Table of Contents

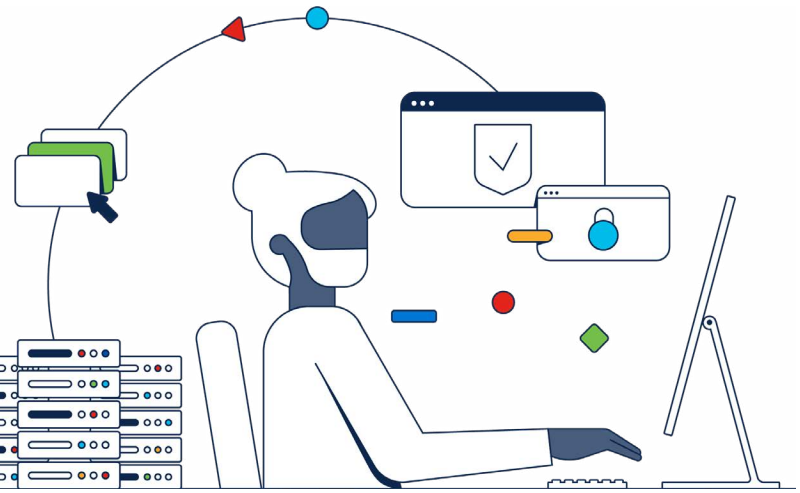
Security made for growth, backed by trusted partners.

Take action with security solutions from Cisco and Microsoft—made to protect every moment in the life of your organization.

Your network perimeter isn't what it used to be. Due to the evolution of your workplace and its workflows, there's an ever-present need to protect your network, cloud, and users.

With Microsoft Azure as your cloud environment provider, Cisco is there to help you easily extend your security solutions. And as your applications expand, and you need to protect your network in new ways, look no further than the Microsoft Azure Marketplace for your Cisco software. Discover how you can implement extra layers of security for a hybrid workplace—covering any of your on-the-go users. Map out goals for your organization, and take a holistic approach to security, with solution access and management all in one place.

Cisco and Microsoft provide more than a one point solution to fit your organization's changing workflow and network requirements. Cisco applications like Umbrella, Secure Firewall, Duo, Secure Endpoint, Cisco Identity Service Engine (ISE), Talos, Secure Email Threat Defense, and Secure Workload keep your organization and users safe. Make the most of the cloud to scale with ease and confidence.



- **Leverage expertise from the best partners in the business**
- **Save time and resources with secure solutions**
- **Identify more threats and prioritize the right responses**

Secure your dynamic environments against new and emerging threats.

Secure Firewall gives your organization always-on, anywhere security.

As your organization advances its hybrid and multicloud journey, your network becomes more complex. These complexities limit key security functions like visibility, control, and the ability to gain context. With users and applications distributed across dynamic environments, resulting security gaps increase business risk, and make it difficult for NetOps and SecOps teams to keep up.

Cisco Secure Firewall gives you consistent security, deep visibility, and advanced threat defense options to maintain business continuity when unpredictable threats and changes arise. Identify and detect threats faster, boost efficiency with easier operations, and realize greater return on investment (ROI) by lowering your total cost of ownership (TCO).

As workers, data, and offices are in distributed locations, your firewall is more relevant than ever before. Secure Firewall helps your organization plan, prioritize, and close gaps with robust protections against even the most sophisticated threats—to bring visibility back to your team, and protect your data wherever it may roam.

Make operations easy

Only productive and efficient security programs succeed. In addition to the current physical and virtual management appliances, Cisco now boosts productivity further with a new SaaS version of its popular Firewall Management Center, so you can manage firewall policies anywhere in the world. With this cloud-delivered solution, you can administer firewalls, correlate and prioritize threats, as well as quickly act on them—all in one place.

Organizations can also use Firewall Management Center to save time when overseeing policies in dynamic environments where static IP addresses are not available. With dynamic attribute support for Azure tags and more, policies can be kept current while reducing maintenance and complexity.

Identify more and detect faster

Threats are continuously evolving, so your firewall protection needs to evolve, too. Cisco Secure Firewall receives continuous, automated threat intelligence updates from Cisco Talos, one of the world's largest commercial threat intelligence teams, protecting your organization from new and emerging threats.

