Symantec
A Division of Broadcom

Privileged Access Management—The Foundation for Combatting and Preventing Targeted Data Breaches

Welcome to the Jungle

Despite the numerous, headline-making incidents in recent years, cybercrime continues to rise with reported data breaches increasing by 75 percent over the past two years[1]. For those that suffer a breach, the repercussions can be costly: increased public scrutiny; costly fines; decreased customer loyalty; and reduced revenues. It is no wonder that cybercrime has risen toward the top of the concern list for many organizations-and the customers with whom they do business.

You've heard many of the stories. Equifax, Uber, Facebook, MyHeritage, Under Armor, and Marriott. Personal data from millions of their customers was stolen. Even though the number of breaches went down in the first half of 2018, the number of records stolen increased by 133 percent to almost 4.5 billion records stolen worldwide[2]. Unfortunately things are only likely to get worse. According to a 2018 study from Juniper Research[3], an estimated 33 billion records will be stolen in 2023—this represents a 275 percent increase from the 12 billion records that are estimated to be stolen in 2018.

Are you ready for more bad news? Thanks to the demands of the application economy, the threat landscape has expanded and protecting against these threats has only gotten more challenging.

THE REALITY IS, CYBERCRIME IS A GROWTH INDUSTRY

$6 TRILLION

Is the estimated global cybercrime damages by 2021[4]

700 MILLION

People in 21 countries were victims of cybercrime in the past year[4]

1. Information Age, September 2018 [https://www.information-age.com/data-breach-reports-increase-last-two-years-123474521/]
2. Business Wire, October 2018 [https://www.businesswire.com/news/home/20181008005322/en/Data-Breaches-Compromised-4.5-Billion-Records-2018]
3. Juniper Research Report 2018 [https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html]
4. Comparitech, October 2018 [https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/]

Victims of the Future

Digital transformation is a necessity for organizations to not only survive, but thrive in the application economy. But these transformations are creating an expanding set of new attack surfaces that must be defended, in addition to the existing infrastructure that you've been protecting for years. These new points of vulnerability include:

DEVOPS ADOPTION: In more sophisticated IT shops, continuous delivery/continuous testing practices have introduced automated processes that see no human intervention at all. In many cases, these scripts or tools are often using hard-coded administrative credentials that are ripe for theft and misuse.

HYBRID ENVIRONMENTS: As your IT environment has evolved to include software-defined data centers and networks, and expanded outside of your four walls to incorporate public cloud resources and software-as-a-service (SaaS) applications, the traditional way of approaching administration and management quickly falls apart—mainly because it fails to protect new attack surfaces like management consoles and APIs.

INTERNET OF THINGS: Smart devices are proliferating our lives, from phones to watches, from refrigerators and cars to medical implants and industrial machinery. And because these devices have connectivity, not only can they be hacked, but they are already being compromised where security is inadequate or non-existent.

THIRD PARTY ACCESS: Outsourcing development or IT operations has become the norm. In addition, many companies are sharing information with partners. However, many of these third-party employees are being granted "concentrated power" via administrative access. Who is watching how they are using or potentially misusing that access?

When you add up these vulnerabilities, it becomes clear how much havoc an attacker could wreak in your environment if he or she were able to gain the appropriate access.

Take Hold of the Flame

Stealing and exploiting privileged accounts is a critical success factor for types of attacks. This is not surprising when one considers that privileged identities have access to the most sensitive resources and data in your environment; they literally hold the keys to the kingdom.

Thankfully, there is a positive angle you can take on this fact. If privileged accounts are the common thread amongst the innumerable attack types and vulnerability points, then these accounts—and the credentials associated with them—are exactly where you should focus your protection efforts.

For many, focusing on "privileged users" is difficult because its population can be so diverse. Privileged accounts and access are not just granted to employees with direct, hands-on responsibility for system administration but also to contractors and business partners. You may even have privileged unknowns who are securing "shadow IT" resources without your knowledge. And finally, in many cases, privileged accounts aren't even people—they may be applications or configuration files empowered by hard-coded administrative credentials.

