# Next-generation network security: your top 5 considerations

In today's security landscape, complexity is the attackers' friend. The ideal security solution for organisations is simple, open and automated. Defences also need to perform real-time, all-the-time, and be wherever your adversaries might be. Which is anywhere on your network.

Here we explore the features of an advanced defence that targets threats before, during and after an attack. We also look at five key criteria you should consider when deciding what's right for your business.

1

## End-to-end visibility

Threats are evolving and increasing, and traditional defences are no longer suited to the nature of the attacks. You can no longer just focus on perimeter defences and particular areas like email. You need to accurately identify the applications active in your environment (regardless of protocol), as well as the large number of connecting hosts, infrastructure and users.

**The industry median time to detect an advanced threat is approximately 100 days** (Cisco Midyear Cyber Security Report 2016).

2

## Advanced protection

Growing threats, such as ransomware, target vulnerabilities that are shared by many companies. That's why advanced malware protection is crucial. You should consider cloud-based security that can share real-time information across your business and with other companies. You'll also need coordination between network defences, endpoint protections and the management console.

Advanced security can protect you against both known and emerging threats, even during peak usage.

**Flash accounted for 80% of successful ransomware attacks from the popular Nuclear exploit kit** (Cisco Midyear Cyber Security Report 2016).

3

## Support for mobile working

Mobile working means your employees are accessing your network from more places than ever. They may inadvertently bypass the VPN or no longer need access to the corporate network to do their work. You'll therefore need granular controls to enable safe access, rather than make employees go around your defences. This requires fine-grained security policies that detect and respond to applications and websites.

4

## Automated performance

To manage information risks, you need to be able to set policies across your business. You'll also need to support both existing and future security controls. And you need network security that can automatically provision and tune these policies, applying them consistently across your network at high speeds. The ability to scale to multi-gigabit networks is crucial.

5

## Easy integration to reduce cost and complexity

An integrated, multi-layered approach can provide a better view of threats, and so provide better protection. Consolidating on a single platform removes the complexity and cost of buying and managing multiple solutions. And integrating with third-party solutions can extend your multi-layered protection. It also simplifies management and deployment, by giving you a single security interface.

***The right security, today – and tomorrow***

Our next-generation security is designed for small and mid-size organisations looking to grow with confidence. It's the only fully integrated, threat-focused solution that keeps organisations safer, mitigates advanced threats faster, and streamlines operations better across the attack continuum: before, during and after they occur.

Explore Cisco Security

***More useful information***

Cisco Next-Generation Security At-A-Glance