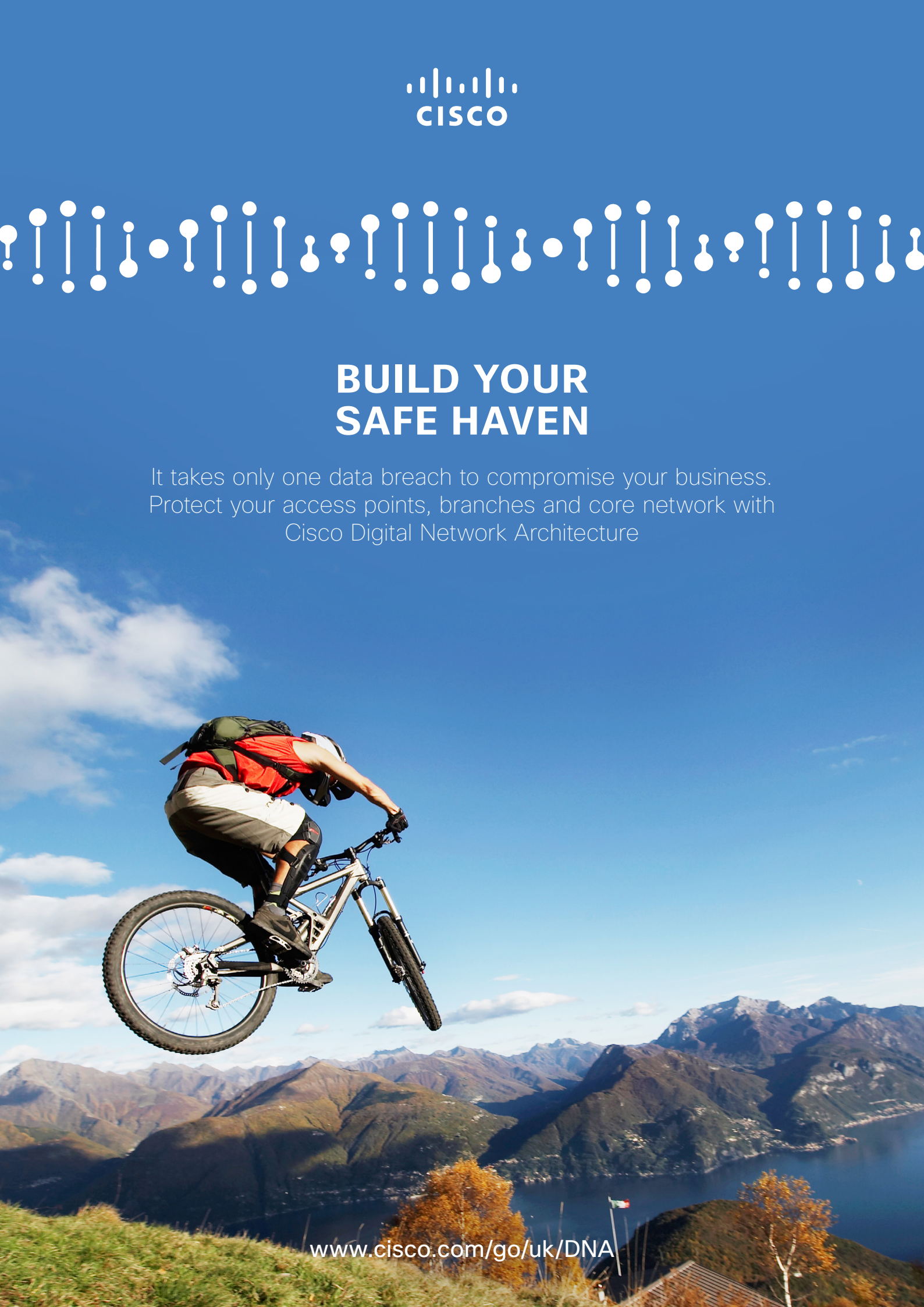

BUILD YOUR
SAFE HAVEN
It takes only one data breach to compromise your business.
Protect your access points, branches and core network with
Cisco Digital Network Architecture
www.cisco.com/go/uk/DNA

Take the risk out of network management

Modern CIOs are increasingly looking to leverage new opportunities to success in the rapidly changing world. But all is good until it goes bad.

