Wireless Security

Top Five Ways Your Network Can Give You More Security

It takes only one network breach to ruin a business. It's no longer enough to just rely on perimeter defenses, because a commoditized network won't deliver the security you require. You need a network that has security built in, without compromising agility or stifling innovation.

Here are five ways you can make your network even more secure:

1. **Right person, right place, right time**
   Let your network be its own bouncer and stop unexpected activity in its tracks. Simplify the provisioning of network access to accelerate security operations and consistently enforce policy anywhere in the network. Classify traffic based on endpoint identity, not IP address. This allows you to stop malicious actors from accessing your network while easily meeting compliance goals.

   Cisco TrustSec®

2. **Should that be happening?**
   Go beyond conventional threat detection and harness the power of network analytics. Continuously monitor the network interior, where sophisticated attackers often lurk undetected. Embed security anomaly detection into the network element, using machine learning for incident response and device-level mitigation. So you can uncover and stop attacks that bypass the perimeter and infiltrate your internal environment. And contain suspicious devices for remediation.

   Cisco® Stealthwatch

   "Stealthwatch is the 2016 CODiE winner for best network security solution."

3. **Who goes where?**
   Simplify access control across wired, wireless, and VPN connections by cascading policies down all types of access points with software-defined security policies. Make it easy to maintain regulatory compliance and policy segmentation. So you can reduce risks and contain threats by dynamically controlling network access, assessing vulnerabilities, and applying threat intelligence. Not to mention containing suspicious devices for remediation.

   Cisco Identity Services Engine and Cisco Rapid Threat Containment.

   "The Cisco solution gives us a very precise way... to identify who is trying to access what. It allows us to place users in the right category and have the right policy to match information security demands."

   – Roman Scarabot-Mueller
   Head of Infrastructure, Mondi Group International

4. **Secure your branches**
   Protect your extended network with the same encryption, visibility, and ease of management as your campus with Cisco Intelligent WAN. Block attacks and get secure connectivity and threat defense by taking advantage of VPN, firewall, network segmentation, strong encryption techniques, and threat defense capabilities to help ensure that your branches get the security you need.

   Cisco Intelligent WAN.

5. **Keep one step ahead**
   Safeguard your infrastructure, your web, and your mobile users with flexible software licensing that delivers features that enable you to defend your network in real time. At the same time it keeps you informed of the latest threats, maintains networkwide policy consistency, and troubleshoots security issues quickly. Be sure that the software investments you make today will last into tomorrow with portability and easy access to upgrades and updates.

   Flexible Software Licensing.

   "Cisco has reduced its median 'time to detection' (TTD) [for new threats] to about 13 hours—well below the current and unacceptable industry estimate of 100 to 200 days."

   – Cisco 2016 Midyear Cybersecurity Report

It's all good. Until it goes bad. Don't treat your network as a commodity. Why take the risk? Get a network with security built in. So you can maintain the highest security without compromising agility, and create a secure foundation for innovation.

Learn more.

C45-738315-00 12/16