



## CASE STUDY: BeyondTrust

# US Privileged Access Management company looks to Authlogics for password compliance and security.

When BeyondTrust needed to find a way of enforcing NIST SP 800-63B compliant passwords company-wide, it turned to Authlogics. Its Password Security Management ensures every password is strong, complies with the latest best practice guidance and has never knowingly been compromised.

### The Challenge

The company wanted to find a password management solution for its internal IT infrastructure that could be deployed company-wide. Crucially, the solution needed to adhere to the latest NIST SP 800-63B Digital Identity Guidelines and be non-intrusive to the end-users as well as work solely through Microsoft Active Directory domain controller rather than the endpoints.

### The Solution

The answer was Authlogics Password Security Management (PSM) software from Authlogics, providing a simple and comprehensive way to ensure that all passwords comply with the latest regulations and that they haven't already been compromised.

Today, when a BeyondTrust employee attempts to reset their password, they do so using an intuitive online self-service portal. When they propose a new password it is automatically and instantly assessed for adherence with the NIST standard. Simultaneously, it is cross-referenced against the Authlogics Password Breach Database - a continuously growing cloud-based blacklist of over 1.8 billion credentials which have been breached, including over 520 million passwords.

### The Benefits

Senior Security Engineer at BeyondTrust, Michael Abadeer states:

*"When we completed the company-wide roll-out of the Authlogics Password Security Management 12 months ago we were 500-strong. Today, through three acquisitions the group has almost 1000 employees."*

The ability to quickly and easily on-board personnel was a key factor in selecting the PSM. As Abadeer continues:

*"Because Authlogics resides centrally on the Active Directory domain controller it is extremely scalable and also means that we have been able to onboard almost 500 new BeyondTrust employees with ease."*

PSM has also had a hugely positive impact on the resources needed to manage password resets, as...

*"With PSM, we can have absolute confidence that all BeyondTrust employees working anywhere in the world, are using fully compliant passwords that have not been compromised, whether through direct hacks, phishing or malware."*

Abadeer concludes:

*"This is all without the need for helpdesk intervention and very little maintenance, other than adding and removing accounts from the Active Directory that we would need to do anyway. PSM is an essential and integral element in safeguarding our employees, infrastructure and assets."*

### Solution highlights

- Deployment of Password Security Management to protect Active Directory users.
- Comply with regulatory requirements and latest best practice:
  - NIST SP 800-63B
  - NYDFS – New York State Department of Financial Services
- Simplify existing password policy to make setting passwords easier for staff while ensuring they are safe to use.
- Ensure non-breached passwords are used.
- Help ensure accountability of staff through unique logon information.





## CASE STUDY: BeyondTrust

# A simple replacement for the legacy Windows password policy.

### About BeyondTrust

With 20 offices around the world, BeyondTrust is a cybersecurity software company and the global leader in Privileged Access Management. The company was recently acquired by Bomgar along with Avecto, and Lieberman Software. Today it is trusted by 20,000 customers, including half of the Fortune 100, and have a global partner network.

### Password Security Management

The Authlogics Password Security Management (PSM) is designed for IT managers and CISOs who require protection from identity attacks, and what simplicity for users while reducing helpdesk costs. PSM is a non-intrusive solution that ensures all users have a secure password which complies with the latest NIST SP 800-63B password policy standard. Unlike traditional MFA vendors who, despite relying on passwords within their solution, don't provide any password security or management, our solution removes the password complexity burden from users while ensuring the password they have chosen has not already been compromised.

PSM analyses password changes in real-time

and uses a combination of granular policy controls, a rules engine, a custom blacklist, heuristic scanning and is powered by the Authlogics Password Breach Database of over 520 million previously compromised passwords to keep your Active Directory safe and compliant.

### Cloud Password Blacklist

Ensuring that compromised usernames and passwords from an unrelated security breach are not used to gain access to corporate systems is a crucial part of meeting the NIST password guidelines.

Our cloud-based password blacklist consists of over 520 million compromised passwords collected from previous data breaches and attacks and is continually updated. An on-premises installation of the blacklist database may also be deployed if required.

Password Security Management performs secure and anonymous checks against this database, only accepting it if it is not found in this list.

### Product & Feature Usage:

- Password Security Management deployment on Domain Controllers
- Self Service Portal for interactive feedback to users while changing their passwords
- Cloud Password Blacklist for real-time protection and regular updates

**81%**  
of data breaches in 2017 were the result of stolen or weak passwords

**5 MILLION**  
records are compromised every day

**HOW SAFE**  
is your company's data?



### About Authlogics

As a global market leader in compliance and user authentication, at Authlogics we believe that increasing password security shouldn't have to mean compromising simplicity.

Our product suite offers users a complete, three-step solution for transitioning to modern authentication processes.

From our unique password compliance solution (Password Security Management / PSM), through our award winning multi-factor authentication (MFA) technologies, to enabling users with a completely password-less environment, at Authlogics we enhance your network security whilst maintaining an easy and uniform user experience, whether you're on mobile, desktop, or cloud.

# Authlogics



www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866