EBOOK

Security’s new frontier: The Cloud
Protection for users, data, and applications everywhere
In this ebook

Times have changed -------------------------------------03
Security needs to catch up-------------------------------04
IT constraints increase vulnerabilities-----------------05
Reactive security isn’t enough----------------------------06
A modern approach to security-----------------------------07
How to secure the cloud --------------------------------08
Manage security better than ever------------------------09
Protect users, devices, and apps — everywhere-----------10
Cisco Cloud Security solutions----------------------------11
Why Cisco? ---------------------------------------------12
By 2018, SaaS usage is expected to increase 70%.

Times have changed

The cloud — at one point it was a revolution in the workplace. But the cloud is no longer a trend or a movement. It’s now so integrated into IT and infrastructures that, for many companies, it’s simply another part of the business. The availability of mobile devices and cloud services has redefined not only the way we work, but where we work. People can work anywhere now — not just from branch or corporate offices, but also from coffee shops, airport lobbies, campsites, city sidewalks, and their homes.

As work migrates out of the traditional office, users are moving off the network and accessing the cloud directly. More applications and servers are moving to the cloud to take advantage of cost savings, scalability, and accessibility. And the changes don’t stop there — critical infrastructures, applications, and massive amounts of sensitive data are now stored in the cloud, leaving companies at risk of damage if cloud accounts are compromised.

While increased mobility and flexibility in the workplace has led to reduced costs and booming productivity, innovation, and independence, it comes at a price. Organizations are no longer safely protected behind their firewall or secure web gateway. With the cloud fast becoming the new normal, network security solutions need to adapt.
Security needs to catch up

More branch offices are now connecting directly to the internet, more unmanaged devices are connecting to the network, and more users are accessing company resources while roaming. With users, apps, and data leaving the perimeter, gaps emerge that leave organizations susceptible to attacks. Cloud services can also lack basic security protections and may even be used without the knowledge and control of the IT team. As a result, IT teams have reduced visibility and control over their environments and sensitive enterprise data.

Security can’t wait any longer — it needs to work now and evolve as new cloud services are adopted. Organizations need a simpler way to gain comprehensive visibility beyond the perimeter. They need to identify potential threats and respond faster, no matter where users access the internet. And they need to be able to simply and effectively manage consistent security policies from one place.
70% of user activity originates from browsers without the latest security in place.

IT constraints increase vulnerabilities

The perimeter has become blurred, and operational complexity is rising. Network and security operations teams spend too much time trying to enforce security policies, and are constantly bombarded with security alerts. And current security systems don’t provide the context, intelligence, or visibility needed to determine which threats are of highest priority. On average, IT teams can investigate only 56% of security alerts on a given day — meaning dangerous threats can slip through the cracks.

Which constraints stand in the way of closing the security gaps? Budget, compatibility with legacy systems, certification requirements, and talent shortages are the main restrictions cited by the Cisco Annual Cybersecurity report. Lack of budget is a perennial challenge for security teams, but disparate systems that don’t integrate — where security is “bolted on” rather than embedded — are becoming more of a problem as cloud usage grows. These non-integrated defenses allow space for cybercriminals to launch attacks. And the lack of IT resources or time intensifies the need to truly understand what is happening in the security environment.
Reactive security isn’t enough

As the workplace evolves and the perimeter grows, attackers also are advancing and developing — they’re invading organizations in more unique, targeted ways. But while cyberattacks are getting faster, smarter, and stealthier, IT professionals are still relying on traditional network defenses like firewalls and secure web gateways. Traditional security can’t extend protection to mobile users or handle the exponential increases in internet traffic that have become commonplace. And they can’t deal with increasingly sophisticated threats.

Conventional network security is inherently reactive: Only after malware, ransomware, phishing, and other malicious attacks are detected can they neutralize the threat. In 60% of cases, attackers are able to penetrate and compromise an organization within minutes, while lagging security defenses take days or longer to detect a breach. This reactive security approach leaves organizations vulnerable.

Traditional security can protect only against malware, ransomware, phishing, and other attacks after they’re detected.
A modern approach to security

As security evolves beyond the perimeter, security in the cloud has become a shared responsibility between cloud service providers and the organizations they support. Cloud service providers are responsible for the security of their infrastructure, while organizations that use those services are responsible for user activities on top of that infrastructure.

Cloud service providers build security measures into their cloud applications and platforms; but their capabilities cannot address the risk introduced by user behavior. It’s critical for security teams to surface and respond to abnormal user activity, but they’re stymied by limited visibility into user activities within SaaS, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Identity-as-a-Service (IDaaS) environments.

