BeyondTrust

IT Needs More Control Over Network Access Privileges

High-profile data breaches like those that hit the U.S. Office of Personnel Management, the IRS, Sony Pictures, Target, JP Morgan Chase, Anthem and Home Depot make news headlines nationwide.

But they represent a minuscule sample size of the number of breaches organizations large and small across all industries suffer every year. The Verizon Enterprise 2016 Data Breach Investigations Report (DBIR) reveals there were 2,260 data breaches worldwide just last year. Even more alarming, the majority of breaches go undetected for weeks, or even months. Preventing your organization from becoming another statistic requires you to have a dual focus: Keep the bad guys from getting trusted access, and preventing people and applications you trust from doing bad things. Organizations that implement effective privileged access best practices are much better able to mitigate the risks of suffering a data breach.

2,260 Data Breaches Worldwide in 2015

That is the key finding of the BeyondTrust 2016 Privilege Benchmarking Study. The global survey reveals that adopting privileged access management policies and technologies is critical to empowering IT and security departments with the information and control they need to jointly prevent breaches. And their top priority is to look inside the network.

Too often people (or sometimes applications) who enjoy trusted access to your network innocently and mistakenly take inappropriate actions. Sometimes they even knowingly abuse their privileges. The result is the loss or theft of crucial information. The DBIR confirms that humans are the weakest link. Phishing is still a prime attack vector: Users open about 30

percent of phishing emails — up from 23 percent last year— and a sizeable portion of those users make the mistake of opening malicious attachments or clicking on tainted links. Once a use has been compromised by a phishing attach, privileges will be leveraged to move laterally through the organizations to obtain access to critical data.

BeyondTrust in May 2016 set out to learn how the world's very best organizations manage privileged access. We commissioned a survey of nearly 550 senior-level IT, IS, legal and compliance executives involved in privileged access management. We asked all respondents 11 questions about their privileged access practices.

30%

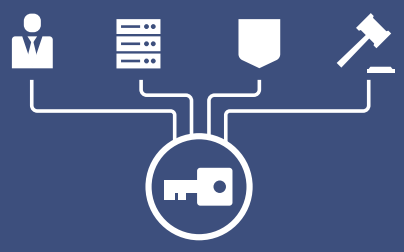
Portion of phishing emails opened up by users

Next, we scored each answer based on industry best practices. Those with the best overall scores became "Top-Tier" performers, while those with the worst overall scores became "Bottom-Tier".

Methodology

- Online survey fielded in May 2016
- 548 responses
- 29 questions
- Limited to:

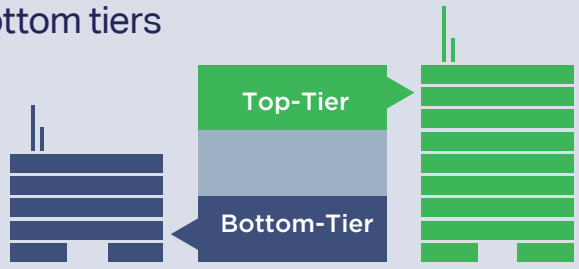
Executive, IT, IS, or Legal/Compliance departments Involved with privileged access management



Tiering Methodology

- 11 questions about privileged access practices
- Answers scored based on industry best pactices

Those with the best and worst overall scores were split into top and bottom tiers



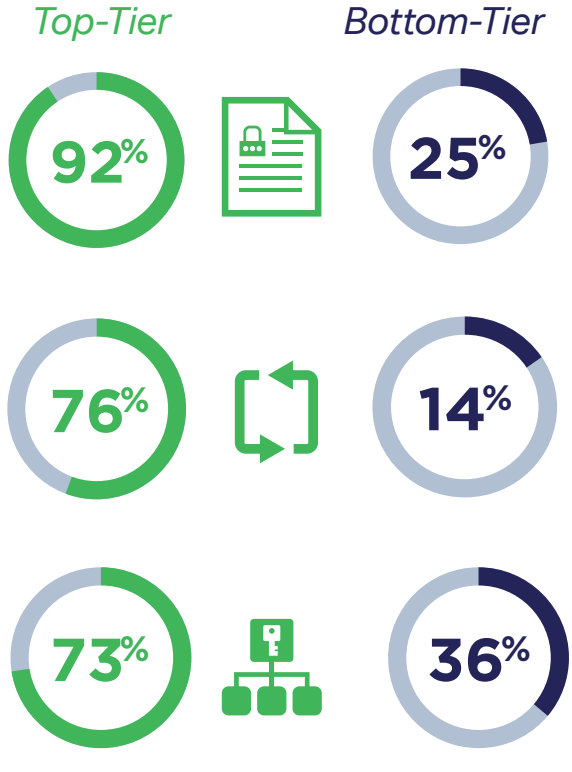
Scores Reveal Practice Differences Between the Two Tiers

