

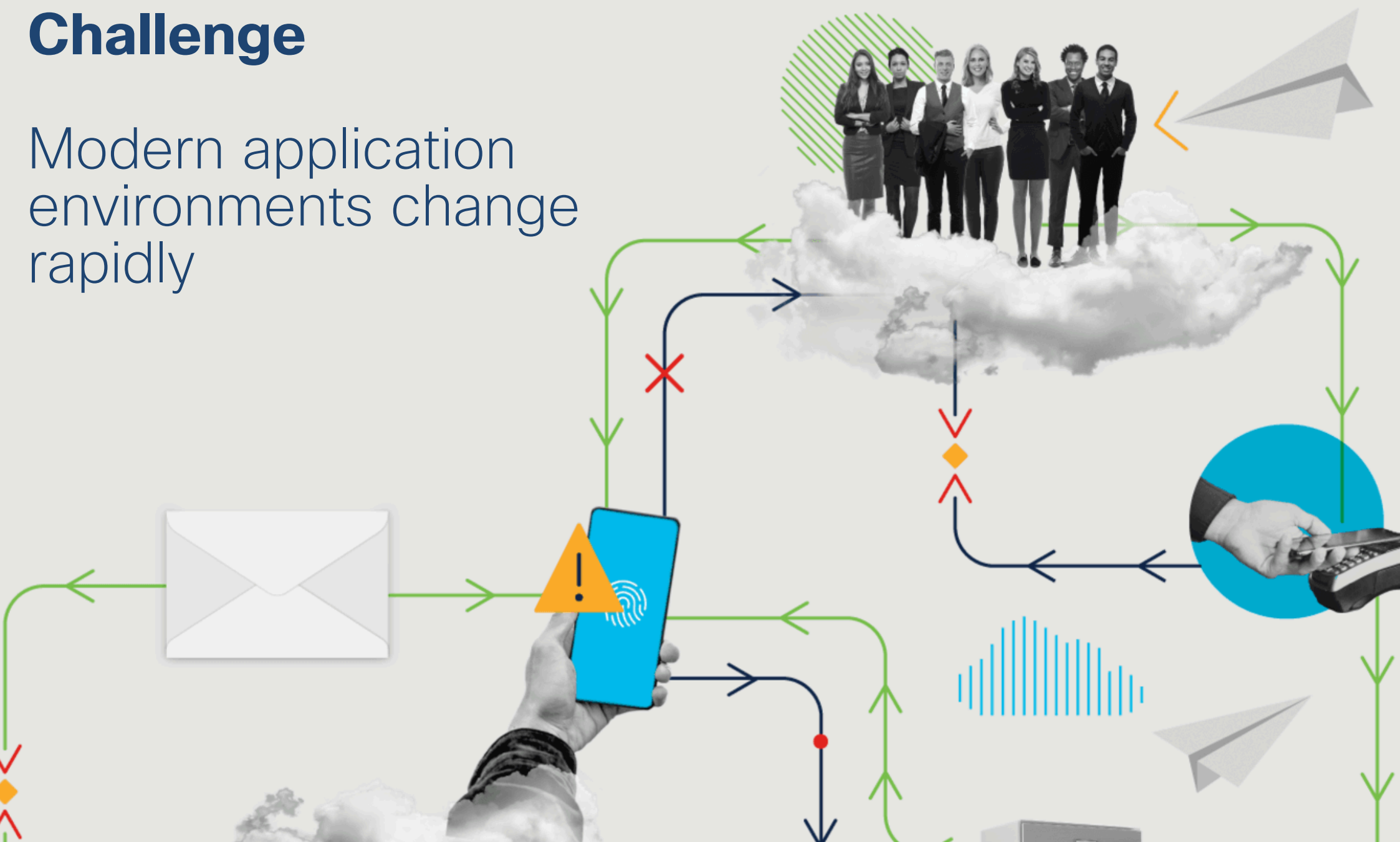
NetWORK: Redefining Network Security



N E T W O R K L O A D

Challenge

Modern application environments change rapidly



It's challenging for the firewall team to keep up.

Today's dynamic applications, so important for business success, create challenges for your security teams.

Protecting them takes a lot of work.



Survey

Cisco co-sponsored
a cloud native
security study

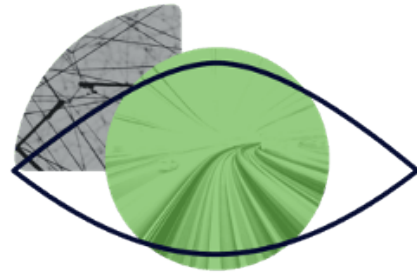


The Survey Says...