Becoming more digital exposes enterprises to greater risk of cybercrime, new strains of malware, and other cyberthreats. How will you manage the heightened threat of an attack as you capitalise on the added value of digital? Can you afford for all to break as you innovate?

Here at Cisco, we've taken the risk out of network management.

Cisco Digital Network Architecture delivers complete threat visibility and protection for internal and external risks across wired, wireless, and WAN network connections. Cisco DNA turns your network into a sensor to avoid, identify, and remediate threats as soon as they enter the network. It also acts as an enforcer to improve protection and response time to attacks, guaranteeing full visibility at all times across your entire network.

"It's really quite simple: the more attack vectors that go unnoticed and the longer we allow attackers time to exploit our systems and infrastructure, the greater their chance for success. It's on us to close that opportunity."

John N. Stewart, SVP and Chief Security and Trust Officer, Cisco

Stop attacks even when you can't see them

Your network continually faces advanced cyberattacks at a time when Internet connections are increasing by the minute. Each network connection, whether created by cloud services, mobility, the Internet of Things (IoT), or something else, represents a potential attack entry point.

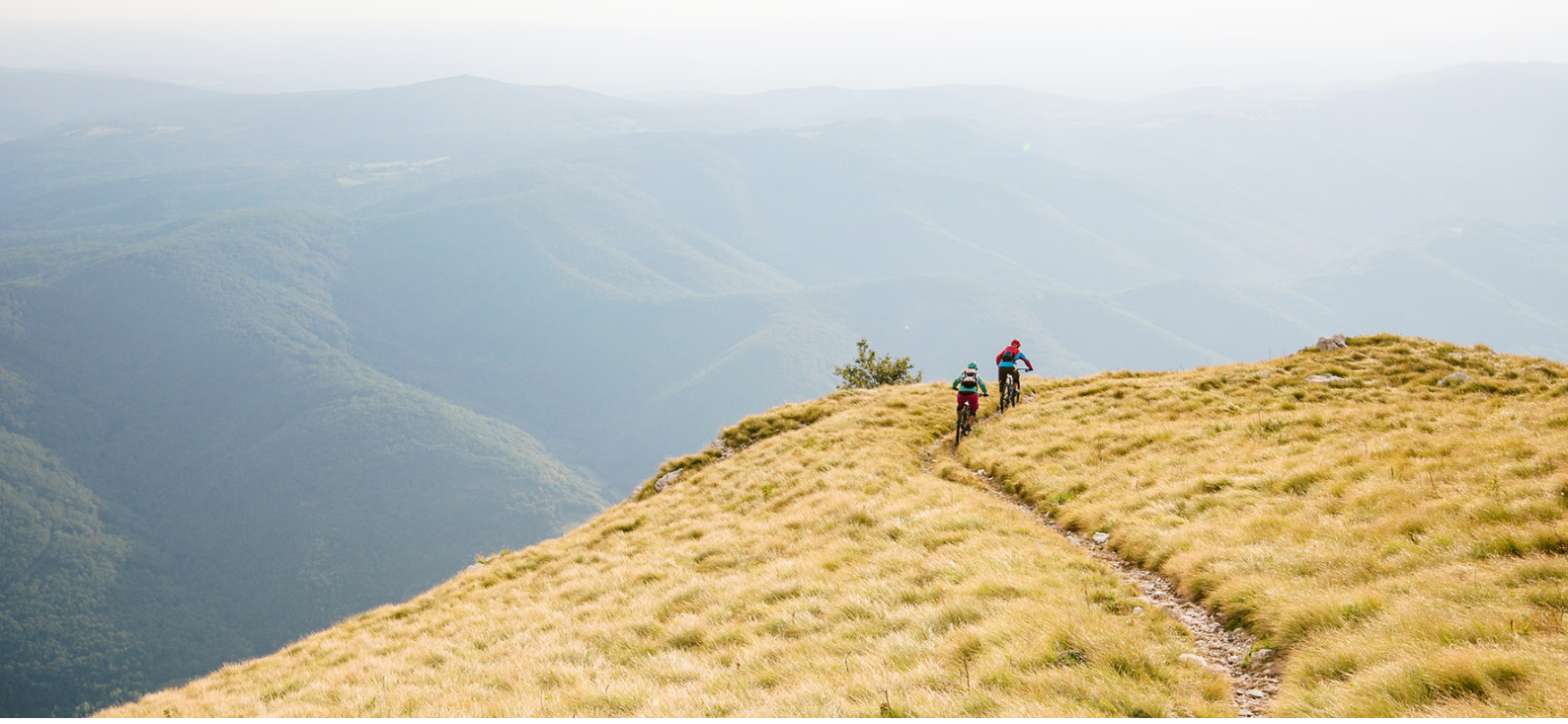
Thanks to Cisco® Identity Services Engine (ISE), that monitors all connections to your network, you will know exactly what devices, users or applications are trying to access your network and apply threat intelligence to any unauthorized access. With Cisco Network as an Enforcer solution, you can then define and apply specific group policies that determine user access based on roles and business needs. This allows you to simplify access management while knowing exactly who and when has access to which data within your network.

