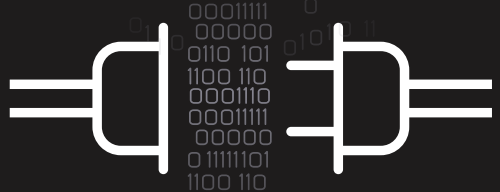
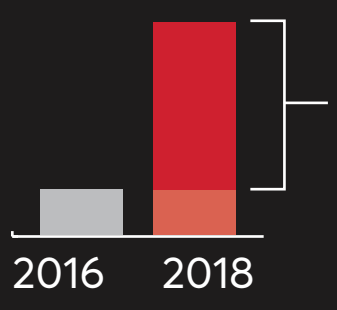
Top Five Reasons to Implement Privileged Access Management

Privileged access management is the creation and enforcement of controls over users, systems and accounts that have elevated or "privileged" entitlements.

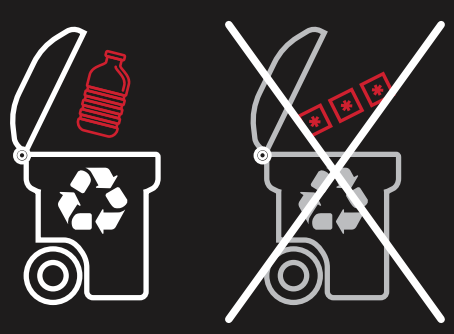
1 Mind the Gap



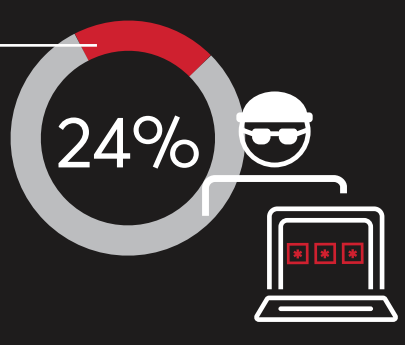


424%
increase in data breaches in 2018[1]

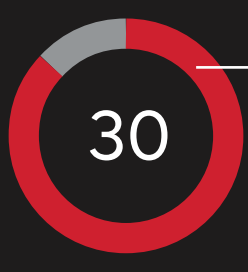
2 Reuse and Recycle— But Not With Passwords



24%
of employees know someone who has sold privileged credentials to outsiders[2]

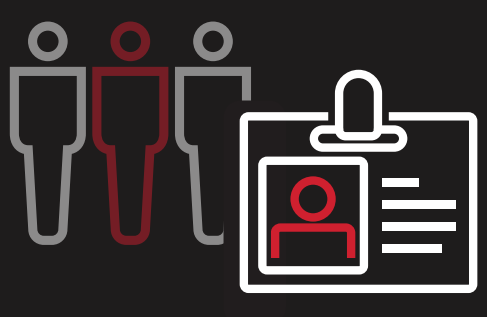


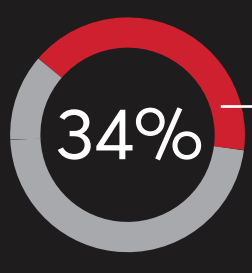
3 Your Luck Can Change in an Instant



billion credential stuffing attacks in 2018[3]

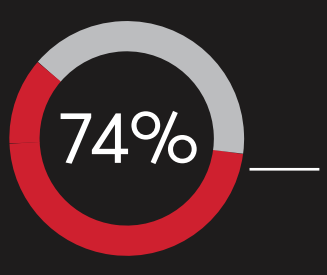
4 Et Tu, Brute?





of all data breaches were caused by insiders[4]

5 What's on Your To-Do List?



of data breaches start with privileged credential abuse[5]

The Keys to the Kingdom—Are You Protecting Yours?

Symantec Privileged Access Management defends and controls privileged users and the credentials they use to access and manage your digital infrastructure. It proactively enforces security policies and role-based limits on privileged user access—all while monitoring and recording privileged user activity across virtual, cloud and physical environments.

Key Benefits

- Control privileged access across all IT resources, from cloud to mainframe
- Apply unified cross-platform protection and management of privileged account credentials
- Automatically discover and protect virtual and cloud-based resources
- Provide tamperproof audit data and forensic evidence for all privileged user activity
- Segregate duties of superusers through fine-grained access control and secure task delegation
- Eliminate hard-coded passwords from apps, scripts, and files and support DevOps toolchains

[1] Bleeping Computer, March 2019
[2] Forbes, April 2018
[3] Dark Reading, April 2019
[4] Verizon 2019 Data Breach Investigations
[5] Forbes, February 2019

Symantec™
A Division of Broadcom