We polled 486 senior IT decision makers and security professionals.

- 50% polled: at least **\$250 million** in revenue
- 50% polled: at least **\$1 billion** in revenue
- Across eight industries: financial, tech, retail, manufacturing, education, government,



Lack of visibility is a key concern

73%

lack actionable insight
into threats & ongoing attacks



Top three drivers for hybrid and multicloud application development

- **40% - modernizing** the most critical parts of the business
- **31% - best practices** for modern application development
- **29% - operational cost savings** projected



Risk & Loss

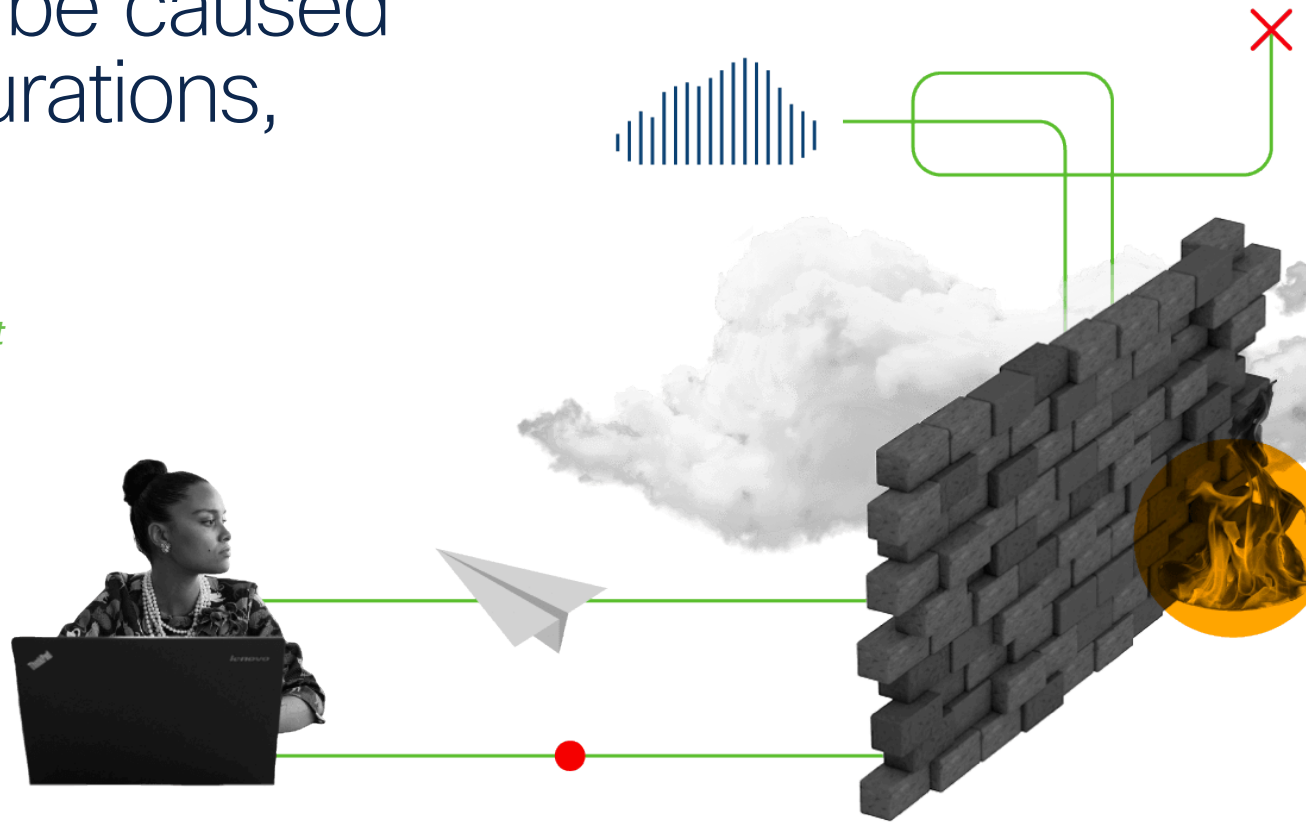
48%

said production environment attack(s) have caused damage Resulting in **system damage (48%), customer data loss (44%),** and **financial data loss (31%)**

What does this mean for firewall operators?

“Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws.”

