Blackfish Data Sheet

AT-A-GLANCE
Blackfish is an enterprise credential security solution that helps organizations protect their websites and mobile applications from criminals who use stolen credentials to take over customer accounts.

ADVANTAGES
- Closes gap between breach and discovery
- Alerts when stolen credentials are actually used elsewhere
- Leverages unique collective defense network to identify stolen credentials
- Doesn't require storage of compromised passwords

BLACKFISH PROTECTS YOUR LOGIN APPLICATIONS FROM STOLEN CREDENTIALS
The average person uses the same password across four different accounts. So even if your organization hasn't been breached, chances are many of your users’ credentials have been spilled elsewhere. Now, instead of waiting for attackers to try those breached credentials on your login applications, you can proactively safeguard your users from the risk of account takeover. Blackfish alerts your company in real-time when criminals actively use your customers’ credentials elsewhere on the web.

HOW IS BLACKFISH DIFFERENT?
Credentials spilled on the dark web are stale
Why are credentials on dark web marketplaces sold for mere pennies? Because criminals have already made their money from them. Criminals weaponize credentials first, and sell them last. When criminals first steal new usernames and passwords, they use the credentials against the highest value targets – the largest web and mobile apps in the world. It usually takes 6-12 months, or longer, for stolen credentials to end up on the dark web.

Blackfish knows when stolen credentials are first used
When a criminal commits a credential stuffing attack on any Shape customer, Blackfish captures the usernames and passwords that are being used and marks them as compromised. Blackfish then immediately alerts any customers for which those credentials are valid. Shape sees over 30M credential stuffing attacks per day and protects over 100M real human logins per day. In other words, Blackfish knows which credentials have been stolen even before criminals begin trading them on the dark web.

Blackfish provides a collective defense against criminal networks
An entire criminal ecosystem has emerged to enable information sharing and allow attackers to operate at scale. Now the security and fraud industry can fight back. The Shape network already includes the world’s highest-value organizations, who are also the world’s most-targeted organizations. Given this unique visibility Blackfish has the power to identify criminals’ very first attempts to weaponize credentials. The more organizations that use Blackfish, the sooner we can all cure the account takeover epidemic.

Blackfish doesn't store passwords
The security of the Blackfish system itself was the most important design consideration. Shape’s patented design uses a Bloom filter, enabling Blackfish to perform lookups of your user’s credentials without maintaining a database of compromised passwords.

“Because Blackfish can see all automated logins in real time, [it] can capture compromised usernames and passwords, instead of buying them.”
— Sarah Squire | Co-author of NIST Digital Identity Guidelines
HOW DOES BLACKFISH WORK?

HOW DO I DEPLOY BLACKFISH?

With 2 deployment options, Blackfish can be easily deployed to integrate with your existing infrastructure.

**Proxy Edition**

For customers of Shape Enterprise Defense, Blackfish Proxy Edition can be deployed using a supported SSE infrastructure. Once enabled and configured, Blackfish will display information about compromised credential use in the same SPM instance you are already using.

**API Edition**

For new customers who aren’t already using Shape Enterprise Defense, Blackfish API Edition provides a flexible integration option that can work with virtually any login application. When a credential is used to login to your web or mobile app, a simple API call determines if the credential is compromised. Code samples demonstrating recommended integration techniques are provided in several of the most common languages.

Both Proxy Edition and API Edition use the same SPM interface to present detailed information about compromised credential use.

Why is it named Blackfish?

Blackfish, or orcas, have remained one of nature’s apex predators by hunting in packs.

The Shape Blackfish solution for credential defense leverages a unique collective defense network that helps organizations work together to hunt down and eliminate stolen credentials.

PROTECT YOUR ONLINE BUSINESS TODAY

Protect your online applications from credential stuffing, account takeover, unwanted scraping, carding and other sophisticated online attacks and automation traffic that would otherwise result in large scale fraud, inflated operational costs, and additional friction for your users.