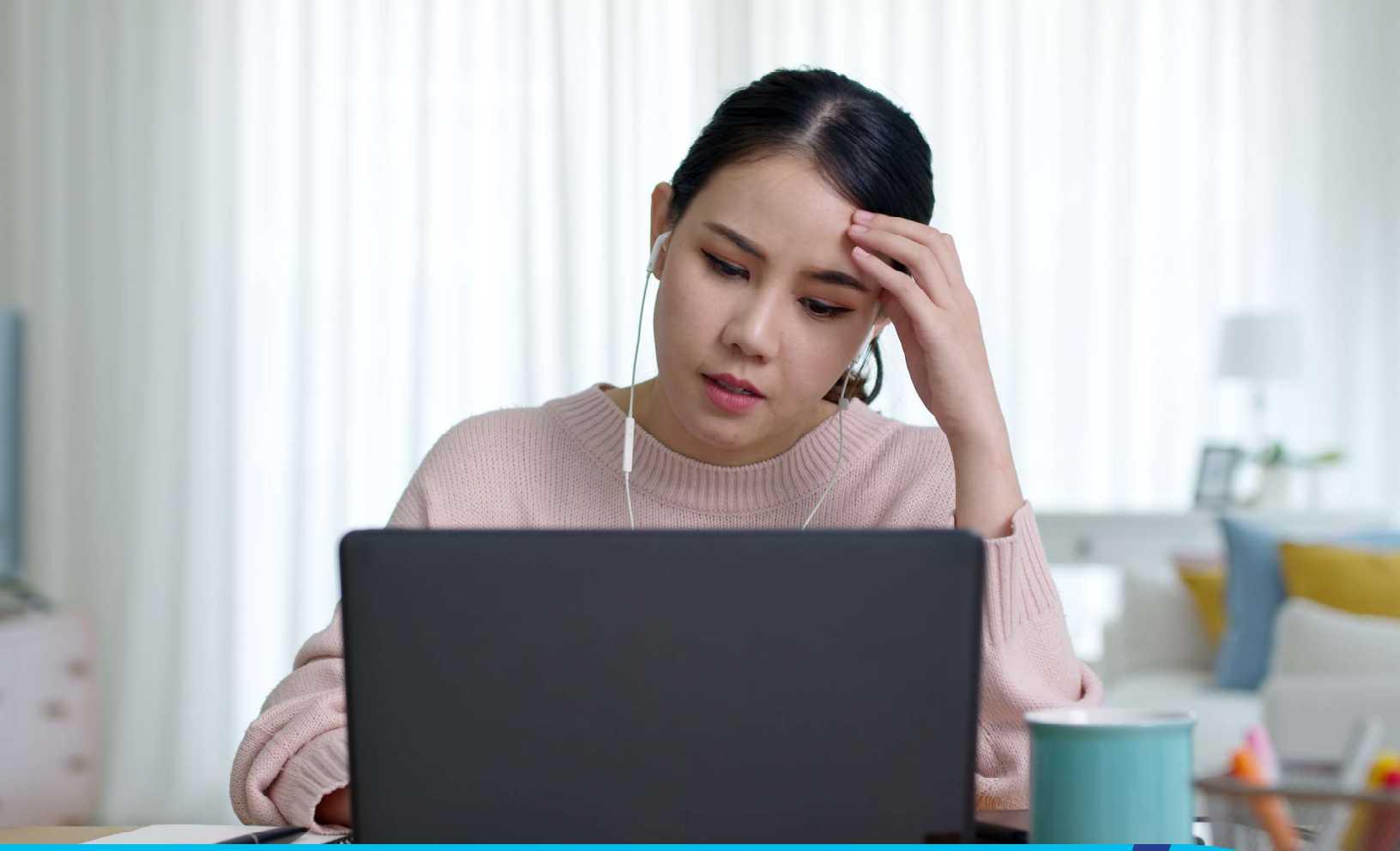


Cisco
Customer Experience

Is your hybrid work security posture a business enabler or disabler?

Guide

Guide
Cisco public

Creating a seamless hybrid work and strong security posture is a delicate balancing act.

The security stakes have never been higher.

400%
Increase in cyberattacks and 600% rise in cloud cyberattacks[1]

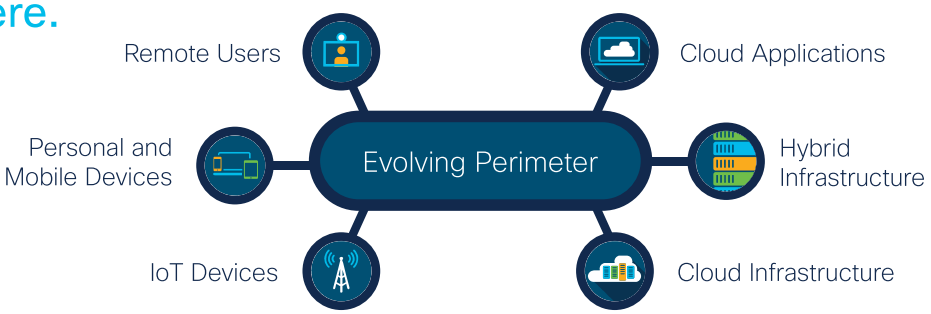
$1 trillion
Cybercrime cost to the global economy[2]

$25 million
Network downtime can top $25M or more a year[3]

36% of employees have picked up bad cybersecurity habits since working remotely[4]

39% of employees admit they practice different cybersecurity practices at home[5]

Enterprise security has changed – users, devices, and apps are everywhere.