Cisco Secure Firewall's best-in-class visibility and protection does not compromise performance. With Snort 3 IPS, you can run more rules, with less resource consumption, for greater visibility and better performance. Snort 3 rules are also human-readable to simplify your experience.

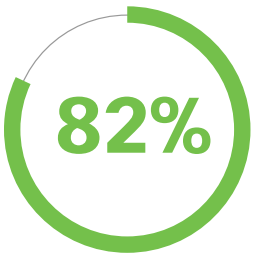
Achieve greater ROI and lower TCO with automation

Delivering on our promise to drive simplicity and lower TCO, Cisco commissioned Forrester Consulting to perform an unbiased cost-benefit analysis of Cisco Secure Firewall to measure its operational efficiency and threat efficacy over a three-year period.

Key highlights include:

- Investment in Secure Firewall with its Firewall Management Center produced a **195% ROI**, **$12.29M** net present value and a 10-month payback period for a typical customer
- Up to **95%** reduction in routine firewall task time
- **55** hours saved on policy, deployment, and updates
- **49%** time savings in threat detection

To learn more about the economic benefits, operational efficiencies, and threat efficacy of Secure Firewall, view the Forrester Total Economic Impact of Cisco Secure Firewall report here.

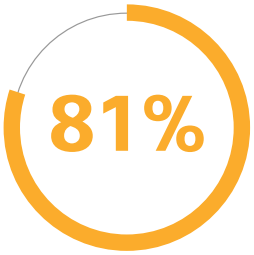


of IT leaders have adopted hybrid cloud.

Source: 2022 Global Hybrid Cloud Trends Report

One way to control security in the cloud.

Comprehensive cloud-delivered security, including DNS-layer security, Secure Web Gateway, Cloud Access Security Broker, Cloud DLP, and remote browser isolation from Cisco Umbrella is a single place for cloud-delivered security everywhere, combining multiple security functions into one.



in the security industry say orchestration between products is challenging.

Source: CISO Benchmark Study 2020

With workers distributed around the globe, your organization's security posture should be covered from all fronts. Security must extend to devices and remote users at every location. By seeing, protecting against, and learning about current and emerging threats to your network, you can create a more resilient cloud-based architecture.

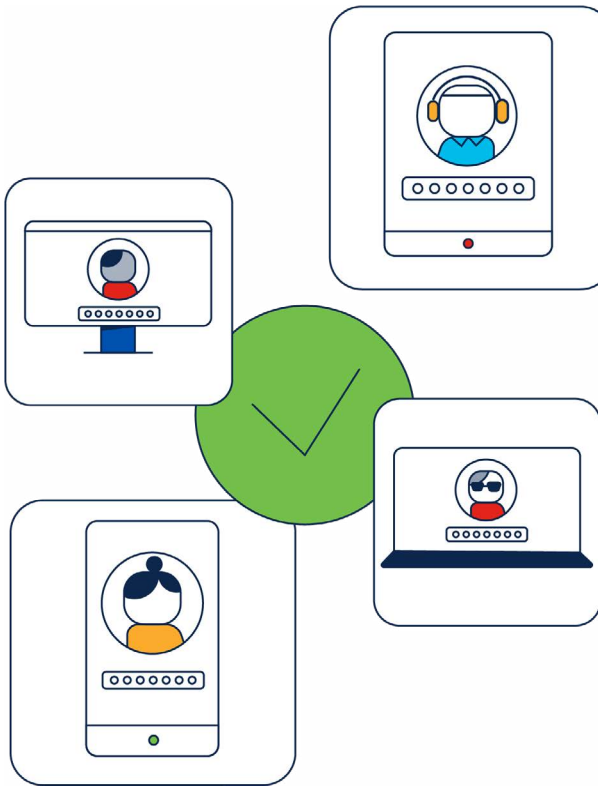
Cisco Umbrella makes it easy for you to oversee the security of your cloud users and applications. Prevent accidental or deliberate exposure to malicious domains with DNS-layer security, and take action by identifying and blocking domains involved in phishing attacks. See into workload activity, and detect threats quickly. Establish DNS policies to address your specific user and application needs in the cloud, and across other sites—for instance, Azure cloud applications.