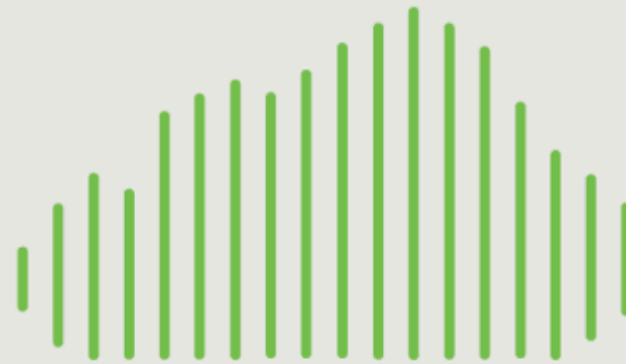
Gartner Technology
Insight for Network Security Policy Management



What we observed:

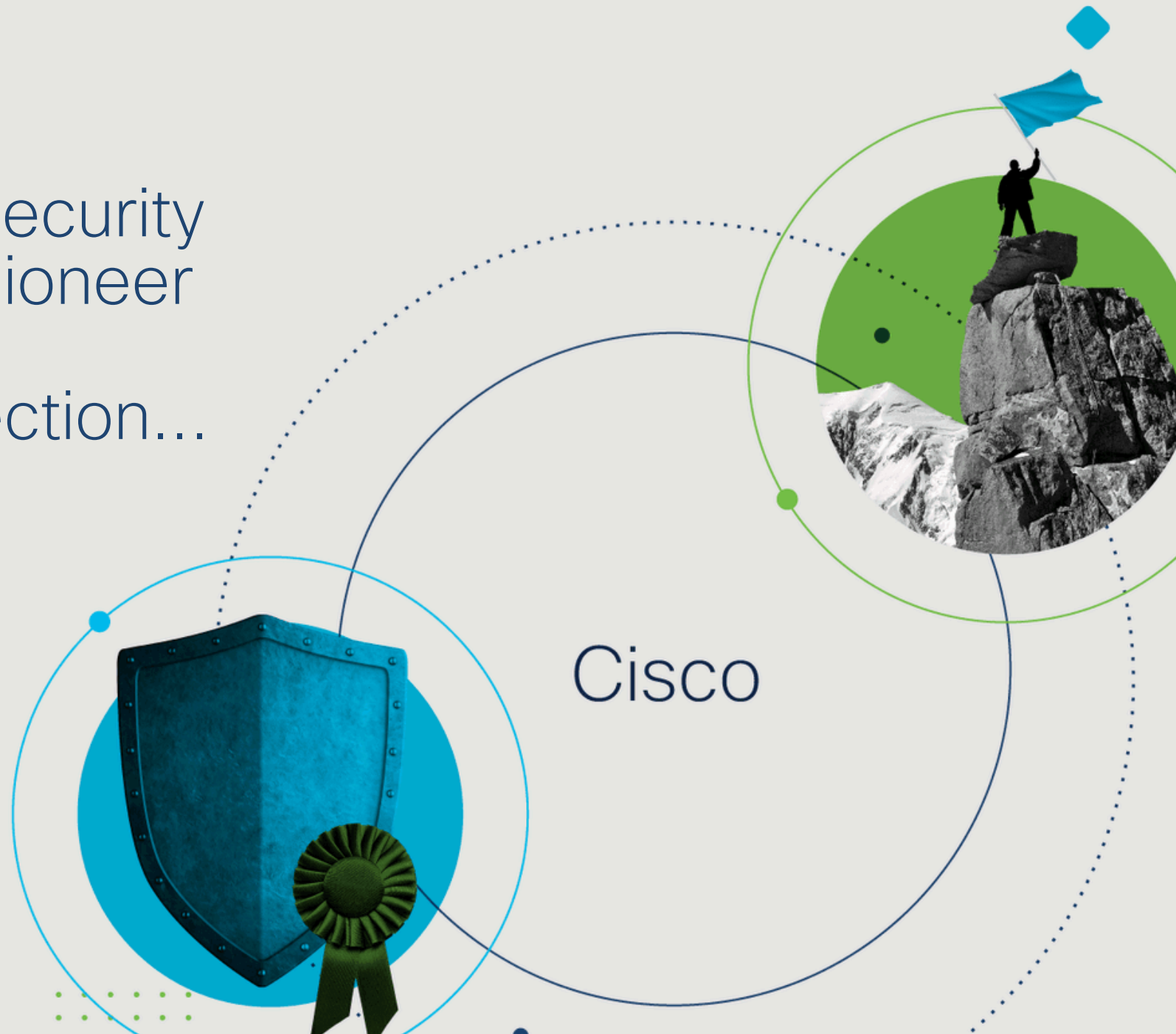
There's a chasm between Network Security and Application Development.

