Six Degrees of Network Security

A number of obstacles stand between you and a safe network. Your security shouldn't be one of them.

These common security pitfalls put your network security at risk.

Trying to stay ahead by staying behind a firewall.

More and more users are working on the move – and not always using VPN – but a firewall protects users only when they're on the network.

82% of mobile workers admit they don't always use VPN.1

Betting on antivirus for off-network protection.

Antivirus software is often the only protection for off-network endpoints. The problem? Signature detection blocks only known attacks - and threats are moving too fast for manual updates.

25% of corporate traffic will bypass perimeter security by 2021.²

Trusting web proxies to handle sophisticated threats.

Web proxies cover only ports 80/443, but attackers use advanced tactics like non-web ports and protocols for network infiltration and data exfiltration.

15% of malware C2 callbacks use ports other than 80/443.3

Turning a blind eye to

SaaS apps.

SaaS apps are great for employee productivity. But you can't protect what you can't see, and on-premises solutions don't have enough visibility or control for SaaS and cloud apps.

475+ third-party applications are used by the average company.4

50

Managing security in a silo.

Traditional security tools won't readily integrate with other solutions, like SIEM or custom in-house apps. If your systems can't talk to each other, you can't get the security intel you need to protect your business effectively.

50+ vendors secure the average company.⁵

Hoping appliance-based tools will scale easily.

Protecting each branch with appliance-based tools just isn't scalable. Deployment, configuration, and ongoing management are cumbersome and intelligence processing capacity is limited.

69% of branch offices have direct-to-internet access.6

There's a better way to secure your organization.

More than 91% of malware uses DNS to gain command and control, exfiltrate data, or redirect web traffic. 7 Built into the foundation of the internet, Cisco Umbrella provides an essential first line of defense against threats – anywhere users ago.

Take a deep dive into what makes Umbrella unique, or get started with a 14-day free trial.

Read ebook

Start free trial

CISCO

- 1. https://learn-umbrella.cisco.com/ebooks/your-users-have-left-the-perimeter-are-you-ready
- 2. https://www.gartner.com/doc/3542117/predicts--network-gateway-security
- 3. https://www.helpnetsecurity.com/2013/10/29/visual-investigations-of-botnet-command-and-control-behavior/ 4. https://resources.cloudlock.com/industry-reports/the-extended-perimeter

5. https://engage2demand.cisco.com/en-us-annual-cybersecurity-report-2017 6. http://info.opendns.com/rs/opendns/images/WP-ForresterTAP-BranchOffice-CommissionedByOpenDNS.pdf 7. https://umbrella.cisco.com/blog/2016/01/21/cisco-security-report-more-orgs-should-be-monitoring-dns/

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.