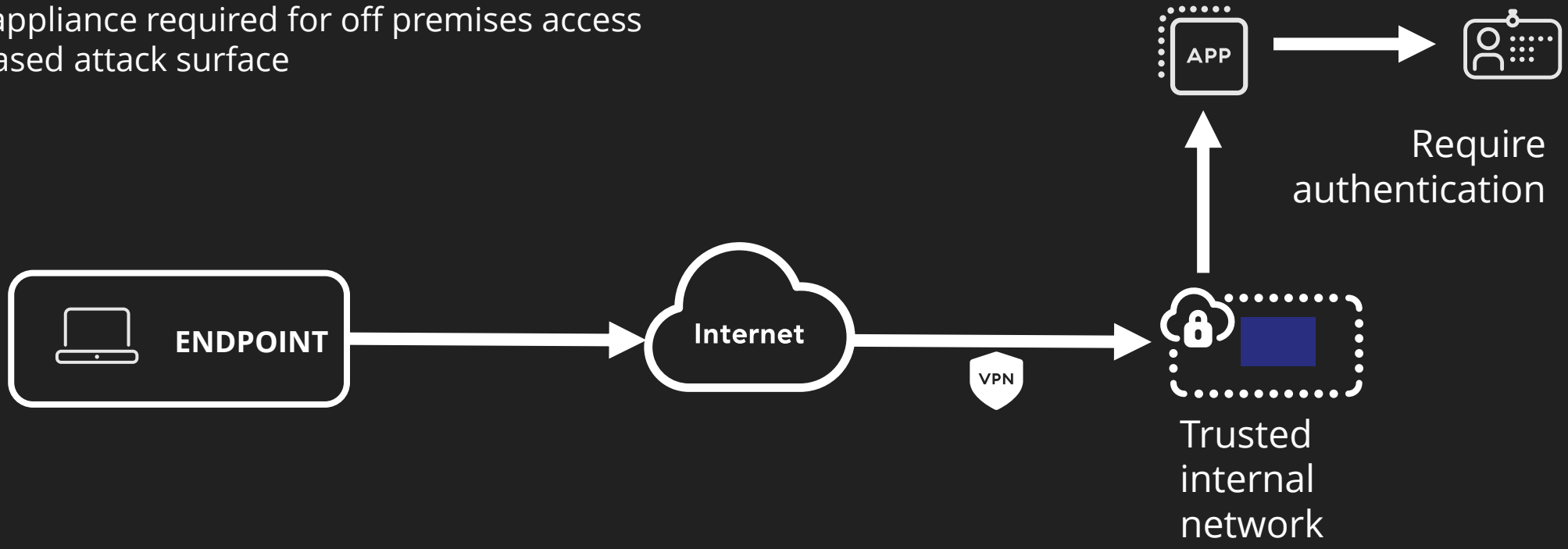
Be aware that MFA can be bypassed easily. Move towards passphrases, remove password expiry, transition long term towards passwordless with biometrics. Implement device-aware Identity systems and utilise that for contextual access policies.

Web Access Policies – Think 'Cloud Apps' not 'Websites'

Avoid where possible blocking websites based on category/URL alone. *Instead, get visibility into granular interactions with web/cloud apps like data flows and their content, activity like download/upload/share and instances like personal OneDrive vs Corporate.*