"The legacy data center as the center of the universe network and network security architecture is obsolete and has become an inhibitor to the needs of digital business." - Gartner

You'll face many challenges when protecting your infrastructure – don't let a lack of security expertise be one of them.

Evolving threat landscape

INCREASED WORKLOAD
Overworked cybersecurity employees are struggling to keep up with the challenges of the job.

EVOLVING SECURITY NEEDS
Cybersecurity is a never-ending race, with new risks, technologies, and bad actors each year.

COMPLEX OPERATIONS
Data must be protected in multiple databases, app, cloud file systems, and SaaS.

Evolving technology

SECURITY TOOLS
Too many cybersecurity tools can be as bad as too few; in 2022 the average organization has 76 (up from 64 in 2019).[6]

INADEQUATE INTEGRATION
Siloed tools aren't integrated into a standardized cybersecurity protection framework.

KNOWLEDGE GAPS
Maintaining institutional knowledge is a challenge.

Lack of skills

SKILLS GAP
86% of CIOs can't find necessary talent for cyber, cloud, and data security.[7]

HIGH TURNOVER
72% of those in IT / tech jobs are thinking of quitting in next 12 months.[8]

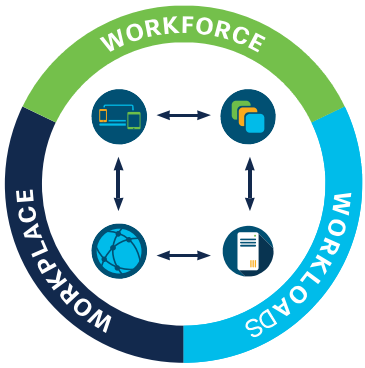
SILOED EXPERTISE
Decentralized IT leads to siloed protection within the organization.

Secure hybrid work can only be delivered by sustainable and agile security at scale.

A multi-architecture approach with embedded security is needed to secure your workplace, workforce, and workloads.

Employees, contractors, vendors, and partners accessing work applications

All devices that connect to the enterprise network to support hybrid work



All APIs, microservices, and containers accessing a database within an application

Make your hybrid work infrastructure robust, resilient, and flexible with Cisco® Business Critical Services

Cisco can help you secure all access across your applications and environment, from any user, device, and location.

Business Critical Services cover:

Strategy, architecture, and design: Security policy and risk management recommendations, architecture blueprint best practices, capacity planning models for scale.

Ongoing assessments: Proactive testing of network devices, security compliance and risks to analyze and minimize gaps for fewer vulnerabilities – from core to edge.

Optimization: AI + human intelligence with automated workflows – enhancing visibility and providing proactive threat detection and remediation throughout IT lifecycle.

Security upskilling: Build in-house IT security knowledge through workshops and webinars – teaching the latest tactics in cyber warfare.

REPSOL

Customer challenge

- Develop a proactive security posture for a large global infrastructure.

Solution

- Migrate to the cloud while maintaining highest security standards.
- Proactively address millions of security threats with automation and AI

Results

- Quicker and more secure product deployments.
- Reduced attack surface

Learn more about Repsol's success story:
https://www.cisco.com/c/m/en_us/customer-experience/customer-stories/repsol-security.html

253% ROI in 3 years[9]

4 months to break even[10]

54% fewer unplanned outages[11]

2x more staff time spent on innovation[12]

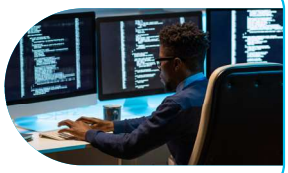
Trust the company that has secured its own hybrid work for more than 15 years.

At Cisco we believe that work is not where you go, it's what you do.

Hybrid-First Pre-Pandemic

Every day, we protect our enterprise by securing:

- 134K combined global workforce
- 3600+ routers
- 19K+ virtual office connections
- 2,200+ IT applications
- 750+ engineering labs
- 500+ cloud applications



With these experts:

- Cisco Talos® is one of the largest commercial threat intelligence teams in the world
- 34,600+ employees certified in foundational security training
- 700+ security advocates and officers
- 100 dedicated incident responders around the globe
- 80+ pen testers dedicated to attacking Cisco's products and solutions

Next steps

Schedule a workshop to identify areas of vulnerability and ways to increase your security posture.

Cisco **Customer Experience**

Sources: 1. ZDNet Week September 2020 « 2. TechRadar, Feb 15, 2021 « 3. HelpNet Security, April 24, 2020 « 4,5. Security Magazine, June 22, 2021
6. Panaseer 2022 Security Leaders Peer Report « 7. Chief Executive Magazine, Sept. 3, 2020 « 8. Business Insider, Oct. 19, 2021 « 9-12 IDC Business Value Snapshot, September 2021