# Application Security

## LEADING DIGITAL BUSINESS TRANSFORMATION SERIES: MODULE 6

# SECURING THE WAY TO DIGITAL TRANSFORMATION

If an organisation wants to achieve digital transformation, protecting workload data and securing the environment is vital.

But there are so many threats out there, from Ransomware and Crypto Mining to disruption attacks like Not Petya.

It's a serious challenge for IT teams. So Cisco advocates an Application First Security Architecture that draws together powerful technology to safeguard applications – and the infrastructure that supports them.

## WHY OVERARCHING SECURITY IS CRUCIAL

Cyber criminals target organisations in so many ways.Through identity theft, apps and devices.

Workloads now move across multiple locations. And more and more people are using their own devices to access business assets. So organisations can't just rely on building a strong security wall around the perimeter of their digital estate.

**A new approach is needed.**

## ZERO TRUST

A zero trust approach assumes that everyone is a potential threat. It:

- Establishes trust by verification.
- Assesses appropriate levels of access.
- Continually evaluates what threats might look like.
- Minimises attack surfaces

Cisco has many ways to help people adopt this new approach.

## DUO

Duo can be used to protect an application by only making it available to authenticated users.

It allows you to build and impose strict policies that restrict access depending on who people are, what devices they're using and where they're connecting from.

## STEALTHWATCH

Stealthwatch gives organisations the power to look at data flows from different apps and networks, giving a clear sense of any threats within the infrastructure.

## TETRATION

Tetration helps establish zero trust workplace security. You can identify workloads and enforce policies, contain breaches, minimize lateral movement and respond to threat indicators.

- **Maps app dependencies** to give an overview of app communications and reveal services being shared across multiple apps.
- **Generates policy based on application first security** e.g. application workload protection using behaviour and attribute-driven policy for microsegmentation.
- **Delivers a consistent security approach** with the power to implement policies across everything from mainframes to containers – on-premise, at a co-location or in the cloud.
- **Draws data from the network**, bare-metal servers, virtual machines, and containers.
- **Monitors real-time traffic** to see if a policy is being correctly followed – useful when confirming compliance with auditors.
- **Detects workload vulnerabilities,** allowing you to respond by setting up policies such as. quarantining a host or blocking systems at risk.
- **Reduces attack surface** by identifying open ports and processes with no activity, exposed apps, workloads and processes, plus data leaks and signs of compromise.

Tetration draws everything together into one easy-to-use security dashboard. It gives app owners a security score every time they log on, highlights security weak spots, and shows which apps are cause for concern.

## TALOS

All Cisco security technology is backed by the industry's leading threat intelligence service.

Talos

Talos analyses all the telemetry that Cisco technology generates, uncovers the root causes of attacks, identifies trends and then feeds all this back to improve the performance of existing security products

## HOW CISCO SUPPORTS YOU

Without a secure environment people lack the confidence to carry out the digital transformation needed to drive their organisation forward and sharpen their competitive edge.

Cisco can deliver a powerful, intelligent and proactive set of tools and services that can improve the robustness of a business and strengthen its ability to ward off potentially catastrophic attacks across its entire estate.

Request a call