TECH TITAN

VERIFY · LIMIT · MONITOR

Gun Chun Len

Trust should be earned at every connection

Managing Director & CEO · Tech Titan Group

A Zero Trust approach for modern workforces, distributed infrastructure and partner-connected business.

Connect on LinkedIn

THE PERSPECTIVE

Never assume. Always verify.

IDENTITY | DEVICE | CONTEXT | ACCESS

Practical security leadership connects technology decisions to business outcomes.

THE STRATEGIC CONTEXT

The network boundary is no longer enough

People, workloads and partners connect from many locations and devices, making location alone an unreliable signal of trust.

Zero Trust replaces broad, persistent access with decisions based on identity, role, device state and context.

Gun Chun Len's practical view is to implement Zero Trust as a staged operating model—strengthening the highest-risk access paths first.

01

THE OPERATING AGENDA

Four decisions behind every trusted session

01

IDENTITY

Verify who is connecting

Use strong authentication and reliable identity information before granting access.

02

DEVICE

Assess connection health

Consider device ownership, configuration and security posture as part of the decision.

03

ACCESS

Enforce least privilege

Limit each user or system to the specific resources required for its current task.

04

BEHAVIOUR

Re-evaluate continuously

Monitor activity and change access when context or risk no longer matches expectations.

02

THE LEADERSHIP LENS

Zero Trust without unnecessary friction

PRIORITY

Begin with critical resources

Protect administrative access, sensitive data and remote connections before expanding.

DESIGN

Make policy understandable

Clear access rules are easier to operate, audit and improve.

BALANCE

Protect productive work

Strong controls should enable secure collaboration rather than create workarounds.

FROM STRATEGY TO ACTION

Build Zero Trust in manageable stages

Treat Zero Trust as an ongoing programme connecting identity, network, endpoint and operational teams.

Explore Zero Trust Security

01

Identify high-value access paths

Map who can reach critical applications, infrastructure and data.

02

Remove unnecessary privilege

Reduce standing access and separate administrative responsibilities.

03

Add identity and device context

Use more than credentials when deciding whether access is appropriate.

04

Monitor and refine policy

Review denied access, unusual behaviour and operational impact regularly.