Security isn't keeping pace with the speed and complexity of the multicloud application world.



Solution

As a network security leader, and a pioneer in application workload protection...



we've brought the
two together,
redefining *network*...



Cisco

N E T W O R K [] [] [] []

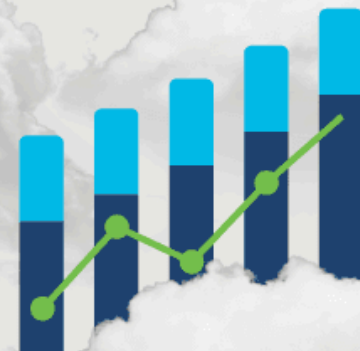


*and workload
security into...*



Cisco

■ ■ ■ **W O R K L O A D** ■





Cisco NetWORK Security

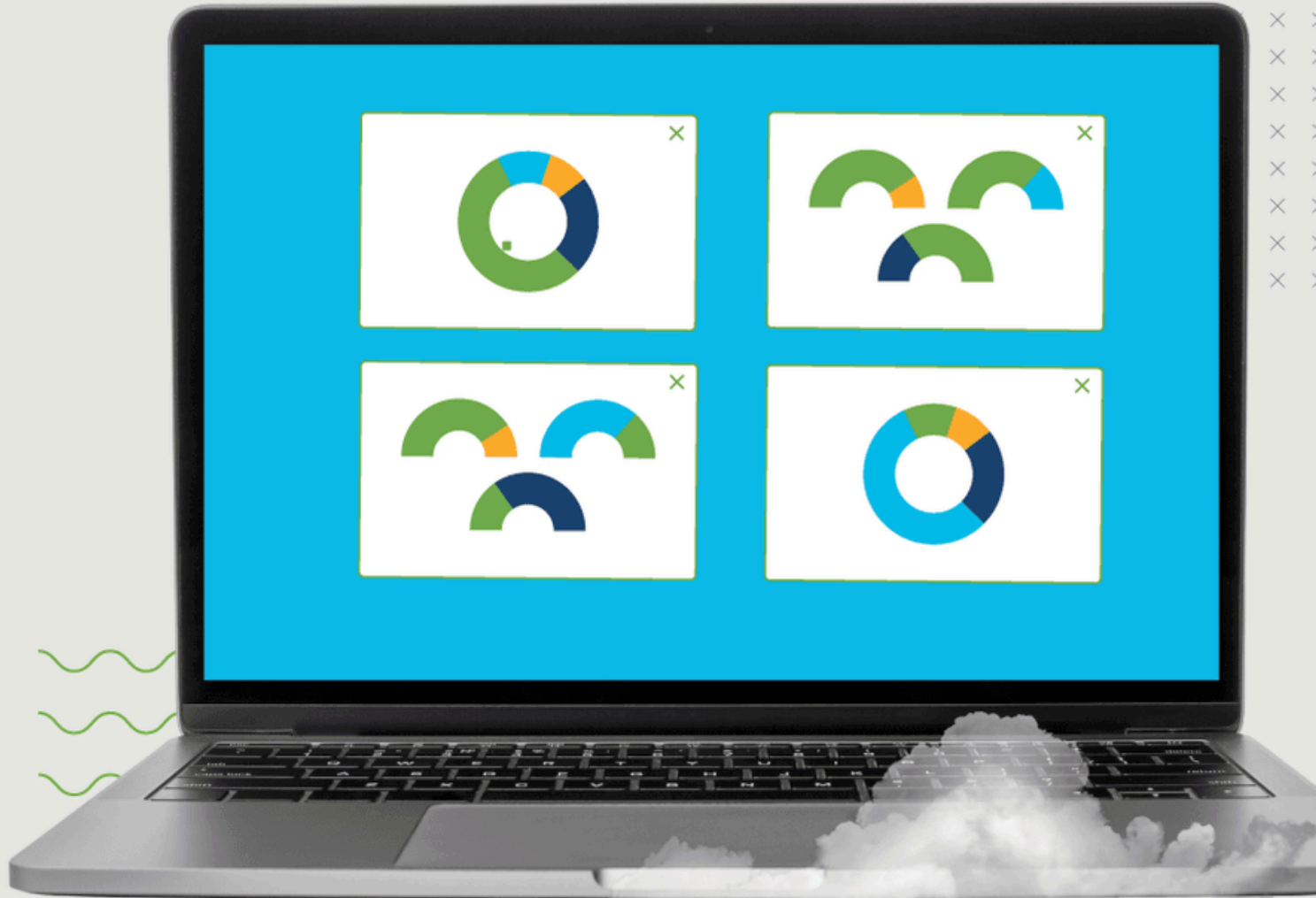
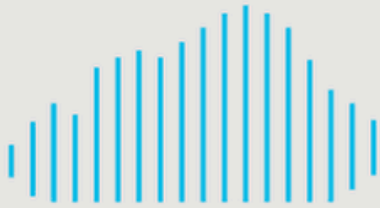
where automation,
intelligence, and
dynamic policies....



