SOLUTIONS IN OVER **27** COUNTRIES WORLDWIDE

CASE STUDY: The City of St.Petersburg

Major US City Council depends on PINgrid to secure remote access to key resources

Known as "The Sunshine City", **St. Petersburg, Florida** in the US averages 361 days of sunshine each year. It covers 61.7 square miles and has a population of approximately a quarter of a million people making it the 5th largest city in Florida. St. Petersburg has emerged as a top destination for the arts with the Dali Museum, the Dale Chihuly world renowned glass collection, and six art districts. It is the job of the city's 2,500+ employees to provide the essential services and support that keeps the city running smoothly.

The city has a growing number of employees that need to access resources on the city network, whilst working away from the office. To help them, wthe city implemented a remote access solution from VMware and mobile device management from AirWatch. However, with many of the software applications not available in mobile versions, it was causing a problem for those logging on via tablets and smartphones.

The solution was to use VMware View, which would give employees remote access to the desktop applications they needed from their mobile devices. However, this increased the security risk, as Brian Campbell, Information Technology Security Officer at the City of St. Petersburg explains: "The only security requirement offered by VMware View to gain access to the users' desktop was their security credentials of user ID and password. Whilst we have stringent policies for user ID creation and robust password management, we recognised that it simply was not enough."

Mr. Campbell uses the example of a mobile device being inadvertently infected with a key-logger, which could capture the login credentials and potentially be used to infiltrate the system and cause disruption.

The city decided that an additional layer of security was needed and a two-factor authentication (2FA) solution would be the most prudent way forward. The city's Information Security team investigated, demonstrated and discounted a number of the market leading solutions. Mr. Campbell explains:

> "The solutions we looked at were not straightforward, elegant, nor in a small enough form factor to make us feel comfortable in choosing any of them. That is until we found PINgrid."

Solution Highlights

- Strong 1.5 and 2 factor authentication using a visual pattern
- Cost effective compared to token based authentication solutions
- Secure remote access to internal AND cloud-based applications
- Active Directory or LDAP database storage without extending the schema
- FIPS 198 & 180-3 compliant cryptography that exceeds OATH specifications
- Rapid user provisioning with auto-generated patterns
- RADIUS & Web Services interface for universal integration
- Free Soft Token download from all major phone application stores
- Out of the box support for Microsoft IIS web servers and Forefront TMG 2010 & UAG 2010

Products Used

Authlogics Authentication Server

st.petersburg
www.stpete.org

Authlogics

“PINgrid is absolutely the solution we were looking for but didn’t expect to find. PINgrid with UAG: Easy, secure and fast. It works perfectly, is consistent and we have no complaints or problems at all. We are very pleased indeed.”

Brian Campbell
Information Technology Security Officer
City of St. Petersburg

Grid Pattern Authentication: Simple, Memorable and Secure

Combines ease of use with patented high security

Initially the simplicity of PINgrid made the team wary, but also intrigued enough to embark upon rigorous and thorough testing to scrutinise every aspect of the solution.

The result was zero failures.

“We had to know if a solution so simple could meet our high expectations,”

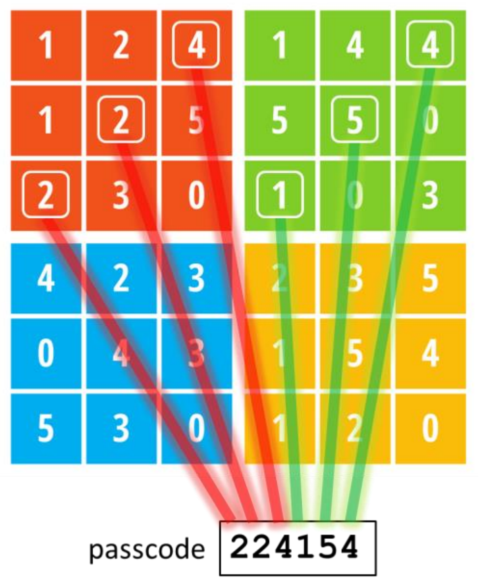
adds Mr. Campbell. “During the testing phase we were in frequent contact with the Authlogics team and their responses to our questions were always immediate and positive. Not only were we impressed with the solution, we were also impressed with their customer service.”

Having found its 2FA solution, the city invested in user licenses for PINgrid for the members of staff who are authorised to have remote access, and today it is fully integrated with the VMware solution.

“The solutions we looked at were not straightforward, elegant, nor in a small enough form factor to make us feel comfortable in choosing any of them. That is until we found PINgrid from Authlogics.”

Brian Campbell

Information Technology Security Officer City of St. Petersburg



1	2	4	1	4	4
1	2	5	5	5	0
2	3	0	1	0	3
4	2	3	2	3	5
0	4	3	1	5	4
5	3	0	1	2	0

passcode 224154

The Benefits

To use PINgrid, all an employee with remote access rights needs to do is download the app (available from all major app stores) on to their mobile device. Meanwhile, the Information Security team creates their account which in turn triggers an e-mail to be sent to the employee, which includes their initial PINgrid pattern. The entire process takes a matter of minutes.

Now all the user needs to do to login is to access VMware View but before they enter their username and password they are prompted for a One Time Code. This code is obtained by simply opening the PINgrid app and entering the corresponding digits that appear in their pattern.

“For staff choosing to install the app on their personal devices, we ensured that they understood that the PINgrid app is essentially a standalone number generator requiring no internet access, no “phone home” requirement, and giving them reassurance that it is completely independent and that they could use it with confidence,” notes Campbell.

“We have found that the beauty of PINgrid is in its simplicity,” remarks Mr. Campbell. “It has been easy to deploy and the roll-out required virtually no user training, even though we offered it to everyone, only around 5% of the users required assistance”.

☎ UK/MEA +44(0)1344 568900

☎ US +1 408 706 2866

sales@authlogics.com

www.authlogics.com

Authlogics