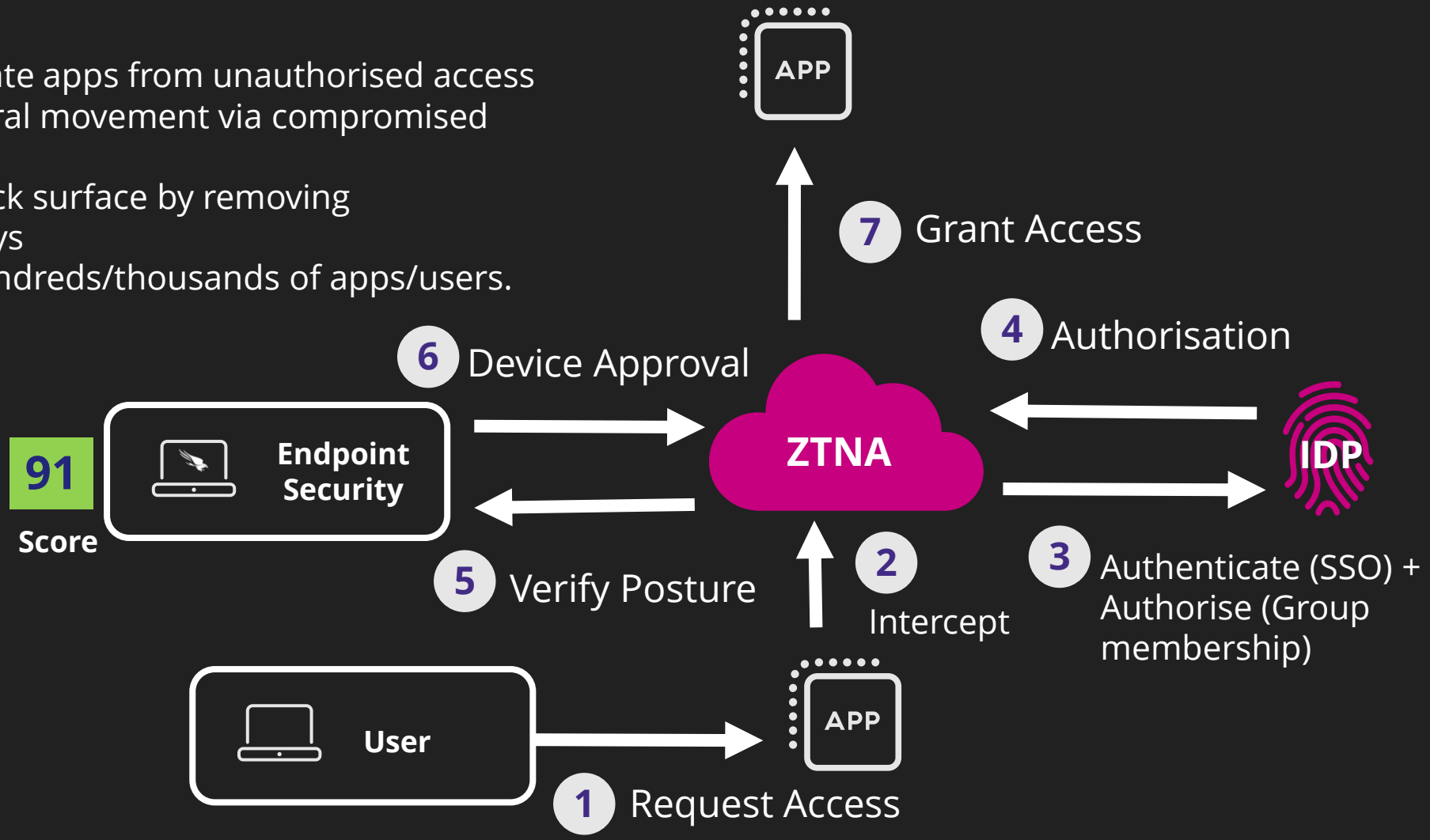
The old way: Connect Users to Private Apps

- Compromised credentials/device equals compromised app
- Lateral movement through compromised /rogue device on network
- VPN appliance required for off premises access
- Increased attack surface