Enable your NetOps team to start running at DevOps speed.



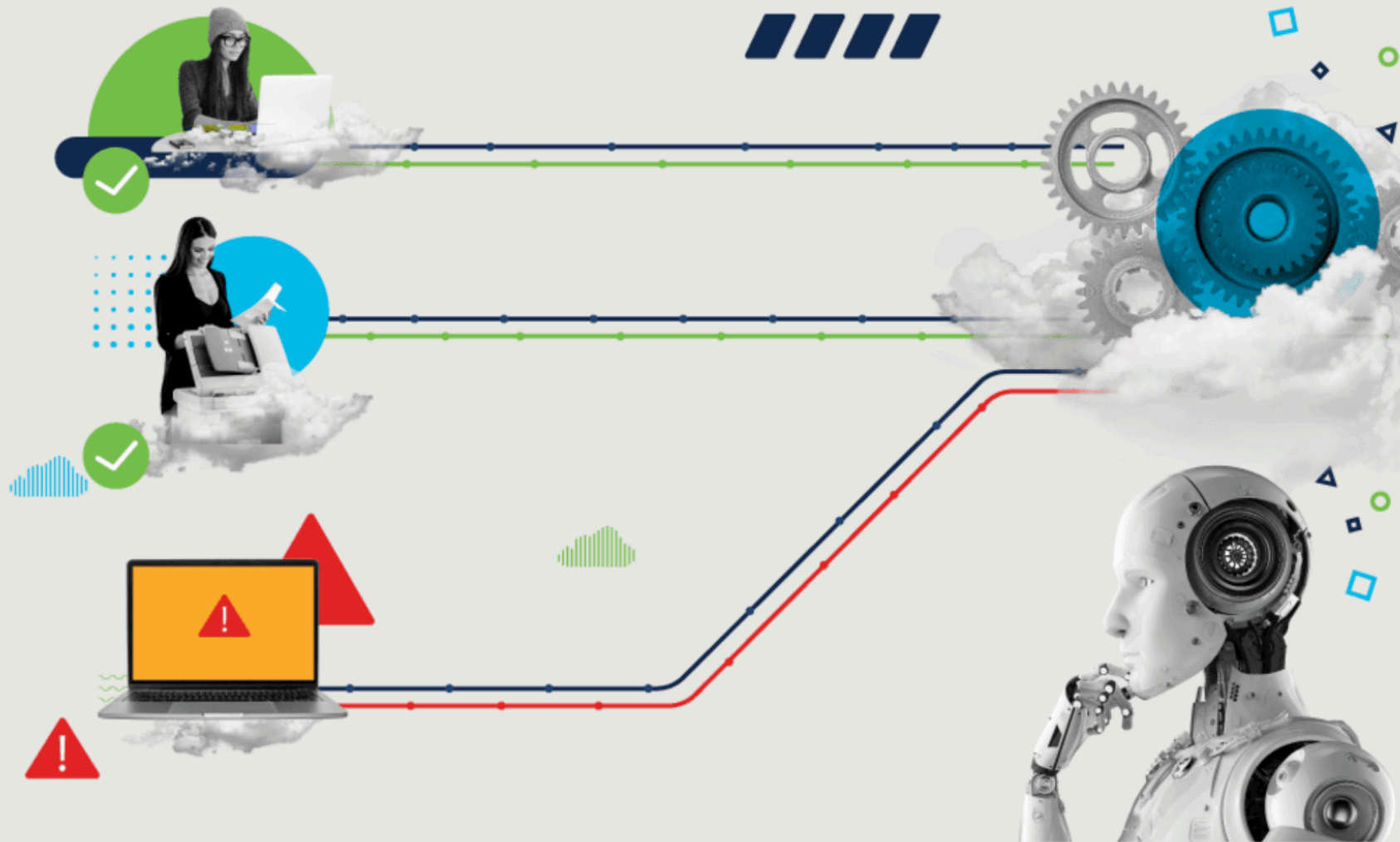
As applications
