

## 3 NAC Advanced customer scenarios

### ...help to protect, enable and simplify

Sophos NAC Advanced safeguards data. NAC Advanced protects information by permitting access to the users who need it and enables companies to create comprehensive security policies to check that any computer accessing the network – even those not owned by the company – are in full compliance. NAC Advanced ensures that computers, including roaming laptops, have up-to-date patches, are running a specific anti-virus solution and have their firewalls enabled.

These three scenarios are examples of how real companies are using Sophos NAC Advanced to ensure compliance with their own internal security policy, with external industry and government regulations, and to safely enable their mobile workforce.

#### Scenario 1: Ensure compliance and stop configuration drift of company computers

##### Challenge

Many corporate computers fail basic checks to determine if all security patches are in place, if client firewalls are active, and endpoint security is active and up to date.

Data that Sophos gathered so far from thousands of PCs worldwide taking the Sophos Endpoint Assessment Test has revealed that 81% of corporate endpoints failed a basic security check. The test discovered that:

63% were missing at least one Microsoft security patch  
51% of endpoints tested had disabled client firewalls  
15% had out-of-date/disabled anti-virus software

##### Customer story

A global engineering firm that specializes in converting architect drawings into building specifications faced the challenge of preventing configuration drift.

The firm has 500 employees with administrative rights over their computers, and some employees were exercising those rights in ways that increased their vulnerability to malware attack and data loss. They were turning off the company-approved firewall in order to access the web, using unapproved instant messaging products, and not installing critical Microsoft OS patches.

##### How NAC Advanced helped

The firm used the pre-defined assessments available with NAC Advanced to examine the configuration of every computer within the organization against its security policy. NAC Advanced:

- checked whether an anti-malware application was active and up to date.
- looked for specific operating system patches and security applications, using over 1300 pre-defined assessments
- automatically fixed computers that were not compliant.
- isolated guest computers that did not meet the organization's security standards, and even told users how to fix their computer's configuration easily.

##### The outcome

Deploying Sophos NAC Advanced resulted in a compliance rate of over 95%, and fixed all non-compliant computers within 24 hours of assessment.

#### Scenario 2: Achieve industry and government security regulation compliance

##### Challenge

Organizations must meet specific industry and government regulations or risk fines, a loss of privileges, bad press, or prosecution for non-compliance.

The security measures deployed to achieve compliance must also be carefully balanced to ensure that information can be readily accessed by those who need it. Healthcare providers, for example, must protect patients' personal data, while giving doctors, insurance companies and the patients themselves access to the information.

#### Customer story

A UK National Health Service trust faced the challenge of achieving compliance with industry and government regulations. The trust provides care for 350,000 patients whose data must be safeguarded.

The trust needed to achieve compliance standards by ensuring data was encrypted, data loss measures were present, and security software was activated before and after accessing the network. The trust was also required to check computers for unapproved software and non-corporate assets plugged into the organization's network.

#### How NAC Advanced helped

NAC Advanced helped the trust to:

- meet specific government regulations for the protection of patient data
- check that security applications and patches are up to date
- control network access
- manage access to servers, applications and data
- monitor and report on compliance status

#### The outcome

By implementing NAC Advanced, the trust was able to easily provide auditors with compliance reports and meet required security standards.

## Scenario 3: Ensure configuration of roaming laptops and devices

#### Challenge

The number of employees accessing their corporate network remotely grew by 71% in 2007, according to the Aberdeen report. Remote users need to be able to access the network via broadband from home and public WiFi while travelling. At the same time, their organization needs to ensure that roaming laptops stay correctly configured. That challenge is even greater when that organization happens to be a news network that relies on its correspondents to submit stories and meet deadlines from anywhere in the world.

#### Customer story

A cable news organization wanted to prevent configuration drift from its correspondents' remote laptops which could introduce vulnerabilities onto the network. The correspondents were active on the network for limited periods of time, and were all in different time zones, making it a challenge to check their laptop configuration.

#### How NAC Advanced can help

NAC Advanced checked reporters' laptops even when they were not connected to the network. Sophos NAC agents communicated via the internet with policy servers or used the currently cached policy on the hard drive to check the status of unconnected laptops. When communication was established, any new anti-malware signatures or patch definitions were automatically downloaded.

#### The outcome

With NAC Advanced, the news organization enabled reporters around the globe to submit stories anytime, anywhere, while ensuring compliance and limiting security risk.

Sophos NAC Advanced can help with all your compliance needs, and our team of specialists can help you create security policies that are right for your environment.

To find out more about Sophos NAC Advanced, visit [www.sophos.com/products](http://www.sophos.com/products)