

Case study

Pizza Hut

SecurEnvoy 
The future of authentication

Pizza Hut wheels out IT security via mobile phones



How Pizza Hut rolled out new security measures for PCI compliance

Pizza Hut's online ordering system has grown quickly in recent years, and deals with a high level of traffic. It's not unusual for the website to process over £1 million worth of orders from hungry consumers in just a week. At busy times, the website takes payments totalling £250,000 in an evening.

This activity requires a robust website, and a very secure payments network. Pizza Hut, in common with retailers worldwide, is subject to the Payment Card Industry Data Security Standard (PCI DSS). This is a global standard designed to ensure card transactions take place as securely as possible, reducing fraud and increasing consumer confidence.

PCI DSS requires that all employees with remote access to a network that contains card payment information must use more than just a password to prove who they are. For Pizza Hut, this meant that all employees with laptops – around 200 in total – had to have an additional layer of security to prove who they were when logging on.

According to Fawad Shah at Pizza Hut, authentication via mobile phones was the most viable option: "We looked at a number of alternative systems, including plastic tokens which generate a random password and cards which do a similar thing, but mobile phones came out on top. Everyone has one with them anyway, and so a system where passcodes were sent via SMS was the cheapest and most efficient way of complying with PCI DSS."

SecurAccess from SecurEnvoy, the pioneer of two-factor authentication using mobile phones, came out as the market leader, and was selected by Shah and his team based on the company's experience in the security sector. By using SMS, SecurAccess sends a login passcode to each employee's mobile phone at the time of authentication, allowing them to connect to Pizza Hut's network securely. The passcodes are different every time, and are delivered as the user logs on.

Pizza Hut's VPN was married up to SecurEnvoy's portal, and the system was deployed to all users in a few days. According to Shah, the rollout went well: "There was some resistance from users at first, which we expected. Employees are generally cautious about change – especially when it comes to IT systems. However, once they started using SecurAccess, they realised it was the simplest and most effective way of securing network access."

"It's a much more efficient method than using traditional authentication tokens," Shah continued. "Tokens are easy to lose and break – employees are far more likely to take better care of their mobile phones. Using SecurAccess, we've achieved what we set out to do. We're compliant with PCI DSS, all our employees with laptops are able to log on securely, and there's been minimum disruption to our online payments systems or our day-to-day working lives."



SecurAccess:

Authentication for the modern business

SecurAccess from SecurEnvoy turns any mobile phone that can receive SMS into a ready made authentication device. This pioneering zero-footprint solution cuts costs by using hardware that is already in circulation.

Unlike traditional tokens that take months to deploy and replace, SecurAccess can roll out more than 15,000 new remote staff per hour without the pain, cost or environmental impact created by legacy hardware distribution.

The solution fully integrates into Microsoft Active Directory, Novell eDirectory, Sun Directory Server and OpenLDAP. Integration is simple as it requires no additional databases or hardware – not to mention their associated cost.

SecurAccess also integrates with all leading remote access servers and web services including Microsoft OWA, Citrix, Juniper and Cisco.

There's also no need for extra software, eliminating costly and time-consuming testing and training schemes. SecurEnvoy has been designed to respond to the constant changes in mobile technology to ensure a competitive ROI.

Worried about network coverage or SMS delivery delays?
SecurAccess is fundamentally designed to let you:

- Pre-load one-time passcodes
- Reuse session passcodes that change daily or after multiple days
- Request temporary passcodes through self-help website
- Obtain passcodes via email if necessary

SecurAccess is changing the game for business security. No tokens, no fuss...
Just rock solid, two-factor security on the move.

For more information about SecurAccess or SecurEnvoy's other products, visit www.SecurEnvoy.com.



About SecurEnvoy

SecurEnvoy are the inventors of tokenless authentication and provide two-factor authentication via mobilephones. Passcodes are sent to the user's mobile phone in order to access corporate internal networks, cloud based services or private emails.

SecurEnvoy's products - SecurAccess, SecurPassword, SecurICE and SecurMail - are adopted worldwide.

Customers benefit from reduced support time, no database management as existing LDAP servers are used and zero footprint as no token deployment is required, so ROI for organisations is relatively high.

SecurEnvoy distributes through the channel, providing customers the value added benefits of working with

local partners. It has built up a technical and sales

infrastructure that supports most languages and

cultures around the world. Partners include: Juniper, Citrix, Fortinet, Sonic Aventail, Cisco, Checkpoint, Celestix, Microsoft and F5. SecurEnvoy's customers include T-Mobile, Symantec, John Lewis, NHS and Save The Children.

Founded by Andrew Kemshall and Stephen Watts in 2003, SecurEnvoy is based in Theale, Berkshire.

For more information about SecurEnvoy and its products, visit www.securenvoy.com.



SecurEnvoy Ltd

1210 Parkview

Arlington Business Park

Theale

Reading, RG7 4TY

T: +44 (0) 845 2600010

E: info@securenvoy.com

W: www.securenvoy.com