PASSWORD MANAGEMENT

Most top-tiers **(92 percent)** have a centralized password management policy. Only **25 percent** of bottom-tiers do.

Leaving the creation and management of passwords up to the user creates risk. Most top-tiers **(76 percent)** cycle passwords for users "often" or "always." Only **14 percent** of bottom-tiers follow those best practices.

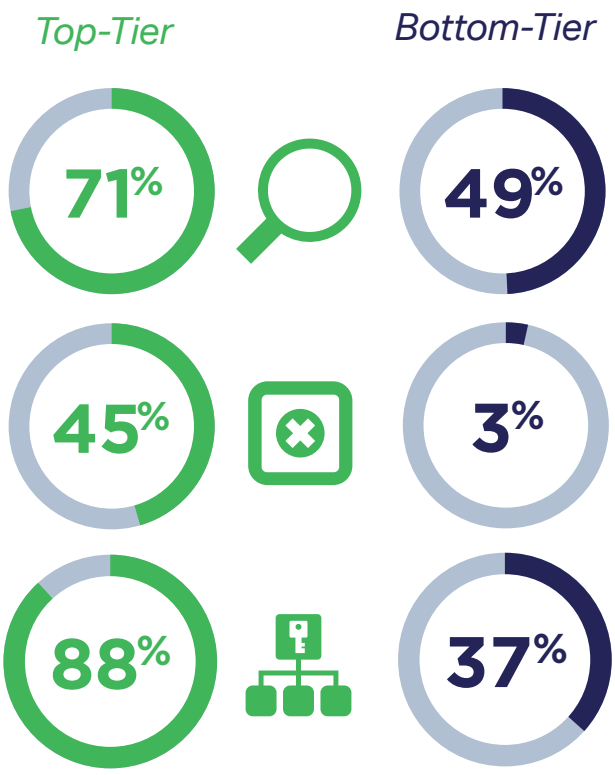
73 percent of top-tiers say they are "somewhat" or "extremely" efficient at managing credentials. Just **36 percent** of bottom-tiers say the same thing.



REAL-TIME MONITORING AND CONTROL

Most top-tiers **(71 percent)** have the ability to monitor sessions involving users with privileged accounts. Only **49 percent** of bottom-tiers have the ability to monitor. Almost half **(45 percent)** of top-tiers can watch and even terminate their sessions in real time while only **three percent** can terminate sessions in real time.

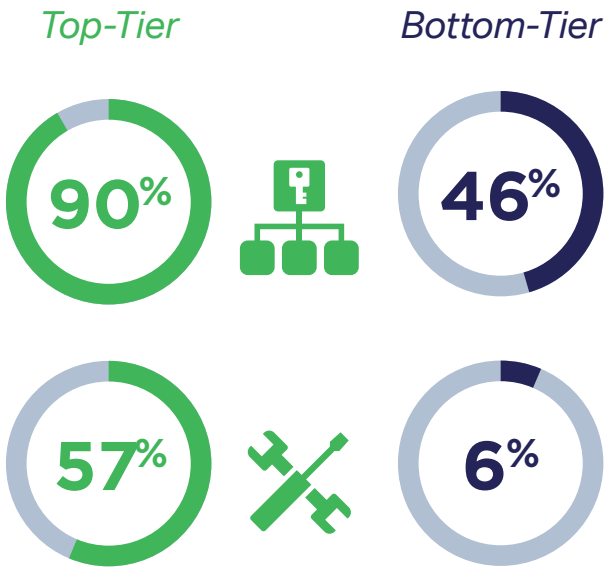
88 percent of top-tiers have granularity in how they can restrict the privileged access they grant (i.e., time and location). Only **37 percent** of bottom-tiers do.