"The Cisco Identity Services Engine prevented any unauthorized access to the network while providing highly flexible operational access management, thanks to centralized policy management and automated network management and configuration procedures."

Mirko Berlier, Cisco Engineer and Expo 2015 Architect

What if the threats made their way into your network? Cisco TrustSec® and Cisco ISE will help you to reduce your "attack surface." Even if the attack happened, thanks to network segmentation and the centralized policy engine, your network will notify you of the attack and close the door to prevent widespread damage.

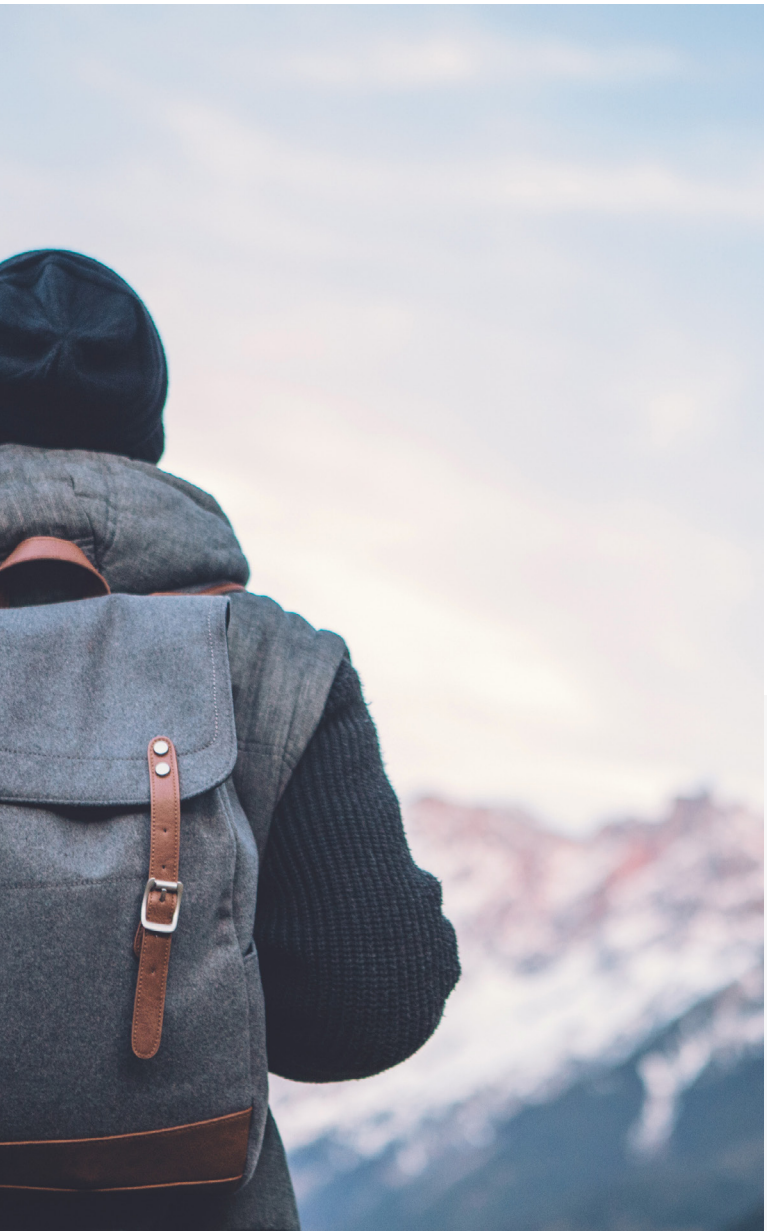
A recent Forrester research paper shows that TrustSec allows IT to implement changes 98% more quickly, lower cost up to 80%, and deliver and return on investment of 140%.

