



CounterACT Compliance Platform

Payment Card Industry Data Security Standard (PCI DSS)

In the wake of widely publicized cardholder information losses, the Payment Card Industry (PCI) has rallied to establish a regulatory standard for the protection of cardholder information: the PCI Data Security Standard (PCI DSS). Enforced through compulsory IT audits, the PCI DSS helps to ensure the security and protection of personal data. Companies governed by the PCI DSS, grappling with how to control access to this private data, are looking to ForeScout CounterACT to help.

CounterACT Compliance Platform

Network Access Control (NAC)

Virtual Firewall

Global Policy Management

PCI Compliance Kit

Essentials of PCI Compliance

The PCI DSS features 12 regulatory requirements with specific guidelines for *controlling access* to cardholders' non-public personal information (NPPI).

ForeScout's CounterACT solution is ideally suited to satisfy these regulations without any disruptions to daily business.

The clientless, out-of-band CounterACT NAC appliance easily plugs into any network - independent of what switch, router or OS is in place - and can be used to protect and control access to cardholder NPPI.

Protecting Assets

The PCI DSS mandates that companies install and maintain a firewall to protect cardholder data.

One of CounterACT's unique strengths is its ability to establish a virtual firewall around specific network assets, such as the storage devices containing cardholder NPPI. This is done by segmenting the network and defining/enforcing network access policies to protect the device (see diagram below).

Although a physical firewall or inline NAC appliance would also work, both come at great costs in terms

of infrastructural upgrades, network downtime, and reduced user productivity. CounterACT's policy management capability helps IT managers avoid these unnecessary liabilities.

Controlling Access

With CounterACT, IT managers can define and enforce global security policies, thereby ensuring that all attempts to access cardholder NPPI - on any storage device - are identified, authorized or blocked, and logged/reported in local languages.

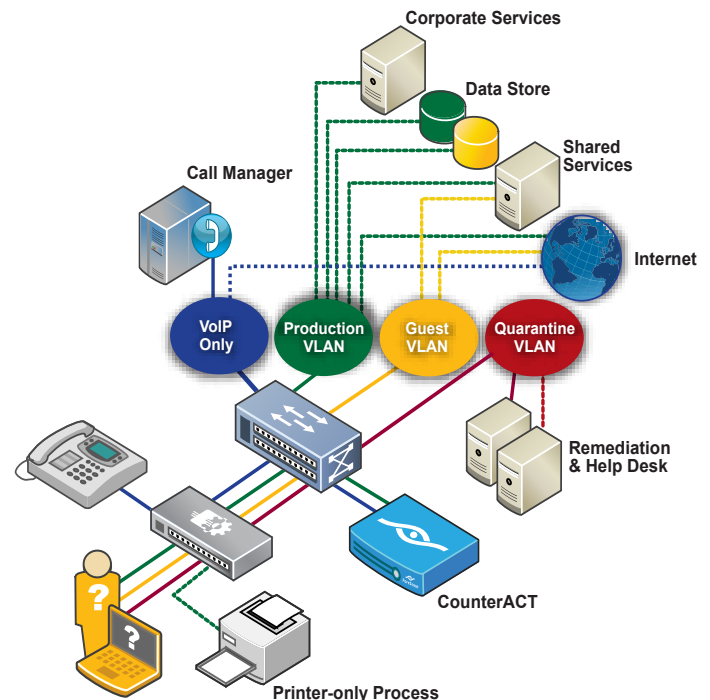
CounterACT Compliance Platform

Identifies the endpoint & determines compliance level. CounterACT detects all network devices without the need for a client residing on the endpoint.

Grants full access if the device is compliant and the person's role justifies their access attempt. This process is transparent to compliant end users.

Grants or denies access based on device compliance and user authorization.

1. Identify and interrogate
2. Allow access to data based on device compliance, user role, status, etc.
3. Flexible enforcement to contain, block or remediate
4. Post-connect monitoring
5. Reporting



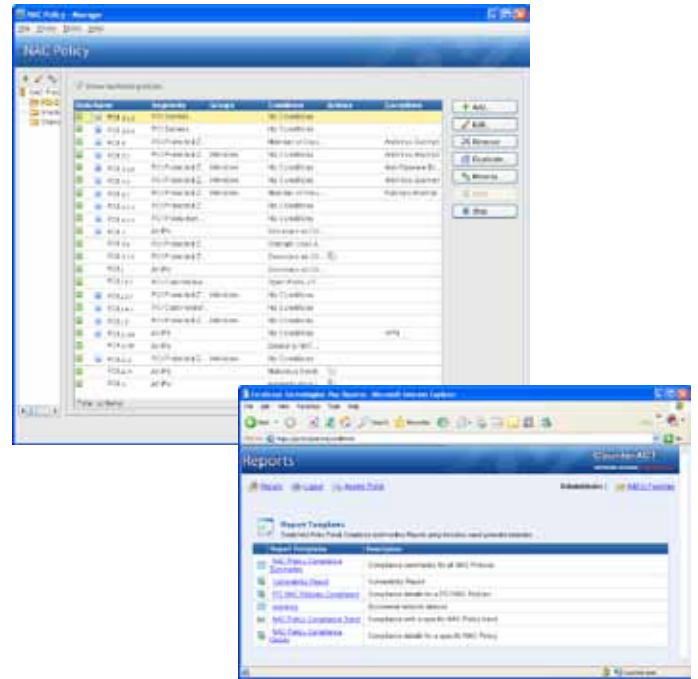
How it works: Using CounterACT's virtual firewall capability, a perimeter can be defined to limit access to the NPPI data stores to authorized users.

The PCI Compliance Kit

The CounterACT PCI compliance kit features pre-defined policies and (localized) reports tailored to address eight of the 12 PCI DSS requirements.

The out-of-the-box policies define controls to payment card information, helping to ensure only appropriate users have access to sensitive information. Based on best practices gleaned from global customers, the policies help managers deploy CounterACT for user as a PCI compliance platform in just a few minutes.

The audit report contains information used to detect and deal with non-compliant items and also show network and device information required for a PCI audit. These reports are offered in local languages, making them immediately relevant to the in-country IT manager and auditor.



Install the PCI plug-in and generate PCI NAC policies and PCI compliance reports. Select the PCI requirements you want to appear in the report; schedule the report to run regularly at a specified time and have it delivered by email.



The report is organized according to the PCI requirements, with each section beginning with the relevant PCI requirement number and followed by detailed information.

The compliance kit offers step-by-step guidelines for using the report to remediate, improve and achieve compliance, and for summarizing details for audits.

