opentext™ | Cybersecurity

White Paper

Protecting the Crown Jewels: Privileged Account Management

Today's workers access company information from anywhere, and most organizations are not doing an adequate job of keeping it safe from hackers. To do that, you need to carefully manage and monitor the users and bots (yes, bots) with access to your most sensitive information. Here's how to do it.

Protecting the Crown Jewels: Privileged Account Management

Security management has changed radically over the last decade.

In the past, organizations protected their most critical assets in on-site data centers.

Today, they store information both on-premises and in public and private clouds. Employees, partners, and contractors access this information outside the company's four walls on a wide range of devices, each with its own operating system and security features. Even if you still keep your most sensitive information in-house, people are getting to it from other places.

The company is no longer a fortress you can defend from the inside. The first new layer of defense has been to build firewalls around systems and applications. We've done a pretty good job of that. Some brute-force attacks still get through, but they're no longer the main problem.

What is? People—people who have access to critical systems and information that could do enormous damage if they get into the wrong hands.

Attackers who gain access to privileged users' credentials sometimes lurk undetected for months while they learn a company's systems and decide what to steal. They can exfiltrate the contents of entire databases and delete logs to hide their activity.

Outside Threats

Sophisticated hackers direct phishing and spear-phishing attacks at people in-the-know—the executives, system administrators, network managers, engineers, and security workers who hold the keys to your finances, intellectual property, customers, formulas, and manufacturing processes—the secrets that make you succeed.

Many of these users are sophisticated themselves, but they're still human and susceptible to cleverly-placed hooks. When Russia's "Fancy Bear" hackers targeted U.S. defense contractors through spear phishing emails, as many as 40 percent clicked the phishing links, the first step in opening up their companies to data theft.

Attackers who gain access to privileged users' credentials sometimes lurk undetected for months while they learn a company's systems and decide what to steal. They can exfiltrate the contents of entire databases and delete logs to hide their activity.

Inside Threats

Workers can also be careless—even privileged account holders. At one company with a distributed IT team, employees set up a Dropbox account containing passwords for the routers, switches, and all the other equipment that ran the company's network. The account was not secure at all, but made it easier for workers to access the information.

Given a choice between convenience and security, most people go for convenience. It's just how we are.

No matter how strong your hardware and software firewalls are, they don't protect you from threats to and from insiders. They don't address our human desire for convenience and our propensity for error.

Humans have always been the weakest link in the security chain. Instead of shrugging our shoulders, it's time we addressed the problem.

Humans have always been the weakest link in the security chain. Instead of shrugging our shoulders, it's time we addressed the problem.

Reduce Threats with Privileged Access Management

Of course, you can't change human nature or control the people who work with you. But you can control what they do, and how and when they do it.

Identity and access management is the foundation of security today, and privileged accounts—the keys to your kingdom—are at the heart of it. To secure their most important assets, organizations must do a better job of managing privileged accounts.

Too many ignore the problem. IT departments always struggle to balance security with costs, and many simply aren't putting their ammunition in the right places. A PwC study found that more than 40 percent of businesses do nothing to manage their privileged accounts, and nearly half have no security standards for their external business partners and contractors, either. Others have a scattershot, hit-or-miss approach to privileged account management.

These companies are setting themselves up for a painful data breach. Attacks by malicious insiders or criminals are costlier than system glitches and negligence. The average breach costs a company $4.24 million, according to the Ponemon Institute. That's a lot of money to pay for a few moments of letting down your guard.

You can optimize your infrastructure investment and lower your total cost of ownership by preventing attacks on your most critical systems, and privileged account access management is the key.

How OpenText Manages Privileged Accounts

Managing privileged accounts requires foresight, planning, careful execution, and constant vigilance. It can be tricky, and a lot of companies get it wrong.

OpenText™ gives you the best privileged account protection possible with a comprehensive four-part system that covers all the bases. Here are the steps we take to make it work:

- **Discover.** The first step in managing privileged accounts is to know who has them.