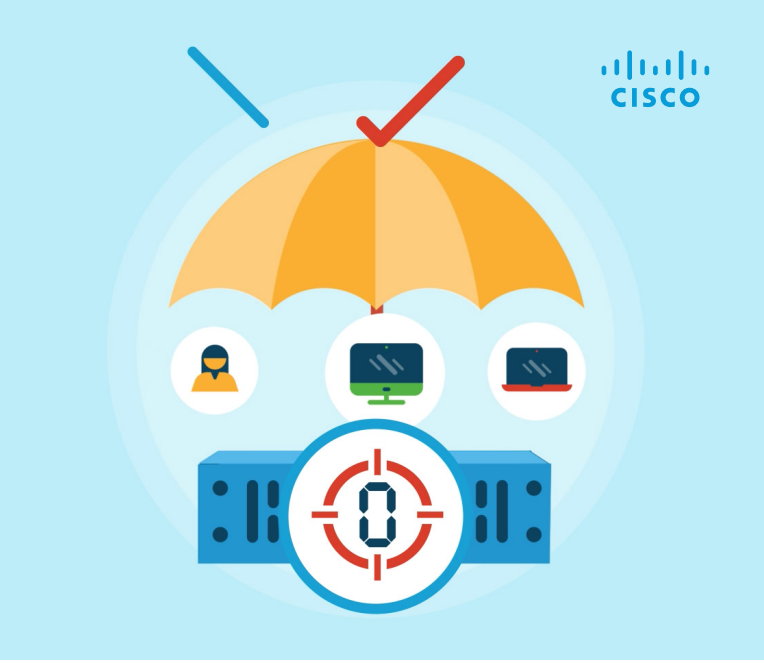


To find out more : Cisco ISE | Cisco Network as an Enforcer | Cisco TrustSec

Protect Your Critical Assets at the Edge

But the attacks no longer happen just at the core of the network. Due to the increased number of access points within campuses and branch offices, the network edge becomes the main point of attack for unauthorized or hostile access. Fortunately, with the built in Cisco Network as a Sensor solution, your Cisco network is transformed into a full-blown security monitoring system. This gives you broad and deep visibility into your network and everything that connects to it before, during, and after an attack.





How does this work?

Cisco Umbrella Branch is a cloud security service integrated with your Cisco 4000 Series Integrated Services Router. Up and running in no time, it is your first layer of defense against threats at the branch office, at no additional costs.

Next, with Cisco IOS® Flexible NetFlow and advanced security analytics, Cisco Stealthwatch® automatically detects anomalous network and user behaviors making it much easier to pinpoint something suspicious to take action.

With Cisco Stealthwatch, network and security troubleshooting time is reduced from days or months down to just minutes.

To find out more:

- Cisco Umbrella Branch
- Cisco IOS Flexible Netflow
- Cisco Stealthwatch
- Cisco Network as a Sensor

Speedier recovery time

Your network can remediate breaches more quickly through automation with the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM). Instead of rolling out mitigation and network remediation box by box over a period of weeks or months, you can apply it in near real time to your whole enterprise at once. Thanks to Cisco Advanced Malware Protection, which watches, analyzes, and records the activity of every file that enters your network, you will know exactly where the malware came from to contain and remediate it in just a few clicks.

100%

of malware, exploits & evasions detected

Cisco is a leader in NSS Labs' Breach Detection test for the third year in a row—detecting 100% of malware, exploits & evasions.

To find out more:

Cisco APIC-EM

Cisco Advanced Malware Protection

Explore the full potential of your network.

Lower your security risks, improve your security operational efficiency, and enhance compliance with Cisco Digital Network Architecture.

www.cisco.com/go/uk/DNA