The problem with privileged users: What you don't know can hurt you

Why all the fuss about privileged users?

Today's users need easy "anytime, anywhere" access to information and services so they can do their jobs. The technologies needed to deliver that simplicity have become increasingly complex, and someone has to be there to keep it all running. These administrators (or super users) need "privileged" access to everything within the system in order to troubleshoot, resolve issues and maintain that immediate level of access.

This privileged access is necessary, but it can pose some serious problems. Today's increasingly complex environments require many administrators, from users with "root-level" access to key systems to Active Directory (AD) managers. And if you're like most companies, you may have more of these privileged users than you think.

According to the Ponemon Institute, most breaches and security incidents today come from insider activity. It isn't that privileged users are malicious—although some of them can be—that's not the only problem. With the level of access that privileged users have, even accidental or unintentional actions can create significant risk for your organization. While the number of breaches and incidents from true insiders is significant, the true scope of what constitutes an "insider attack" expands considerably when you consider the damage done by malicious attackers who gain access through privileged accounts. These attackers look like insiders, but actually aren't.

When a privileged user logs in, how do you know that it is really them and not a hacker with stolen credentials?

Today's hackers know the importance of gaining the access rights of privileged users (or any user with broad access rights). Your data is a precious commodity, and there's a good chance that someone wants access to it, whether it is personal data, credit card information, corporate secrets or even access rights shared between companies. Hackers have become very good at acquiring the credentials of these privileged users and infiltrating systems. Once they're inside—the question becomes not "if" they can gain access to everything," but "when" they will gain access to everything.

FOUR STEPS TO REDUCING BREACH RISK:

- *Limit the level and number of access rights granted*
- *Monitor changes and access to the systems and data that matter most*
- *Use identity to determine if user activity is business-appropriate*
- *Establish a baseline of "normal" behavior*

NetIQ

What's behind **insider activity breaches?**

Lost or stolen computing device **49%**

Unintentional employee action **46%**

Third-party mistake **41%**

Criminal attack **40%**

Technical systems glitch **32%**

Malicious insider **12%**

Intentional non-malicious employee action **8%**

Note: All incidences of breaches were included so there were multiple answer possible.

Source: "Fourth Annual Benchmark Study on Patient Privacy & Data Security", Ponemon Institute Research Report 3/2014

The question you have to ask is this: When a privileged user logs in, how do you know that it is really them and not a hacker with stolen credentials?

You can't eliminate privileged users—but you can reduce the risk

The answer is actually pretty simple: Use a risk-based approach. First, identify projects that are a business priority and align your resources accordingly. Within these key projects, place the best protection that you can around your data and systems that matter. Then, pay attention to what's happening to, and being done with, that data. Because the problem isn't that hackers have access to sensitive data—the problem is that they're going to use that access to do something you don't want with the data.

So what does a risk-based approach look like? The first principle is simply limiting the level of access granted to privileged users across the employee lifecycle. In many organizations, privileged users not only have administrator privileges, but the privileges they have are too broad. And once those access rights have been granted, they often aren't revoked in a timely fashion. This happens because it is difficult or time consuming to provide granular access rights, and people either don't have time or they forget to turn off access once it is no longer needed.

Second, look at the data and systems that matter most to your organization. Make sure that you have a solution in place that can alert you when certain critical pieces of data or certain systems have been accessed or changed. And ideally, you should be able to tell who has made the change, when they made it and from where. But just knowing who has made the change isn't enough—changes are made all the time, and you'd spend all your time chasing after false alarms. Unfortunately, that's the default state of most security teams.

