BeyondTrust

# THE 7 PERILS OF PRIVILEGE

Common Security Pitfalls
& How to Avoid Them

> **"The dangers of cyberattacks continue to evolve, and understanding the underlying risks is critical to protecting your business."**

## Introduction

Cyberattacks are continuing unabated, impacting companies in all industries and regions. The threat landscape evolves quickly, and the pandemic and massive shift to remote working caused attackers to quickly pivot to exploit new vulnerabilities — 94% of companies experienced a business-impacting cyber-attack in 2020.

Headlines are ablaze with large-scale breaches, from SolarWinds and Colonial Pipeline to the UK's National Health Service (NHS) and Virgin Media. The list is endless — hackers do not discriminate when it comes to industry or company size.

Despite these threats, many organizations struggle to identify and implement the right security strategies and solution. This can be for multiple reasons — lack of resources, issues with prioritization,  or simply a 'It can't happen here' attitude.

Outlined in this document are "7 Perils of Privilege," how they impact security at your business and guidelines on how to prevent them. Regardless of which ones resonate with you, there are solutions to avoid falling victim and mitigate the risks of a cyberattack.

# The Speed of Digital Transformation

## Digital Transformation now, security later


of organizations are engaged in a Digital Transformation project[1]


of companies experienced a business-impacting cyber-attack in 2020[2]

*Sources: 1. Nominet: Cyber Security in the Age of Digital Transformation, 2019*
*2. The Rise of the Business Aligned Security Executive Report, Tenable, 2020*

According to a study by Nominet, 93% of organizations are currently engaged in a digital transformation project. In the wake of the coronavirus pandemic, **the massive shift to remote working has also accelerated cloud adoption** as a key driver of digital transformation initiatives related to productivity.

The promises of what Digital Transformation can achieve for the efficiencies of business can tempt companies to roll out new technologies without prioritizing their security strategy. The fast pace at which this happened meant that security may not have been adequately considered.

**The promises of Digital Transformation projects can tempt companies to roll out new technologies without prioritizing their security strategy.**

And employee behavior when using personal "BYOD" (Bring Your Own Device) smartphones or laptops presents issues as well. A recent poll by Gartner found that remote workers are more susceptible to using personal devices to commit "Shadow IT sins" — finding and using third-party applications outside of those approved by IT.

It is critical that organizations who are undergoing digital projects consider the importance of cybersecurity. Ecosystems are expanding, perimeters are evolving, and the explosion of privileges have all contributed to the expansion of the attack surface. A comprehensive Privileged Access Management solution can mitigate these risks by managing and controlling users, sessions, and passwords across your network, including those related to digital transformation or cloud deployments.

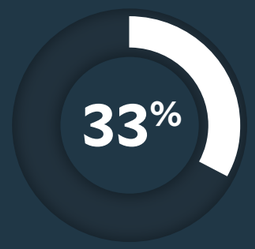
**To Learn More:** **Secure Your Digital Transformation Journey**

# Cloud Proliferation

## All that data, all those clouds, all those privileges

**1,935**

average number of cloud services used by an organization [3]




of all data exists in (or passes through) the cloud [4]

*Sources: 3. Cloud Adoption and Risk Report McAfee, 2019*
*4. Hosting Tribunal, Big Data Stats for the Big Future, 2021*

Today, most organizations are not merely in 'a' cloud—they are in many clouds (PaaS, IaaS), and their end users consume dozens, or even hundreds, of different SaaS applications. The great cloud migration is enabling the successes of increased remote working and is propelling a renewed embrace of digital transformation initiatives.

But with this mass shift to cloud comes **more opportunities for hackers, with more attack vectors to explore and multiple pathways into your network.** If your environments lack sufficient security architecture and management of identities and credentials, hackers will exploit the gaps to compromise your network.

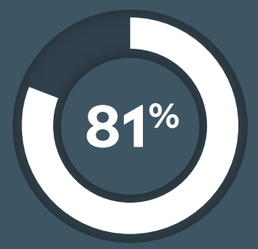
Last year, cloud-related cyber-attacks were up 630% according to McAfee's Cloud Adoption Risk Report. Adopting security practices focused on securing cloud identities play a key role to decrease these risks, and include enforcing least privilege, discovering and managing cloud assets and privileged accounts, implementing application control, and securing your DevOps tools.

**Most organizations employ three or more public clouds... that's three or more times the security risk.**

**To Learn More:** **The Guide to Multicloud Privilege Management**

# 3 Risky Password Practices

Yawn — is creating complex passwords and changing them regularly really necessary?




of hacking-related breaches involve either stolen or weak passwords[5]


data breach victim accounts used 123456 as their password[6]

*Sources: 5. Verizon Data Breach Investigations Report, 2019*
*6. National Cyber Security Centre (NCSC) Survey, 2019*

**It only takes one compromised password to initiate a breach that could have devastating results.**

According to a recent study by NordPass, **the average person has around 100 passwords they need to remember.** As a result, employees are often overwhelmed and may store passwords insecurely or reuse the same password across multiple accounts.