change



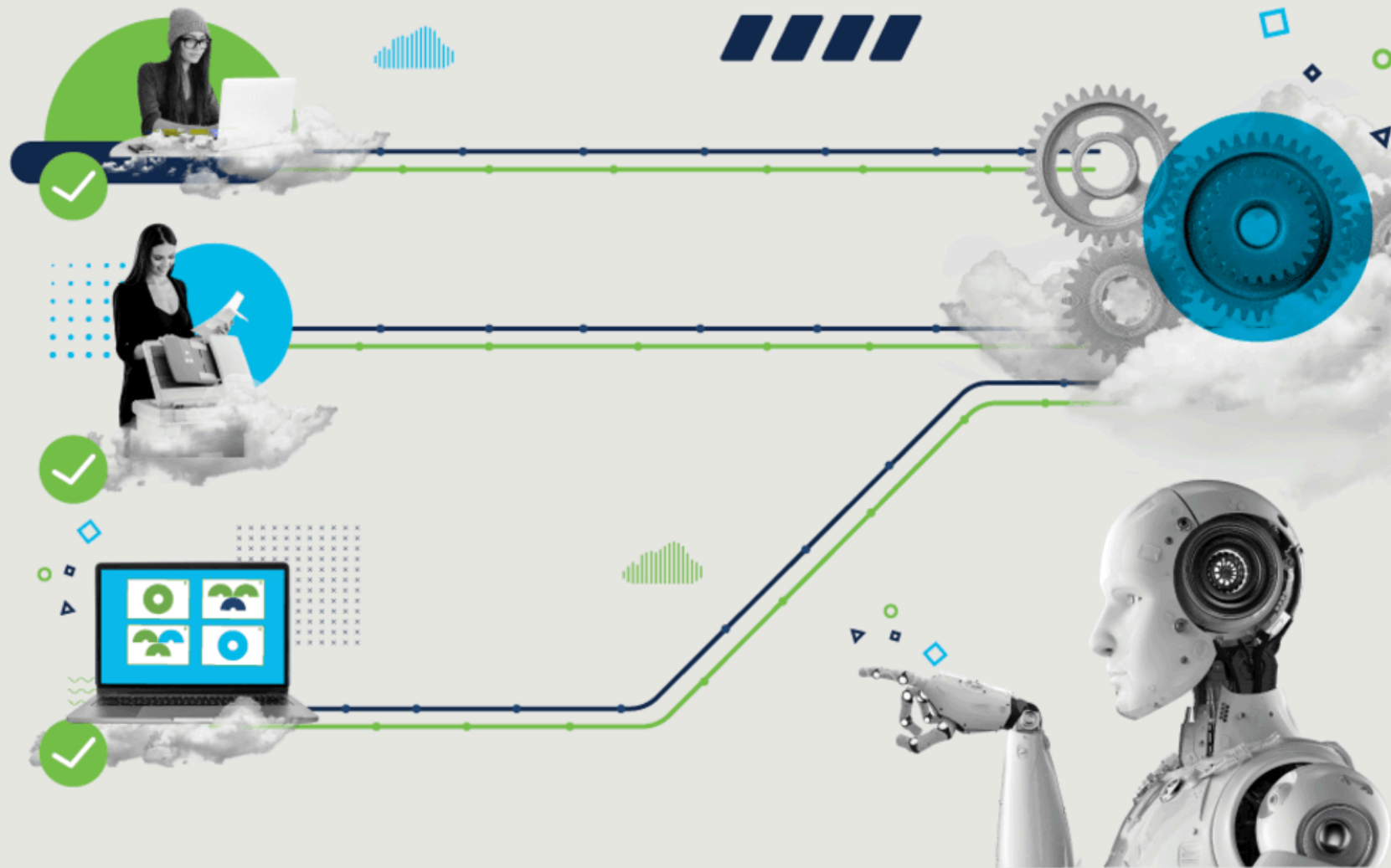
and new workloads
come online



Cisco Secure Workload provides