CASE STUDY

Securing Financial Data from Within

Corporate databases chock full of sensitive client information have become an increasingly enticing target for cybercriminals. And though plenty of attacks come from outside an organization, many of today's threats originate from within an organization in the form of improper user privileges.

When companies have too many people with high-level rights, chaos ensues if those employees undertake a malicious effort or have their accounts compromised by hackers. Trustwave's 2019 Global Security Report found that privilege escalation flaws, which allow low-level users to gain administrator-level access, is one of the most common database vulnerabilities.

Trustwave®

Client Spotlight

A major accounting firm, this client must manage and secure untold reams of personal and financial data for its thousands of clients spread across dozens of countries. And because certified public accountants are held to particularly high standards of confidentiality, a single cyberbreach can fatally damage a firm's reputation.

The Challenge

A global accounting firm needed to secure its databases, which were filled with millions of confidential records belonging to clients ranging from Fortune 100 companies and government agencies to very-high-net-worth individuals. The company wanted to ensure that only the appropriate personnel had access to client data. To do so, the IT staff needed to perform vulnerability management and user rights audits for each database it maintained. The problem? The firm didn't have enough in-house IT staffers who were expert in every type of database—and a dire industry-wide talent shortage made recruiting more workers difficult.

> *"With AppDetectivePRO, the client was able to accomplish a point-and-shoot audit program that provided information on misconfiguration, vulnerability, and user privilege."*
>
> Andrew Herlands, Vice President, Global Security Architects

Like many large enterprises, this company's databases and user rights hierarchies have grown unsystematically over a long period of time, making auditing and privilege management an arduous task.

The Solution

The firm implemented Trustwave's AppDetectivePRO, a database and big data scanner that identifies identification and access control problems, configuration mistakes, missing patches and other issues that can create escalation-of-privilege or denial-of-service attacks.

By quickly deploying the easy-to-use tool, the firm's IT team was able to easily audit all user access levels and configuration states and immediately identify any recent changes. In fact, the firm determined all users and privileges in just a couple of hours—versus the multiple days such a task would have otherwise required. The firm was able to do all of this with existing staff and avoid incurring additional headcount and training costs. The AppDetectivePRO dashboard and reports made it easy for firm executives to view—and understand—all vulnerabilities, risk and threats across its various database types.

Industry Threat

Accounting firms of all sizes are prime targets for cybercrime because they aggregate so much valuable financial data, from Social Security numbers to direct-deposit details. In 2017, malicious actors broke into a multinational professional service firm's networks—by compromising accounts with admin privileges—and accessed data belonging to major corporate and government clients. More recently, a major hack of accounting software used by 93 percent of Fortune 500 companies kept users offline and unable to file their clients' returns on time. Moreover, the evolution of modern offices heightens this vulnerability: As tax professionals at multinational firms globetrot to visit clients, access data on-the-go and rely on third-party accounting software, risk continues to increase.

> *"AppDetectivePRO goes beyond, 'Hey, you need to fix these vulnerabilities,' to also address how and why certain users obtained access."*
>
> Thomas Patterson, Trustwave Senior Product Manager

Trustwave®