A modern security approach extends protection to cloud infrastructure so that users, data, and applications are covered everywhere — not just on the corporate network. So what’s needed for your company to secure beyond the perimeter and into the cloud?
How to secure the cloud

Companies need to adopt new technologies and security measures without affecting employee productivity or business growth — so it’s no surprise that by 2020, more than $1 trillion in IT spending will be directly or indirectly affected by the shift to cloud.

It’s not realistic — or necessary — to completely overhaul existing security infrastructure. Instead, additional protection that extends existing security investments off premises must be able to seamlessly integrate with current security layers, so employees are protected anywhere they work — and on any device. And while employees, applications, and data move beyond the perimeter, IT teams need to simply and effectively manage security from one single place.

Security teams need complete visibility and control for all internet activity, including traffic to bought and built cloud applications so they’re protected against internal and external threats, like malware, compromised accounts, and data breaches. They need reliable intelligence that enables them to identify, respond to, and protect against potential threats faster and earlier — and a way to enforce this intelligence whether employees are on or off the corporate network.

What companies need

- Comprehensive visibility and control over connected cloud applications
- Scalable security across cloud environments, and seamless integration with existing stacks
- Earlier and faster responses to threats, on or off the network
- Identification of malicious infrastructure and remediation of sensitive data in the cloud
- Discovery of compromised accounts and malicious insiders
Manage security better than ever

Cisco Cloud Security helps you securely adopt and use the cloud, and better manage security for the way the world works today.

Gain better visibility into internet activity across all office locations, roaming laptops, and cloud applications. Employ automatic threat detection and faster responses. Deploy in minutes across distributed sites. Cisco Cloud Security is an effective security platform that is open, automated, and simple to manage. And it’s backed by industry-leading threat intelligence.

While secure web gateway products have traditionally been used to control the sites visited by users, Cisco Cloud Security solutions put the focus on actually helping you safely adopt the cloud and secure users wherever they access the internet. Now you can protect users and secure your data and applications in the cloud.
Protect users, devices, and apps — anywhere

Cisco Cloud Security complements existing network security by providing an additional layer of protection when users connect directly to the internet and cloud services. This comprehensive coverage delivers complete visibility and protection for employees accessing the cloud and for applications bought or built in the cloud. It’s cloud-managed security that is simple to use, fast to deploy, and completely scalable.

- **Block threats earlier**
  Stop malware before it reaches your network or endpoints. Reduce the time spent remediating infections.

- **Extended protection**
  Remove blind spots. Protect users anywhere they go, anywhere they access the internet.

- **Secure users, data, apps**
  Protect users, data, and apps in the cloud against compromised accounts, malware, and data breaches. Enable compliance.

- **Enable secure cloud use**
  Improve security with no impact on end-user productivity.
Cisco Cloud Security solutions: effective security made simple

Built into the foundation of the internet, Cisco Umbrella delivers complete visibility into internet activity across all locations, devices, and users, and blocks threats before they ever reach your network or endpoints. Cisco Cloudlock helps accelerate use of the cloud and protects users, data, and apps across software as a service, platform as a service, and infrastructure as a service. Together, Cisco Umbrella and Cloudlock enable visibility and protection for your mobile, cloud-connected enterprise.

Cisco Umbrella, a Secure Internet Gateway, provides the first line of defense against threats wherever users go, even off the VPN.

“Umbrella’s time-to-value was nearly immediate. Within days of deploying Umbrella, we could see that endpoints away from the corporate network were protected against malicious attacks and websites.”

— Greg Peterson, Senior Director, IT Security, Avanade

Cisco Cloudlock, a cloud access security broker, protects against compromised accounts, data breaches, and malware in the cloud.

“The biggest benefit Cisco Cloudlock provides for us is visibility into what users are doing, what they are storing up in the cloud. Without Cloudlock, we would not have had nearly as good a view into what is out there and how to take action on it.”

— David Duchan, Information Security Engineer, Ahold
Why Cisco?

Cisco Cloud Security solutions are backed by the proven strength and stability of Cisco, with 30 years of building the world’s networks.

- 100 TB data received daily
- 135+ billion internet requests daily
- 1.5 million daily malware samples
- 250+ full-time threat researchers
- 27 global data centers
- 100+ threat intelligence partners

Extend your security and protect your users, data, and applications anywhere with Cisco Umbrella and Cisco Cloudlock.

GET STARTED TODAY