MINIMIZING HUMAN ERROR

Top-tiers are more likely to take access privileges out of the hands of users. **90 percent** grant privilege to the app, not the user. Only **46 percent** of bottom-tiers do this, while the remaining 54 percent grant privilege to the user.

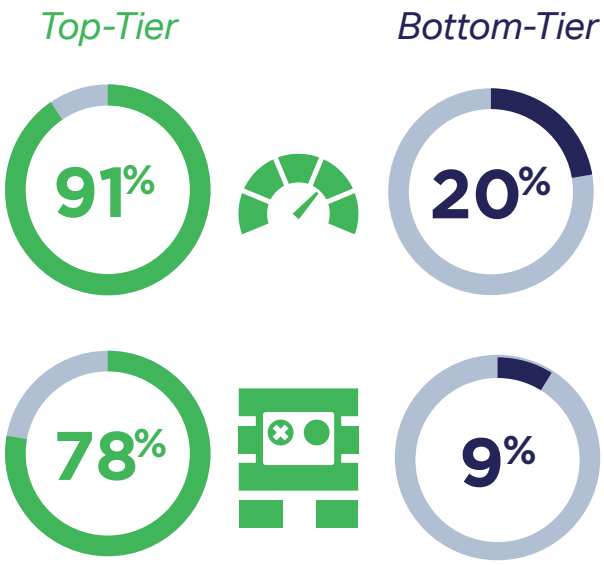
It's critical for IT and security teams to determine the relative risk for individual apps and systems. More than half of top-tiers **(57 percent)** have tools that provide this capability. They decide how to grant privileges to an app or system. Only **6 percent** of bottom-tiers do, with nearly half (52 percent) reporting "they just know" what the relative risks are.



MANAGING RISK

91 percent of top-tiers conduct vulnerability assessments to score their apps or systems based on their relative risk. Only **20 percent** of bottom-tiers do so.

The majority of top-tiers **(78 percent)** have an enterprise solution for managing privileged access. Only **9 percent** of bottom-tiers do. In fact, 39 percent of bottom-tiers do nothing at all.



Of course, becoming a top-tier organization is easier said than done. Hardening the security perimeter and reducing the risk that malicious and innocent insiders pose is a difficult job that gets harder each day. Networks are more complex and workforces grow more remote. The fact that app-to-app connectivity has grown, requires IT to give trusted access to apps themselves.

To further complicate matters, networks and operating systems supply a patchwork of tools that are not integrated and have very shallow capabilities. Some vendors offer enhanced tools with deep capabilities, but these point tools are still not integrated. This makes them difficult to manage and creates gaps in coverage that creates security vulnerabilities.

Recommendations

Fortunately, the data from the BeyondTrust 2016 Privilege Benchmarking Study points to five best practices that any organization can implement to improve privileged access control and accountability.

Implement granular least privilege policies to balance security with productivity: Ensure your users have only the right amount of privileges they need to do their jobs; nothing more, nothing less. Expect some initial resistance from users who worry about the appearance of restricting them from what they believe they need.

Use vulnerability assessments to achieve a holistic view of privileged security: Go beyond the standard protocol of delegating access to target systems. Employ super user privilege management, control privileges for administrators, and conduct vulnerability assessments to score applications based on relative risk.

Reinforce enterprise password hygiene with policy and an overall solution: Centralize password management, and manage passwords as part of the broader enterprise solution for managing privileged access. Also, be sure to cycle passwords for users and systems often.

Improve monitoring of privileged sessions: Enable IT and security organizations to monitor sessions and take actions in real-time. The ability to watch a privileged session live and pause or terminate that session provides a layer of control that can thwart a data breach.

Integrate solutions across deployments to reduce cost and complexity, and improve results: Cobbling together multiple tools makes managing privileged access unnecessarily complicated. When evaluating a privileged access management solution, consider two key factors: the breadth of its capabilities, and whether it can integrate with your other point security and risk management solutions.

When it comes to evaluating a privileged access management solution, you must consider two key factors: the breadth of its capabilities, and whether it can integrate with your other point security and risk management solutions. The objective is two-fold: Prevent outsiders from gaining trusted access; and provide trusted insiders with access to information and systems they need without compromising data security.