  Most organizations have no idea how many privileged accounts they have or where they are. OpenText has the tools to find them. We look across networks, directories, and application servers throughout company groups and offices and spot all the accounts that have access to important data or critical systems.

You might think you don't have that many. Most companies are shocked when their list comes back. One organization we worked with had 25,000 employees and 8,000 privileged accounts. Some companies actually have more privileged accounts than people.

How can that be? Microsoft Windows, the operating system used by most companies, allows you to have service accounts, which are run by systems and applications, not people.

Accounts are not just for people. They can be held by systems, devices or internet-of-things sensors in machines. Anything that has access to critical systems is a privileged account, whether it's in Windows, Linux, Unix, or another operating system.

While it's normal to have a large number of privileged accounts, most organizations have far more than they need.

Accounts are not just for people. They can be held by systems, devices or internet-of-things sensors in machines. Anything that has access to critical systems is a privileged account, whether it's in Windows, Linux, Unix, or another operating system.

- **Simplify.** Providing too much root-level access to critical systems broadens your surface of attack and increases system complexity, making intruders harder to spot. You need to simplify.

  Chances are, you're still granting access privileges to employees or contractors who no longer need them, simply because no one thought to revoke them. That's the first logical place to swing the axe.

  Another is old service accounts. These accounts, which are operated by web servers, mail transport agents, and databases, should be disabled after they perform their functions. But many times, they're not. They provide an ideal opening for intruders because nobody pays attention to them—they appear to be machines just doing what they were programmed to do. OpenText helps you identify them and shut them down when you no longer need them.

- **Control.** Once you've cut out all your non-essential privileged accounts, you need to manage what's left. To do that, OpenText employs the principle of "least privilege." That means giving people (or service accounts) just enough access to the resources they need to do their jobs, but no more.

  How do we do that?

  By mapping accounts to current job functions and keeping track of changes. The way we do it depends on the role.

  Some roles operate through what we call "structured administration." People in these jobs perform a defined, repetitive set of tasks—for example, the IT help desk worker who resets passwords.

  These people need to access some of your privileged information, but certainly not all of it. Yet many organizations grant them full access, and others provide much more than they use. OpenText limits what they can see and do to only what they need.

  It's all too easy to set blanket permissions, but the consequences can be dire. OpenText provides an additional layer of security by requiring two administrators to confirm a change.

  Why would you need that?

One company that was preparing for a quarterly review had an administrative assistant working overtime to gather information about customers from 20 databases across the enterprise. At 11 p.m. one night, she accidentally pressed the delete key. It turned out the backup program hadn't been working for six months. The company lost over $35 million because it no longer had the information it needed to run the business.

Permissions aren't always straightforward because roles aren't always clearly defined. A network engineer may work on upgrading a network one day and managing a database the next. For "unstructured" administrative roles like this, we use privileged session management to make sure that on any given day, workers only access the applications and systems necessary to perform their duties, even if they have the ability to go beyond that.

Permissions aren't always straightforward because roles aren't always clearly defined. A network engineer may work on upgrading a network one day and managing a database the next. For "unstructured" administrative roles like this, we use privileged session management to make sure that on any given day, workers only access the applications and systems necessary to perform their duties, even if they have the ability to go beyond that.

In addition to job function, you can control access by location and time. An executive in New York shouldn't be logging onto the server in London at midnight. A regional database manager doesn't need to see revenue information at headquarters.

These controls provide security while still giving organizations the flexibility they need to operate efficiently. For example, publicly traded companies must restrict employees from making changes to their retirement and investment plans during blackout periods. OpenText makes it easy to revoke and later restore their access.

We also help you keep track of job roles to avoid "privilege creep" when people change positions and no longer need the same access they had before.

