Advanced Authentication for Meeting the PCI Mandate

Advanced Authentication at a Glance:
Advanced Authentication enables organizations to comply with the Payment Card Industry Data Security Standards (PCI DSS) security requirements mandated so that those who "hold, process, or pass cardholder information" meet a minimum level of security.

Using Right Framework
As organizations of all shapes and sizes continue to fall victim to outsider breaches, it is clear that protecting access to internal information with traditional username and password is no longer sufficient. Today, not only do organizations have information in digital format, users and their devices used to access them are continuously connected and exposed to a variety of attacks. Even when users are working from inside an organization's facilities, many of the services they access no longer reside inside their firewall's perimeter, but rather out in the cloud, allowing ubiquitous access for all, both friend and foe.

Since criminals and conspirators are effective at duping people into divulging their credentials (what they know), an effective way to increase security is to leverage what they have (such as a FIDO U2F device) or what they are (such as a biometric reader). NetIQ® Advanced Authentication allows a central place for all authentication policies to be managed. This is important because organizations are usually forced to manage and maintain multiple infrastructures. Not only are multiple authentication infrastructures complicated to manage, they are less secure. What you need is a single, two-factor or multi-factor authentication framework for all of your devices and methods. Having a single framework keeps costs down, and Advanced Authentication scales to any size environment.

In addition to the MFA flexibility that Advanced Authentication offers, it also comes out-of-the-box integrated with the market leading single sign-on solutions from Micro Focus®, which covers virtually all applications and most platforms: Access Manager™, xAccess and SecureLogin. Having a robust single sign-on solution is an essential element of convenient access by delivering access to all the user's relevant services. For ubiquitous compatibility, Advanced Authentication’s framework also integrates with other single sign-on solutions.

Advanced Authentication provides broad platform support for the platforms that are key to your environment, including: Windows Credential Provider, OSX, iOS, Android, Windows Mobile and Linux Pluggable Authentication.

Payment Card Industry—Data Security Standards (PCI-DSS)
The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. The Payment Card Industry Data Security Standards require that merchants protect sensitive cardholder information from loss and use good security practices to detect and protect against security breaches.

PCI DSS Requirements restrict access to cardholder data by business need to know—requires that: organizations must ensure that critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on a need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements track and monitor all access to network resources and cardholder data. "Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs."
About Envoy Data Corporation

Envoy Data Corporation’s security solution practice and customer service make them an excellent choice for purchasing and deploying Advanced Authentication. Envoy Data Corporation (EDC) has over 15 years experience architecting, distributing, deploying, and supporting complete multi-factor authentication solutions, and can assist you with a solution specified for your environment. Using Advanced Authentication’s open integration framework, EDC will match the authentication experience to fit your user’s needs.

In recent years, government regulators have set more stringent security policies that are more specific about the requirements for securing access to protected information. As a result, your IT security managers may face an increasingly complex challenge of keeping up with their access control needs and potential solutions. EDC’s trained professionals stay current on the latest government security policies and are experts at designing an authentication that matches your organization’s needs.