This begs the question, if you can't even get a clear tally of who represents your privileged user population, how can you hope to protect these accounts? By securing those accounts at each stop along the breach kill chain.

THE RISK OF PRIVILEGED ACCOUNTS AND CREDENTIALS

74%

of data breaches start with privileged credential abuse[1].

"The truth is that all men having power ought to be mistrusted"

— James Madison

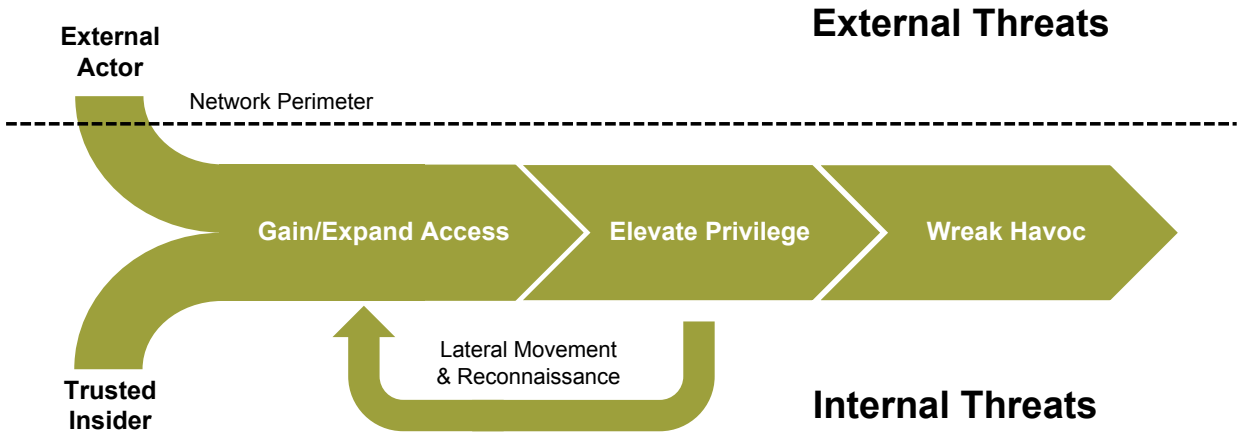
[1] Forbes, 2019

Breaking the Chains

What is a kill chain?

It's the series of steps an attacker typically follows when carrying out a breach.

While the chain can comprise numerous steps, there are four key ones in which privileged credentials represent the cornerstone of an attack. These include:



GAIN ACCESS AND EXPAND

To access the network, insiders might exploit the credentials they already have, while outsiders will exploit a vulnerability in the system to steal the necessary credentials.

ELEVATE PRIVILEGES

Once inside, attackers will often try to elevate their privileges, so they can issue commands and gain access to whatever resources they're after.

INVESTIGATE AND MOVE LATERALLY

Attackers rarely land in the exact spot where the data they're seeking is located, so they'll investigate and move around in the network to get closer to their ultimate goal

WREAK HAVOC

Once they have the credentials they need and have found exactly what they're looking for, the attackers are free to wreak havoc (e.g., theft, business disruption, etc.).

Explore what you can do during each step to manage your privileged identities and secure your business.