Access features like

- Secure web gateway
- Cloud-delivered firewall
- Cloud access security broker (CASB)
- Interactive threat intel

Secure your remote and hybrid users.

Ensure access to private or SaaS applications—across and beyond the Microsoft ecosystem—is seamlessly covered with strong security solutions like Duo.



Cyber attacks have been targeting multi-factor authentication (MFA) at unprecedented levels. Duo's identity and access management ensures security efficacy, and a secure network experience for your users, wherever they are. Duo's reach across your full workforce—from employees to contractors and partners—ensures your network is accessed with reduced risk.

Securely access internal applications, or cloud-based applications like email through Office 365, from any device on any browser. And with two-factor authentication for remote users and applications, get complete visibility into all devices that are granted access, including corporate-managed and unmanaged devices. Implement features like:

- Role-based access control
- Single sign on
- Device trust
- Remote access
- Adaptive access and compliance policies

Once your organization has gained visibility across devices, go even deeper. Decide which devices you trust across managed and unmanaged devices, create user trust policies across all employees, and apply policies on an application by application basis—specific to private or SaaS applications.

With these policies in place, you can take security action. Notify users about vulnerabilities, and make sure they have relevant upgrades in place for protection. Ensure credentials are secure, and that your organization is on top of risky devices. And that's just the beginning.

Level up user protection.

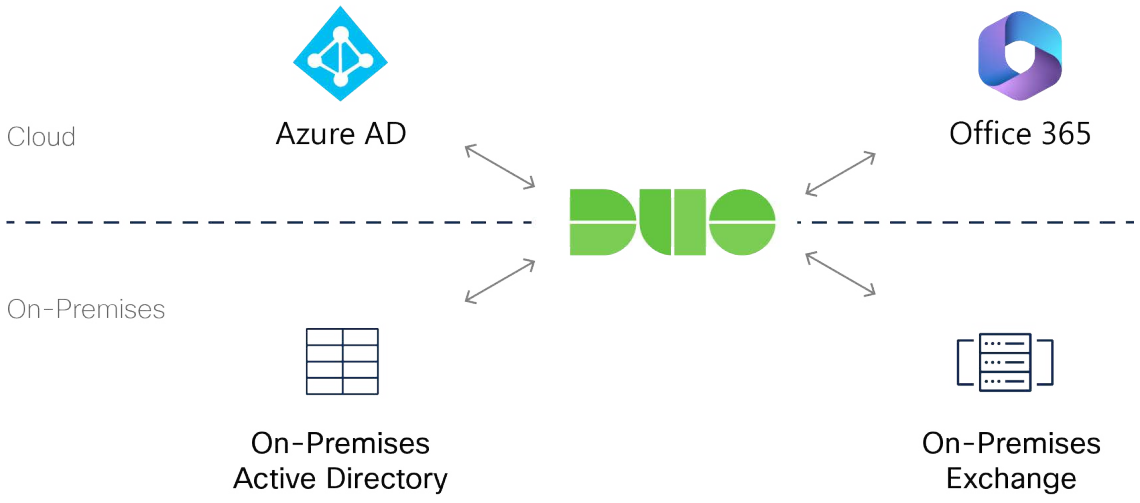
It's easy to deploy Duo and establish user trust, gain visibility into bring your own device (BYOD), enforce adaptive policies, and implement role-based access control.

increase in Microsoft brand impersonation phishing emails in January to March 2019.

Source: Agari Data Inc.