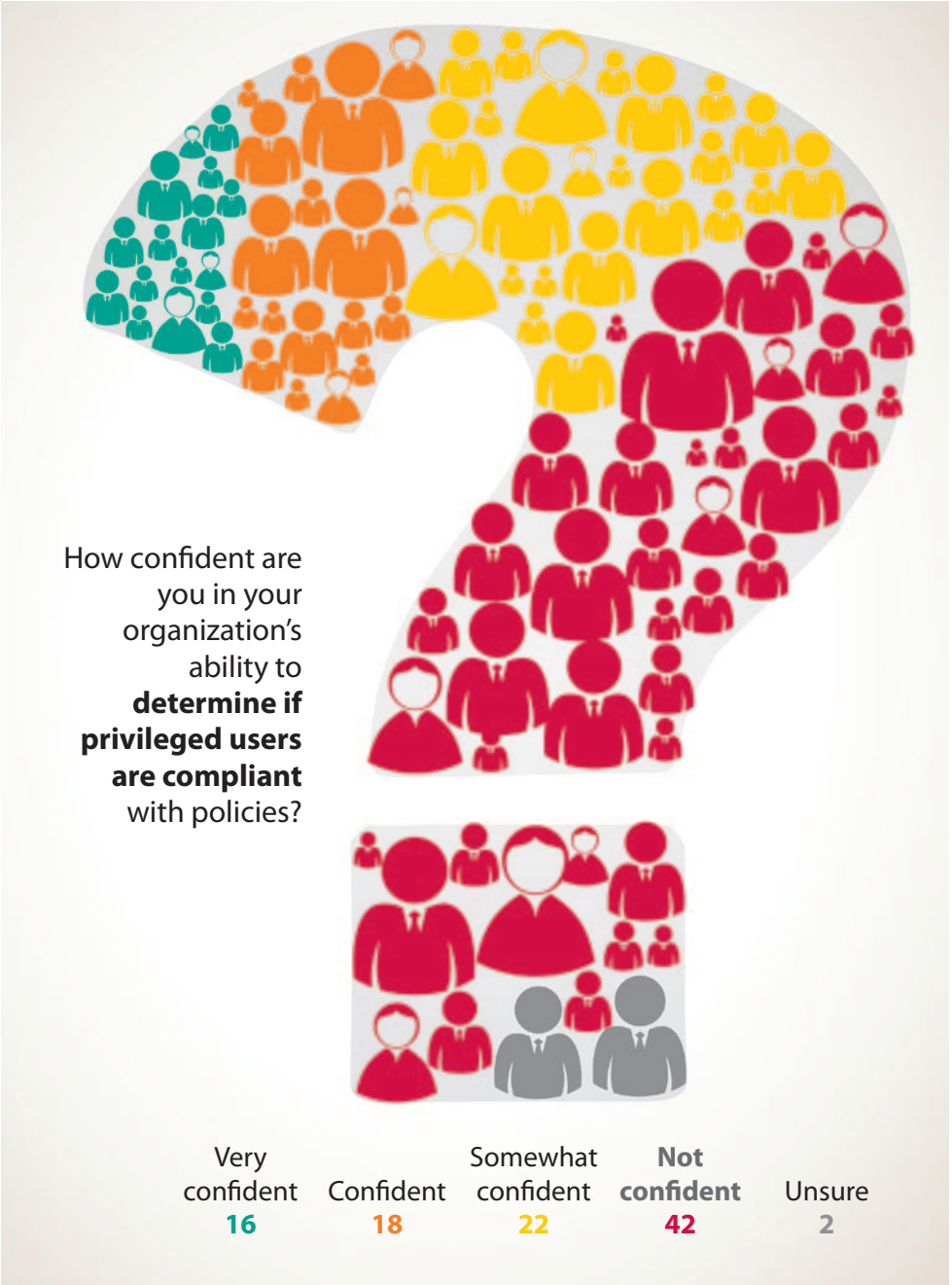
The third key to managing privileged users: identity. Identity goes beyond the access credentials of the user to provide additional context such as business role and location. When you integrate this identity context into your security monitoring data, you gain real security intelligence that helps you to better understand when user activity is appropriate (Yes, Bill should be accessing the server from our offices at 3:00 p.m.), and when activity is suspicious and should be investigated (No, Bill probably shouldn't be accessing the server from halfway around the world at 3:00 a.m.).

And that brings us to the final key to managing privileged users: tracking behavior. You have to be able to track behavior and link it to the identity behind the user account. To track behavior in a meaningful way, you have to establish a baseline of "normal"

behavior against which to measure. This is important even when things accidentally go wrong. Root-level users can mistakenly alter system settings and bring entire networks down. If you can't tell what was done to create the problem, it becomes much more difficult to fix. But if you're able to retrace their steps, you can identify where the problem occurred and fix it. More importantly, behavioral tracking allows you to triangulate on threats—is the data sensitive? (Yes/no) Should the user be accessing that data based on their role? (Yes/no) Should they be doing whatever they're doing with the data? (Yes/no)

Unintended outages can be big problems. Popular cloud services, such as Amazon Web Services (AWS) are used by many start-up Internet companies and increasingly by large enterprises. Netflix is one of the companies that uses AWS. On Christmas Eve in 2012, Netflix experienced an outage, not the result of a malicious attack, but rather an error in assignment of access rights that allowed critical files to be inadvertently erased. Resolving the outage took several hours.

Simple access mistakes can prove to be costly—both financially and in customer experience.



Source: "Privileged User Abuse & The Insider Threat", Ponemon Institute Research Report 5/2014

Automating systems can keep out problems:

1. **Automated provisioning/ de-provisioning/ re-provisioning of user access rights and privileges**
2. **Centralized HR source for creation, deletion or updating of rights**

This is especially helpful when large groups of users who require privileged access (such as contractors or temporary employees) leave the workforce. Don't leave the door open for them!

Let's face it: the only truly secure solution would be to not grant any access—but you can't do that, so the best approach is to ensure that you're only allowing the right level of access. The beauty of this sort of approach is that it doesn't prevent administrators who should have access from doing their jobs—they can continue as before. And—because response to monitored incidents can be automated—it alleviates the need for security staff to manually review incident logs.