comprehensive visibility



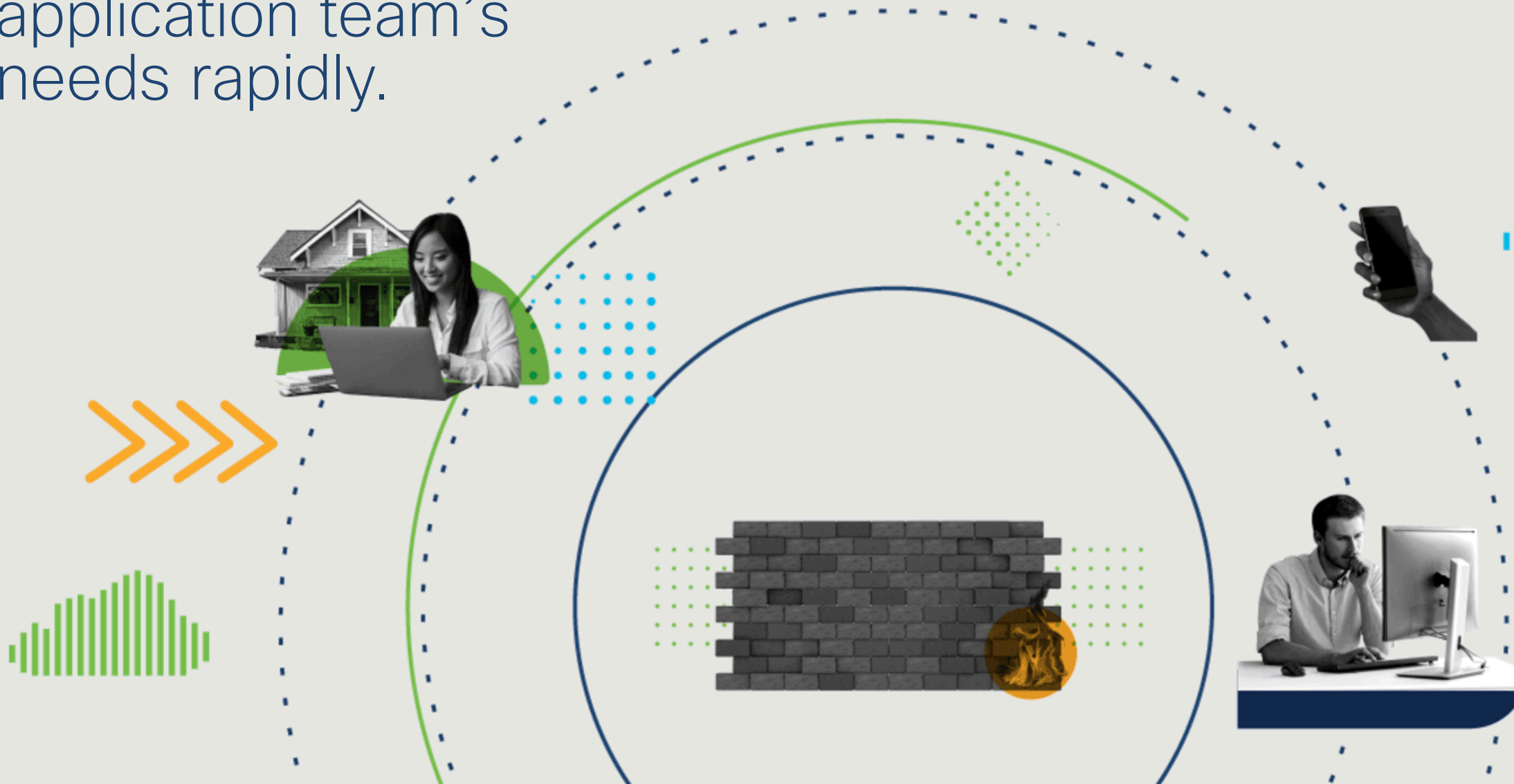
and automated policy recommendations on-the-fly.



