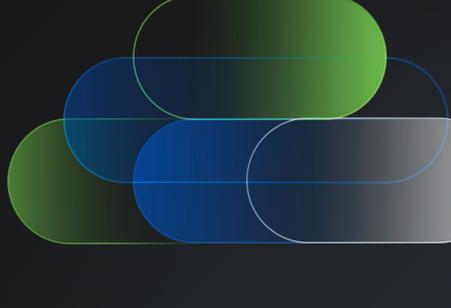


# Meeting users where they are in a hybrid, multi-cloud world

The way we work is making cybersecurity harder. Here's how to achieve security resilience in a multi-cloud future.



## The world of work is changing fast. Is security keeping up?



### 8 out of 10 organisations

have a multi-cloud strategy, which can create chaos. Perhaps that's why 75% of C-suite execs say their organisations are [too complex to secure](#).

Meanwhile, hybrid work is here to stay. [More than half of employees](#) want to be able to log in anytime, from any location, on any device. And 85% of CIOs want to make sure they can. But are they setting Themselves up for success?

## Complexity breeds security chaos

**Complexity is the enemy of security.** The average security team uses **40-50 security tools**. And multiple cloud platforms reduce visibility into threats and vulnerabilities.



## 280 Days

Average time needed to identify and contain a breach

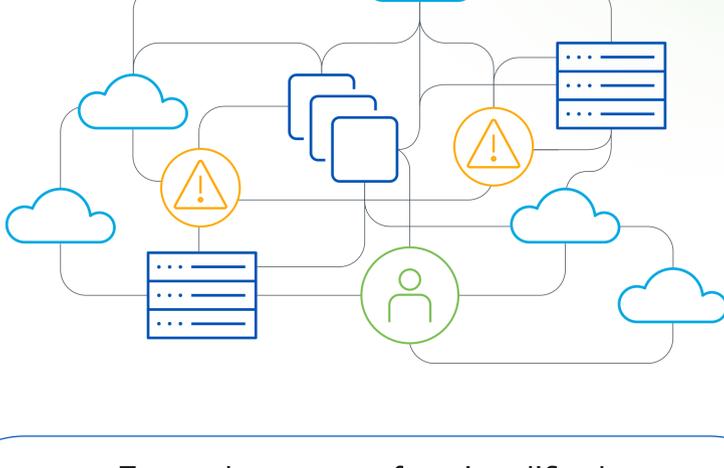
### IT complexity leads to security complexity.

- Security and networking silos
- Cloud vendor lock-in
- Low visibility
- High-friction user experience

## Attackers are taking note - and they're targeting hybrid workers

- 125%** increase in cyber intrusions in 2021
- 4/5** successful web app breaches stem from stolen credentials

## Look familiar? Chaos is hard to hide



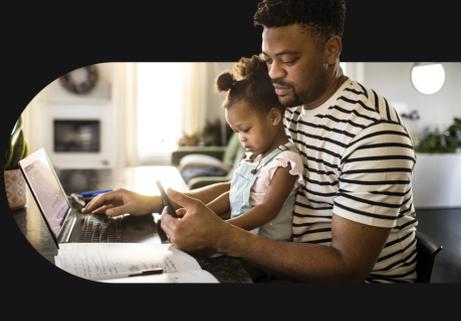
## Four elements of a simplified, unified security environment

It's impossible to tackle new disruptions with old strategies. These next-level challenges call for rethinking how networking and security align with your business.

- Cloud-native**  
Meet users where they are by harnessing the power of cloud security to protect people, networks, apps and data.
- Unified**  
Unified policy management, product consoles and dashboards help security work more efficiently from end to end.
- Frictionless**  
Make security transparent and persistent, but never in the way.
- Open**  
Extensive APIs for broad integration and a robust developer ecosystem, so your environment can evolve along with your business challenges.

## The Cisco Security Cloud

Cisco's vision for end-to-end security across multi-cloud environments is the **Cisco Security Cloud**. This open, unified platform is how we plan to **secure all users, networks and applications** - no matter how complex your environment.



### The economics of public cloud - without the limitations

No more vendor lock-in! API integration, and a developer ecosystem and marketplace keep the Cisco Security Cloud open and extensible for people, networks, apps and data.

### Complete visibility into all threats and vulnerabilities

We're removing silos to gain visibility and actionable insights across networks, clouds, endpoints and applications.

### Intent-based and AI-driven security

Constantly verify user and device identity, device posture, vulnerabilities and more. A unified policy engine will allow users to set policies centrally and propagate them.

### The power of automation!

**74 fewer days** to contain a data breach compared to manual processes

### A frictionless experience for all

Ensure security is effective but invisible with **single sign-on (SSO)** capabilities, an easily replicated **microservices-based architecture** so every connection is protected and more.

### More efficiency, more wins

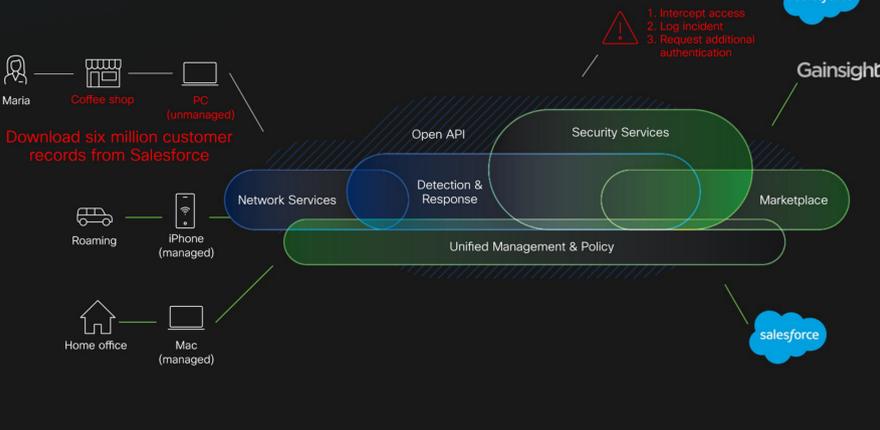
SecOps, NetOps, ITOps and DevOps will all benefit

## Protect everything, everywhere

- On-premises**  
Monitor and defend everything in your data centre, desktop office systems and laptops and mobile devices at home.
- In the cloud.**  
Integrate with the platforms and software you rely on to operate your business, no matter what or where they are.
- Hybrid**  
Protect everything, everywhere with end-to-end coverage.

## Secure and connect everything your business relies on

Continuous Trusted Access



## To learn more, read our eBook: The Cisco Security Cloud

The multi-cloud, hybrid future is already here. Are you ready?