10 REASONS TO TEST, NOT GUESS

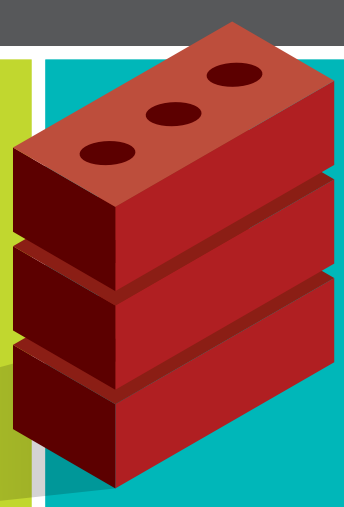
Security strategy shouldn't be a guessing game. Know what's working and what's not. Most importantly, know before an attacker does.

Databases, networks and applications make up your organization's security DNA. Effective security requires that businesses make fact-based decisions based on real-word knowledge of their databases', networks' and applications' ability to withstand attack. Make more informed security decisions. Learn the 10 reasons you should test, not guess.

REDUCE THE RISK

Vulnerabilities in databases, networks and applications introduce security weaknesses that can increase your data breach risk.

81% of businesses failed to detect data breaches themselves in 2014.



BUILD SECURITY INTO IT PROJECTS

77% of IT pros have been pressured to unveil IT projects that were not security ready.

SECURE YOUR INTERNET OF THINGS

Whether it's smart toilets, ATMs, WiFi-connected homes or business automation systems, Trustwave has tested many internet of things devices that lacked often-times basic security controls. Consumer and business products shouldn't hit the shelves before they're tested for security vulnerabilities.

PROTECT YOUR WEB APPS

98% of web applications tested by Trustwave were vulnerable with a median number of 20 vulnerabilities per application.

GO MOBILE, SAFELY

95% of mobile applications tested by Trustwave were vulnerable.

PROTECT YOUR DATABASES

Cyber-criminals are after data – sensitive, valuable and saleable data. Configuration mistakes, identification and access control issues, missing patches or any toxic combination of settings can lead to escalation-of-privilege or denial-of-service attacks, data leakage or unauthorized modification of data.

70% of IT pros believed they were safe from cyber-attacks and data compromises.

AVOID GETTING LULLED INTO A FALSE SENSE OF SECURITY

PLUG THE PASSWORD PROBLEM

"Password1" is the most common business password, and 39% of passwords tested were only eight characters long. It takes only one day to crack an eight-character password but an estimated 591 days for a ten-character password.

THE CLOUD NEEDS TESTING TOO

47% of IT pros were pressured to use or deploy cloud-based solutions.

CHANGE CAN INTRODUCE NEW VULNERABILITIES

Infrastructure changes introduce new vulnerabilities. If you don't test, and test often, you're likely putting your business at risk. Constant vigilance through testing puts you ahead of attackers.

Sources: 2015 Trustwave Global Security Report, 2015 Security Pressures Report from Trustwave, 2014 State of Risk Report from Trustwave, Forrester Research, Juniper Research, IDG Connect, USA Today

Trustwave®

www.trustwave.com/test