If Société Générale had applied this kind of restriction to rogue trader Jérôme Kerviel, he wouldn't have been able to make 50 billion euros worth of unauthorized trades. Kerviel was jailed for forgery and fraud, but interestingly, a French court also ordered the bank to pay him over $500,000 for improper dismissal, citing weaknesses in its own risk-management procedures.

It's your responsibility to control who has access to your data.

- **Monitor.** You should monitor all privileged accounts 100 percent of the time. The mere presence of a monitoring system is enough to deter some users from misdeeds. No one wants to get caught.

  You may think you're already covered if you have a security and event management system that does real-time monitoring of your networks and hardware. But you're not. Those systems don't provide enough information to the security team to let them know of potential threats from users.

  OpenText's advanced user activity monitoring system alerts the security operations center whenever a privileged user acts outside of policy or tries to make changes that could pose a threat. The system can monitor specific console commands and record and play back all activity to the security team in near real time. That gives them the critical time they need to react before a system is altered or data is stolen.

Simplify Auditing

In addition to being a critical component of security, OpenText's monitoring system helps you meet compliance and auditing requirements. It records all administrative activity, and compresses and stores it in tamper-resistant logs. The logs provide detailed information on who accessed your data, when they did it, what they retrieved, and where the data was stored. You can easily generate customized reports, both for your own use and to show regulators how well you meet security requirements.

Monitoring privileged accounts gives you peace of mind so that you can focus on growing your business instead of worrying about threats.

It's All About Time

No security system—not even ours—is guaranteed to keep all hackers out or prevent malicious insiders from trying to cause trouble.

The key to privileged account management is buying time. Identifying, simplifying, controlling, and monitoring privileged accounts gives your security team a critical heads-up when user activity looks out of place.

Nothing, absolutely nothing is more crucial to security than reaction time. Monitoring your equipment can tell you when something's amiss, but it may be too late. The only way to save your critical systems and information is to stop privileged users in their tracks, before they can inflict damage. Months of forensic analysis will never make up for the harm that can be done in just a few minutes.

An attack can occur at any time, and from people you'd never suspect. At one energy company, an IT worker learned that layoffs were coming to his department. Before he was let go, he used his privileged credentials to obtain the company's specifications for oil and gas fittings, which he sold to a competitor.

The theft wasn't discovered until a year later. If the company had monitored his activity at the time, it never would have happened in the first place.

Monitoring privileged accounts gives you peace of mind so that you can focus on growing your business instead of worrying about threats.

If a contractor in Atlanta visits your finance database in New York at 2 a.m., the security operations center can shut off his access immediately—before he has a chance to steal data—and ask questions later.

The crucial minutes they gain can make the difference between an uneventful day that no one remembers and a breach that costs millions of dollars.

Improving the Security Operations Center

The OpenText privileged access management solution also has a broader benefit: it enables your security operations center (SOC) and security and event management system (SIEM) to be far more efficient and productive.

Traditional SIEM solutions rely on analyzing logs of events from operating systems like Windows. These logs are chock full of discrete events that provide little useful information on an individual basis. For example, there may be as many as eight separate events to indicate the simple renaming of a file.

Reviewing a multitude of events is not only tedious and time consuming, it diminishes the SOC's effectiveness in spotting suspicious activities and responding to them in a timely manner.

OpenText has a different approach. Each event in our system is given context—it answers the all-important questions of WHO did WHAT, and WHEN and WHERE they did it. These easy-to-read events reduce the time it takes for SOC investigators to see what's going on. As a result, the SOC improves its reaction time and formulates more effective solutions for stopping malfeasance in its tracks.

Connect with Us
www.opentext.com

About OpenText

OpenText provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, OpenText customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the OpenText homepage at **www.cyberres.com/netiq** to learn more. Watch video demos on our OpenText Unplugged YouTube channel at **www.youtube.com/c/NetIQUnplugged**.

NetIQ is now part of OpenText's Cybersecurity line of business

Learn more at
www.microfocus.com/en-us/cyberres/identity-access-management/privilege-management

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.