The combination of limiting elevated access rights; change and access monitoring of critical data and systems; and the application of identity-enriched context and behavior tracking to security monitoring leads to a better understanding of potential impacts. This approach not only facilitates the identification of incidents and breaches, it can do so faster and provide better information for how to fix them.

Choosing the right solution

There are many ways that you can address these problems, from a range of Security Information and Event Management (SIEM) products, to identity management solutions, change management systems and automation solutions. However, as you evaluate your choices, make sure that you choose an option that will:

- **Work together seamlessly.** While each of the systems serves a unique purpose, they are actually complementary. In an ideal scenario, they need to be able to talk to each other and hand information back and forth. If they don't, you aren't really solving the problem in the first place.
- **Allow sufficient automation.** Let's face it—this is a lot of stuff that we're expecting to happen. If it requires manual intervention or extensive subject matter expertise, it isn't going to be practical. And the whole point of this endeavor is to try to make it easier for your team to distinguish between real threats and incidental events.
- **Allow policy-based monitoring.** Enriching security monitoring with identity context doesn't really help if you can't build a set of rules and policies around particular business scenarios. This is the piece that really brings the whole solution together.

- **Be affordable for the long term.** Think beyond the purchase price and consider what it'll cost long term. Is it easy to use? Will it work with the systems you already have in place? How much additional management time is needed? How much additional training will you need?

As you evaluate which solution will work best for you, consider Identity-Powered Solutions from NetIQ. They integrate with identity management, access and security solutions to help organizations reduce the number of users with privileged access, ensure people have the right access when they need it and provide the identity context for security monitoring to respond to breaches and reduce risk. These solutions allow businesses to leverage identity intelligence so that you can balance the access required for productivity with the growing security challenges in our hyper-connected world.

- NetIQ® Change Guardian™ provides the who, what, when and where for user activity in the enterprise, whether it be configuration changes or access to sensitive files (file integrity monitoring). It gives you the security intelligence you need to rapidly identify and respond to privileged user activities that could signal a data breach or result in compliance gaps.

- NetIQ Sentinel™ is a full-featured SIEM solution. Sentinel simplifies the deployment, management and day-to-day use of SIEM. It readily adapts to dynamic enterprise environments and delivers the true actionable intelligence security professionals need to quickly understand their threat posture and prioritize response.

- NetIQ Identity Manager delivers a complete, yet affordable, solution to control who has access to what across your enterprise—from inside the firewall and into the cloud. Identity Manager enables secure and convenient access to critical information for business users, while meeting compliance demands.

- NetIQ Directory and Resource Administrator™ provides smart AD administration features like granular delegation of administrative privileges and control of administrative access. It easily delegates proper administrative powers in AD and Microsoft Exchange Server without granting unnecessary access.

- NetIQ Privileged User Manager™ allows IT administrators to work on systems without exposing administrator or supervisor passwords, as well as root-account credentials to the administrator. It specifically targets managing, controlling and recording of all privileged administrator activities for UNIX, Linux and Windows environments.

Learn what next steps you can take by visiting NetIQ.

About NetIQ

We are a global enterprise software company that meets the demands of today's IT environments with a wide range of proven solutions for identity and access management, security and data center management.

Today's hybrid IT infrastructures are creating new challenges for business and IT leaders. IT services are now being delivered across an increasingly fragmented combination of physical, virtual and cloud environments. These services are being accessed from an expanding number of locations, on a growing variety of devices. And the technology environment is changing faster than ever. In the face of this combination of forces, organizations like yours often struggle to balance consumerized user expectations with the need to reduce organizational risk. All while still embracing the business value that can be achieved by leveraging innovations like cloud computing [link to cloud page] and mobile technologies [link to mobility page].

So how do you keep access to IT services simple, while preventing unauthorized or risky user activity—all in the context of where and how users are connecting? That's where NetIQ comes in. Our broad portfolio of Identity-Powered Access and Security solutions, combined with our data center management solutions helps you manage the complexity of hybrid environments to ensure that the right people have the right level of access to the IT services they need, whenever they need them. With NetIQ, you can incorporate new technologies and services more securely, faster and with less effort. And our solutions help you understand what is going on in your environment—in real time—so you can mitigate risk while still taking advantage of opportunities.

Quite simply, this means that you can secure, manage and measure what matters most to your organization. Even more important, this new level of clarity will create new opportunities—and competitive advantage—by enabling you to understand, maintain and make sense of the shifting relationships between individuals, devices, behaviors and technology services. That's how you can drive the successful business outcomes that will deliver ongoing value to your organization.

Learn what you need to do by visiting **www.netiq.com**.

Worldwide Headquarters

515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
Worldwide: +1 713.548.1700
U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com
http://community.netiq.com

For a complete list of our offices in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit **www.netiq.com/contacts.**

Follow us:

584-000014-001 PO 12/14