Insecure password storage and lack of rotation have been proven to lead to phishing attacks and breaches; multiply this risk of vulnerable passwords by the number of users accessing your network. If an employee with administrative privileges is using a low-strength password across multiple accounts, then it will take a hacker minutes to infiltrate a network and deliver ransomware.

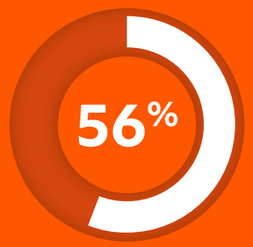
You can't depend on users overcoming the limits of human nature. To address password risk, take away the pain point for end users. Instead of asking them to create and keep track of complicated passwords for multiple accounts, give users a tool for system access that doesn't require them to know the password. A phishing attack relies on tricking a person into clicking a link or providing their credentials through convincing social engineering methods, but a user can't compromise a password they don't know.

Credential Injection is a feature of leading remote access and password management solutions, enabling users to simply select from a list of credentials to log in to the systems they are approved to access. This eliminates the need to store and track shared credentials manually and creates a more productive user experience by streamlining access to shared passwords.

**To Learn More:** **Privileged Password Management Explained**

# 4 Too Many Admin Rights

## Do all those employees really need admin rights?




of critical Microsoft vulnerabilities in 2020 could have been mitigated if admin rights were removed[7]


of organizations expect privileged user sessions to increase significantly in the next two years[8]

*Sources: 7. Microsoft Vulnerabilities Report 2021, 2021*
*8. Evolving Privileged Identity Management (PIM) In The 'Next Normal', 2020*

The need for access is a persistent issue, and **users are often given full administrative rights in roles that do not warrant them**. They give employees full access and control of their systems, in the hope that they will never need to bother the IT service desk. The employee is happy because they are self-proficient. The organization is happy because productivity has not been impacted. The service desk is happy because they are not overloaded with access requests. However, this approach presents a huge security risk as overprivileged accounts are lucrative targets for threat actors.

Stop attacks by tracking and controlling the use, assignment, and configuration of administrative privileges on computers, networks, and applications. Implementing the principle of least privilege and removing administrator rights is a key requirement for many compliance mandates around the world, and removing admin rights is the single best step you can take to mitigate critical Microsoft vulnerabilities. However, you must also consider the impact to users – if they suddenly become too locked down to complete their day-to-day tasks, they will become frustrated and the service desk could become overwhelmed with requests.

Effective Endpoint Privilege Management solutions can implement least privilege in hours, without over-restricting users or driving up service desk tickets. Organizations are made far more secure, and end user productivity is not impacted – effectively solving the security vs. productivity balancing act.

**Excessive admin rights enable ransomware attacks to quickly take hold and spread across a network.**

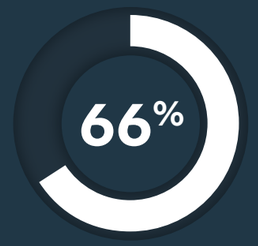
**To Learn More:** **Microsoft Vulnerabilities Report 2021**

# Malicious Insiders

Hell hath no fury like an employee scorned!

**$11.45 million**

the total average cost of insider related incidents in 2020[9]




of global businesses consider insider attacks or accidental breaches more likely than external attacks[10]

*Sources: 9. 2020 Cost of Insider Threats Global Report, Proofpoint & Observe IT, 2020*
*10. Tech Journey, Insider Threat Statistics, 2021*

**Malicious insiders are a leading cause of cyberattacks.** They are classified as current or former employees – even contractors or business associates - who have information concerning the organization's security practices, data and computer systems. While many insider breaches are a result of unintentional mistakes, in the case of this peril, it is the wrath of a disgruntled former employee that creates significant risks to your cybersecurity.

**Insider attacks are initiated by disgruntled employees wanting to harm their current or former organizations through data theft and sabotage — or to seek financial gain.**

Recently, Cisco lost approximately $1.4 million in employee time to audit their infrastructure and fix the damage caused by a former employee's unauthorized access. The company also had to pay a total of $1 million in restitution to affected users. This is just one of many insider threat cases highlighting the ramifications at stake.

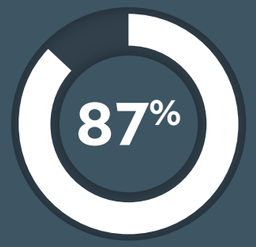
Taking positive steps to mitigate insider threat risks include implementing least privilege, rotating privileged credentials frequently, and accounting for job role changes (including employees leaving the organization) by changing or removing their access in a timely manner. Privileged Password Management solutions securely control, monitor, and record access to privileged accounts. Keep passwords fresh with automated rotation – either on a scheduled basis or upon check-in after use - to eliminate the risk of passwords leaving the organization.

