PWN Achieves Watertight Security of Endpoints and Applications

Profile:
The water company and administrator of the dunes of North Holland

Industry:
Utilities and Infrastructure

Location:
The Netherlands

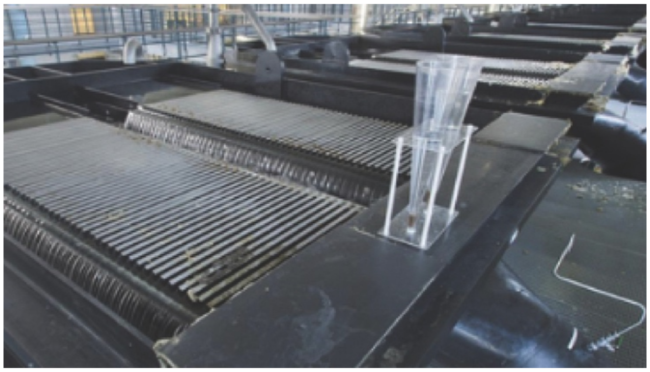
Website:
www.pwn.nl

Solutions:

- Ivanti® DesktopNow

Key Benefits:

- Controlled privilege management of 800 endpoints
- Watertight security through blocking of unknown applications/code, preventing malware from entering the PWN network
- Control of applications with intelligent, policy-based tiering
- Easy migrations of operating systems
- Security of Windows applications outside of PNW network & CYOD incorporation



PWN is responsible for the continuous availability of drinking water for 1.5 million people in North Holland. As providers of the infrastructure and processes to purify surface water into safe drinking water, PWN insists on deployment of the highest levels of security and vigilance right across the organisation to eliminate contamination risks.

Paul-Peter Polak, Business & Information Architect, PWN, remains crystal clear on the organisation’s objectives: “The provision of pure drinking water is an essential part of the regional infrastructure which entails deploying as many layers of protection as we can whilst allowing our employees to remain productive. Cyber security of our 800 endpoints is therefore of paramount importance to PWN.”

Back in 2011, PWN detailed two further steps to ring-fence cyber security over and above the existing solid firewalls and antivirus solutions. PWN highlighted that a structure of defined user-privilege control, together with a granular system of checking all applications before download, would form a final defensive line for users within their Windows environment. With previous positive experience with Ivanti’s endpoint security capabilities, Paul-Peter further explored and adopted the Ivanti DesktopNow solution to design a watertight protection process that would block malware and stop uncontrolled applications from downloading. Additionally, Paul-Peter knew from previous installations that upon deployment of DesktopNow, PWN would see significant resource savings in software migrations and upgrades between operating systems.

The Solution: Deploying Ivanti DesktopNow across Endpoints

Indeed, easy migration was the initial objective behind the phased install. PWN embarked upon a two-month proof of concept (POC) across 25 endpoints that would significantly ease migration from Windows XP to Windows 7. To achieve this, DeskopNow first moved user files, user personalisation, and application settings seamlessly between the two Windows operating systems without IT configuring endpoints manually. Once proven, IT was able to hand over the bulk migration to PWN's incumbent managed service provider, Fujitsu. The remaining 780 users were rolled out by Fujitsu in batches of 50, all personalised upon login, straight into their new desktop environment.

> ***"We take our corporate responsibility extremely seriously. Cyber security of our 800 endpoints is therefore of paramount importance to PWN and that's why we rely on Ivanti to solidly act as our final line of defence."***
>
> — **Paul-Peter Polak**
> *Business & Information Architecture, PWN*

In the detailed security-planning phase, a four-tiered controlled privilege policy was selected. Tiers 0 and 1 were deployed across every managed desktop—providing all endpoints access to Microsoft operating systems and basic Office apps. If users in these tiers tried to introduce apps or unknown code, the items would be prevented automatically from launching. Tier 2 deployment and access privileges were factored from job roles and requirements, allowing certain endpoints further access to applications managed and deployed by IT. Tier 3 deployment was reserved for a select group of qualified users providing elevated rights to install applications on demand. Requested applications were first cross-checked against blacklists. Once authorised, Tier 3 users themselves could then commence the often lengthy and complex download, further saving IT time.

Results: A Multi-layered Security Model that Prevents Execution of Unauthorised Software

With DesktopNow running in the background, PWN can now check software for whitelisting approval to prevent unsanctioned applications from being run and installed. Checking against the constantly updated listings remains the ultimate safeguard against new types of malware entering the PWN network.

"Other companies have seen application breaches and, more recently, have been exposed to ransomware attacks through inadvertent downloads or simply employees sharing software on USBs," Paul-Peter said. "At PWN, we're reassured that our network is protected through background checks provided by DesktopNow, meaning that unauthorised apps cannot run."

With an increasingly large mobile workforce and a lower cost of laptops, the desktop journey that PWN embarked upon five years ago has changed. Today, IT is focusing on moving user environments from Windows desktop roaming to a programme of increased netbook and laptop usage. Regardless, Ivanti continues to stand guard across all PWN endpoints. Even when accessing applications outside of the PWN corporate network, users can gain secure access through Citrix protected by DesktopNow. IT are also working on a CYOD (Choose Your Own Device) strategy for maximum productivity and again, can be assured that any device adoption will be ring-fenced by DesktopNow.

Notes: PWN's noted results are specific to their total customer environment/experience of which Ivanti is a contributing product. Individual results may vary based on each customer's unique environment.

www.ivanti.com

☎ **1.800.982.2130**

✉ **sales@ivanti.com**