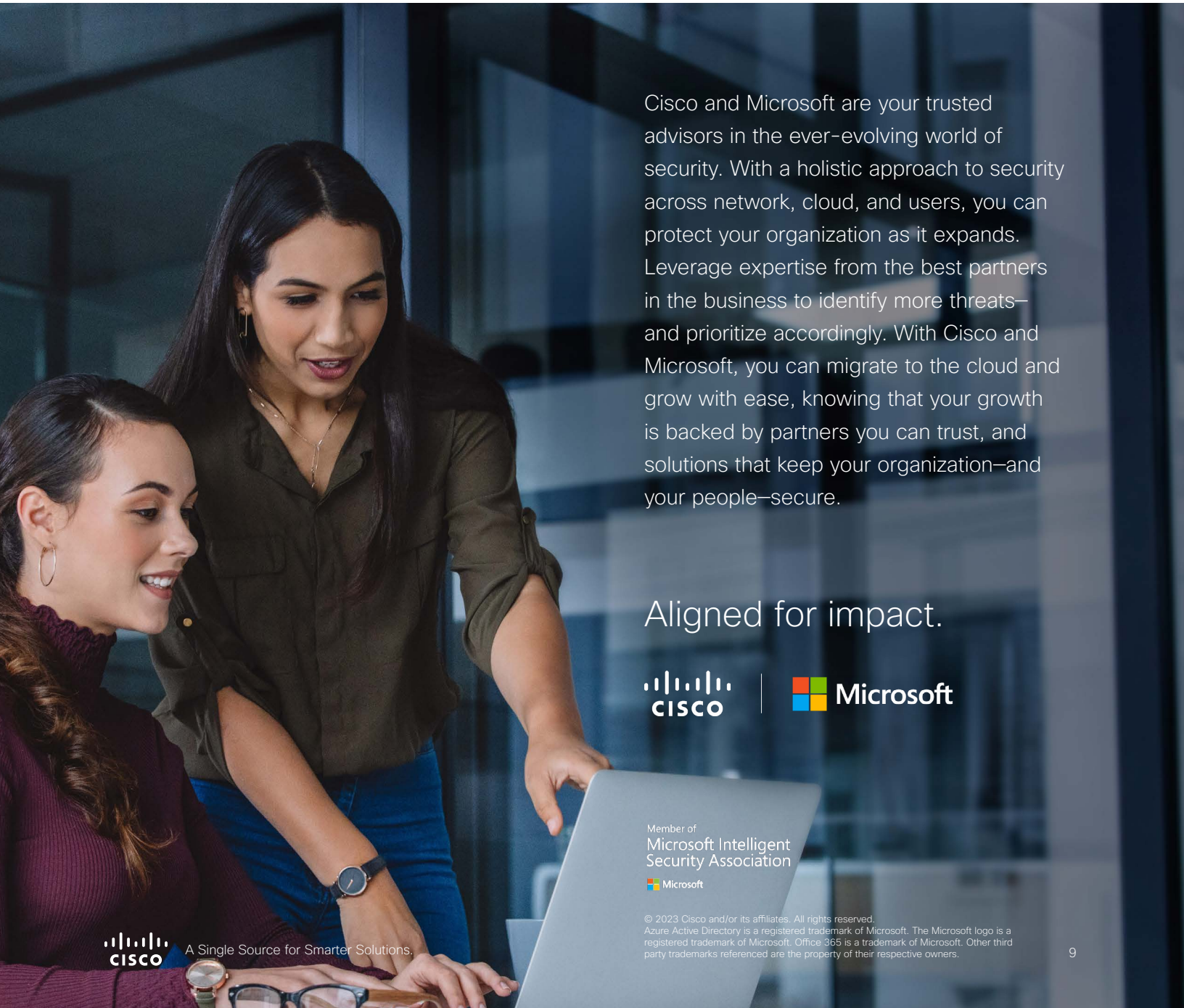
By using Duo, your organization can answer questions like:

- Can you identify your users and where they log in from?
- Is my user's browser up to date?
- Which specific users have access to applications, whether cloud or on-prem, and on which devices?
- Which of these devices is potentially vulnerable to exploits and attacks?
- Are compliance requirements being met across devices?
- And more



Here. There. Everywhere.

Take a holistic approach to security, and protect your organization as it grows.



Cisco and Microsoft are your trusted advisors in the ever-evolving world of security. With a holistic approach to security across network, cloud, and users, you can protect your organization as it expands. Leverage expertise from the best partners in the business to identify more threats—and prioritize accordingly. With Cisco and Microsoft, you can migrate to the cloud and grow with ease, knowing that your growth is backed by partners you can trust, and solutions that keep your organization—and your people—secure.

Aligned for impact.

Member of
Microsoft Intelligent Security Association

Microsoft