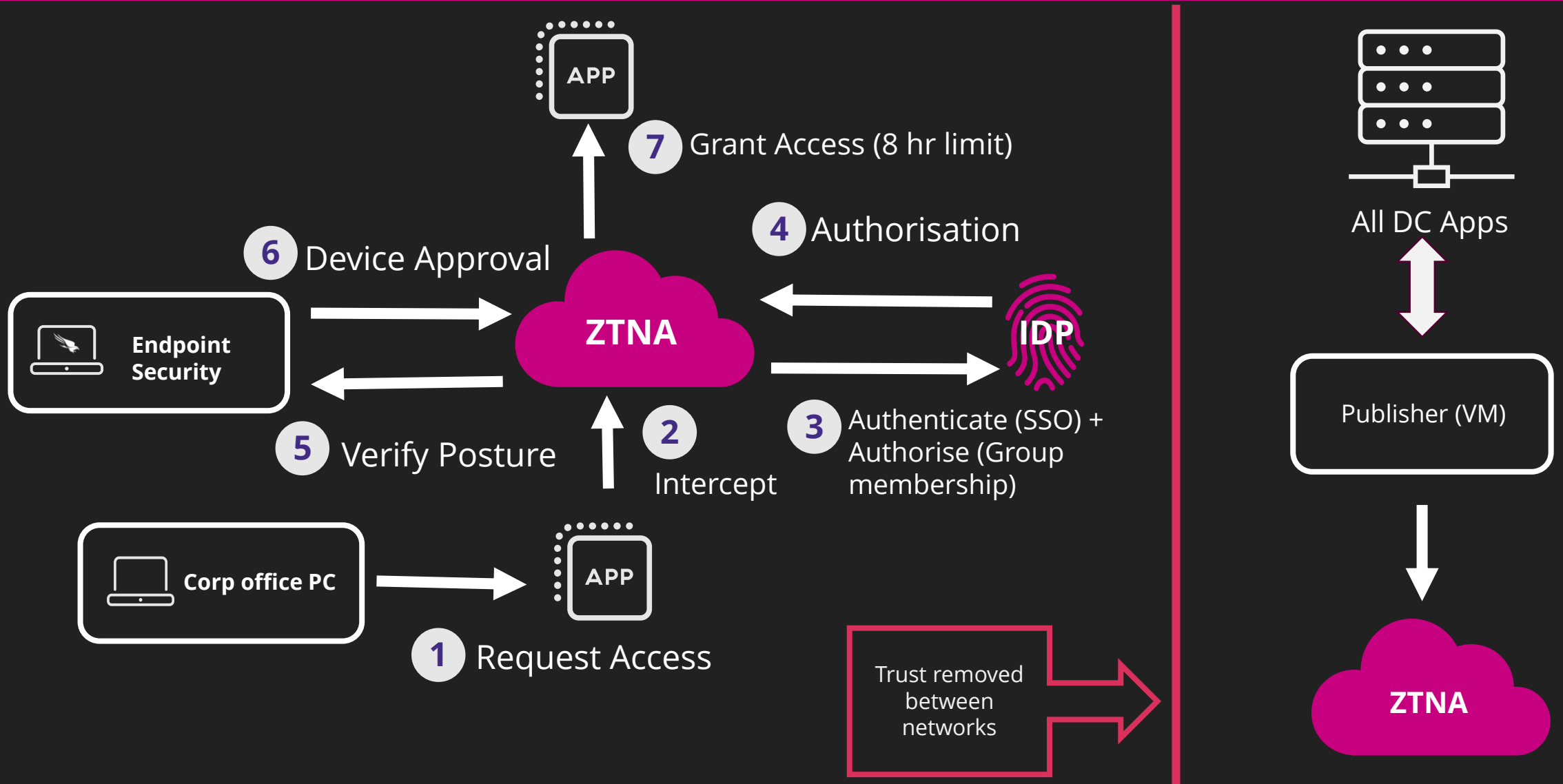


The ZT Way: Connect Remote Users to Private Apps

- Protect private apps from unauthorised access
- Prevent lateral movement via compromised device
- Reduce attack surface by removing VPN gateways
- Scales to hundreds/thousands of apps/users.



Corporate Office – Zero Trust Network Used Internally




Thank you