**To Learn More:** **Privileged Access Threat Report**

# 6 Too Much Confidence

## Of course our employees are vigilant and aware of cyber threats


of organizations lost data due to a phishing attack in 2020[11]




rise in phishing attacks on finance employees in 2020[12]

*Sources: 11. 2021 State of the Phish Report, Proofpoint, 2021*
*12. Abnormal Quarterly BEC Report Q2, 2020*

**Even the most diligent employees could still fall for a hyper-realistic phishing scam via email or social media.**

Every company would like to assume that their employees couldn't be fooled by a phishing attack – but the reality is that 65% of US businesses report experiencing a successful phishing attack. A recent Proofpoint report revealed that phishing remains the most likely threat type to cause a data breach, and hackers know this. The FBI reported that phishing was the most common type of cybercrime in 2020, with 241,324 incidents reported in the US alone.

It's not just phishing either. Other forms of social engineering in 2021 include the rise of deepfake attacks. Deepfakes are sophisticated forms of media (video, audio, photographs and even websites) that exude a realism that is able to convince the most knowledgeable professional. A recent revelation showcasing the concerning abilities of deepfakes was a spoof TikTok account that went viral for pretending to be Tom Cruise.

Artificial Intelligence (AI) is allowing deepfake technology to outpace our abilities to identify them. We could be engaging in communications in a chat window with (what we thought was) a human, but is in fact a malicious robot collecting sensitive information.

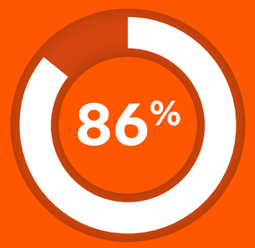
The prevalence of phishing, along with the increasingly convincing and sophisticated methods of deepfake delivery, means that **even well-trained users will still occasionally fall for these tactics, and it only takes one slip to result in a major breach.**

Cybersecurity awareness training is a good step to take, but it has limits.  Your employees are human beings, who may still make mistakes even with extensive knowledge about potential threats. In addition to training, you can enable solutions that reduce the ability of an employee to be compromised - even if they click a link they shouldn't – by removing admin rights and implementing application controls.

**To Learn More:** **5 Critical Steps in Your Endpoint Security Strategy**

# 7 Understaffed IT Service Desks

## The IT Service Desk is understaffed and under-resourced




of service desk teams note having a help desk system increases their productivity[13]


the average time to provide a first response to an internal support ticket[14]

*Sources: 13. HubSpot, 2020*
*14. The ZenDesk Benchmark Report*

When it comes to budget and team expansion, **IT Service Desks are often one of the more underfunded departments.** But as other teams inevitably grow, so does the influx of service desk tickets. More recently, due to the pandemic, the large shift to remote working has also driven an increased demand for remote access and support. These combined factors result in IT teams being stretched, overworked and unable to provide efficient resolutions.

It's not just employees demanding attention, third-party vendors requiring network access also puts pressure on IT teams. Boarding and managing vendor access can be manual and inefficient, and vendor security practices may be lower than yours; 58% of organizations believe it is likely they have suffered a breach due to vendor access.

**Demands driven by the pandemic and massive shift to remote working have increased the pressures on IT teams — and they are here to stay.**

Enabling IT teams with the right tools for remote access and support are critical to driving productivity without compromising security. A comprehensive Secure Remote Access solution enables efficient remote support to resolve technical issues on any device or system, as well as granular remote access for users and vendors that is simple to control, manage, and audit — no VPN required.

Additionally, implementing an Endpoint Privilege Management solution not only removes security risks, but it empowers Service Desk teams to maintain manageable workloads by reducing tickets. End users can gain access to known applications via scalable whitelisting, and applications are verified by using simple command prompts.

**To Learn More:** **The Top 5 Remote Access Problems**

# Protect Your Organizations From These Perils With Privileged Access Management

**When it comes to security, human nature has its limits.** The constant pressures at work mean that training and knowledge can only get you so far. However, you can close the security gaps that result from the 7 Deadly Sins with Privileged Access Management (PAM).

PAM consists of cybersecurity strategies and technologies for exerting control over privileged access and permissions for users, accounts, processes, and systems across an IT environment.  By controlling accounts and credentials across your ecosystem, enabling secure remote access for workers and vendors, and eliminating excessive privileges, Privileged Access Management (PAM) significantly reduces your attack surface while providing the flexibility your end users need.

An effective PAM strategy will help you disrupt multiple points in the attack chain. Unlike traditional PAM approaches, BeyondTrust's unique Universal Privilege Management model allows you to start with the use cases that are most urgent to your organization, and then seamlessly address more requirements over time.

The BeyondTrust PAM portfolio is an integrated solution that simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

> **Breadth of functionality and strength of deployment and scalability approaches makes [BeyondTrust] a good fit for global enterprises.**
>
> *— Gartner Critical Capabilities for Privileged Access Management, by Felix Gaehtgens, etc., 16 July 2021*

### Privileged Password Management

Discover, manage, audit, & monitor privileged accounts

### Endpoint Privilege Management

Manage privileges on Windows, Mac, Linux, & Unix endpoints

### Secure Remote Access

Centrally manage & secure remote access for service desks & vendors

Learn more: beyondtrust.com/solutions

BeyondTrust

# About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com

V2021_07_ENG