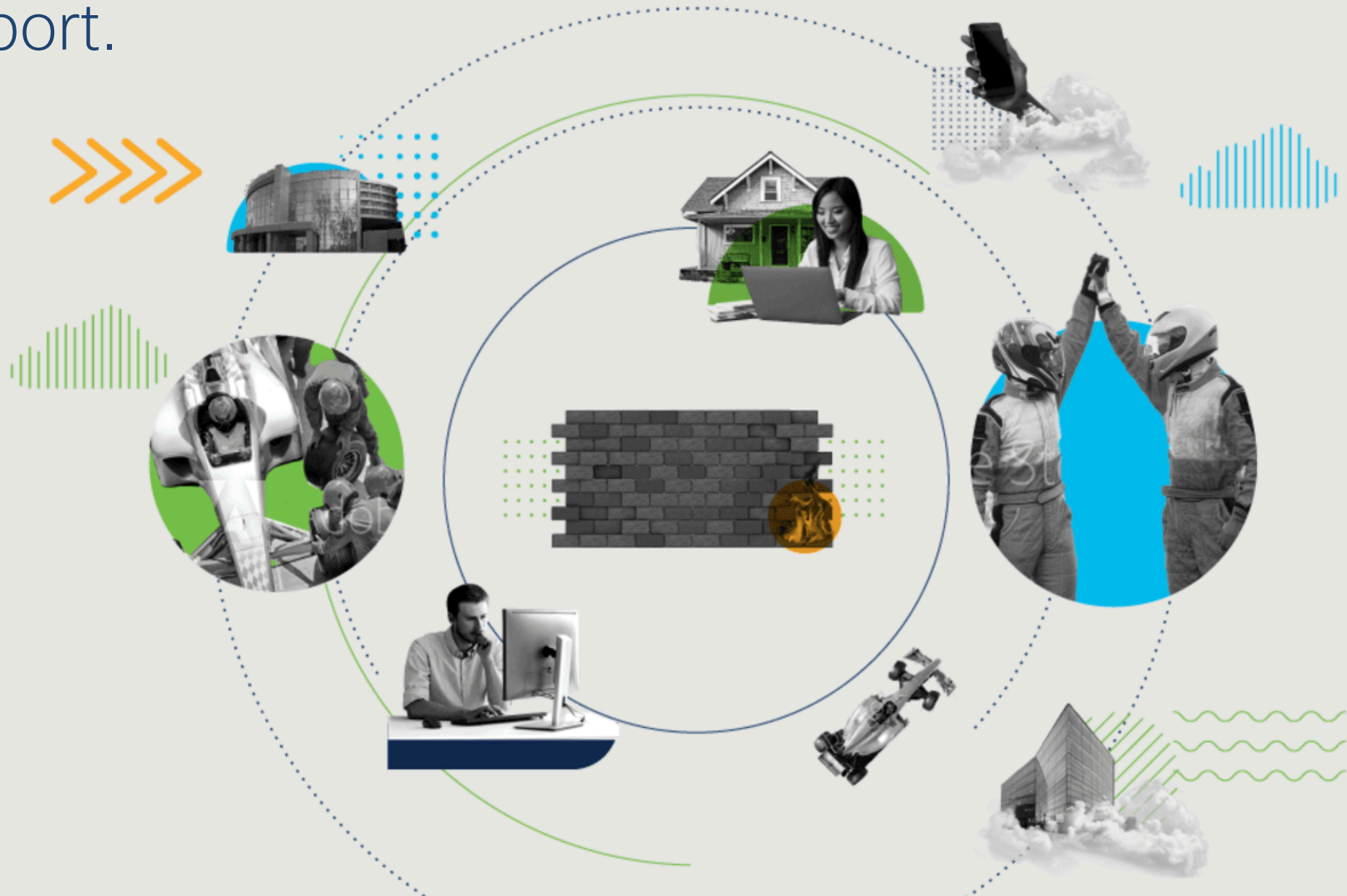
This context is shared dynamically with Cisco Secure Firewall,



so your firewall team
can support the
application team's
needs rapidly.



After all, security is a team sport.



Secure Firewall also enhances your security posture...



With threat inspection
across your network,
data center and
cloud.



You can inspect
critical flows with
Snort 3 IPS,

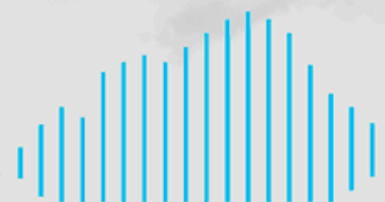


Snort 3 IPS

and leverage the scalability of Secure Firewall Cloud Native, a Kubernetes-based firewall.



Kubernetes 



For granular control
at the workload level,
Cisco Secure
Workload



enables micro-
segmentation
enforcement



directly on your applications



It's the perfect choice when you're adopting a zero-trust model.



Take a platform, not piecemeal, approach to your security.



With Cisco NetWORK security you can comprehensively protect your network and your workloads



to securely accelerate application delivery

Cisco Secure Firewall's dynamic policies are driven by intelligence from Secure Workload, protecting network & workload levels of application environments.

As workloads constantly change, you get visibility and automation informing your firewalls of needed network changes.

Results:

Strengthened security posture
Faster application delivery



Thank you for reading

Redefining Network Security

For more information and a demo, [click here](#).



NETWORKLOAD