Two Out of Three Ain't Bad

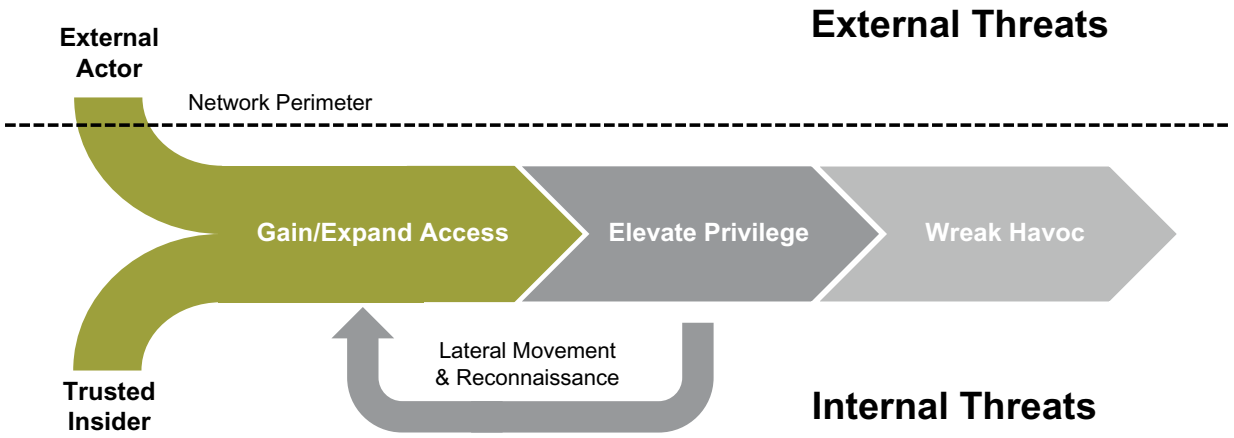
PREVENTING UNAUTHORIZED ACCESS

If you can prevent an unauthorized user—insider or outsider—from gaining access to the system in the first place, you can stop an attack before it even starts.

To prevent unauthorized access, you must:

- **Store** all privileged credentials in an encrypted vault and rotate these credentials on periodic basis
- **Authenticate** all users, applications, and services before granting access to any privileged credential

STEP 1



- **Employ** automatic login and single sign-on so users never know the privileged credential

BENEFITS INCLUDE

- **Protects** and manages privileged credentials
- **Ensures** users are whom they claim to be via strong authentication
- **Links** actual users to privileged access and activities

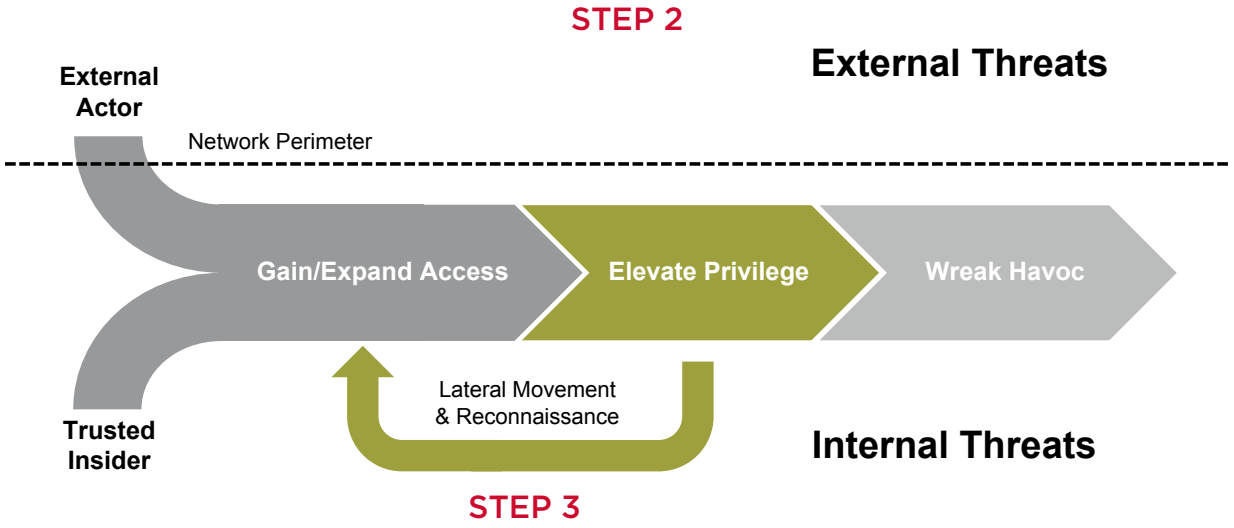
Keeper of the Seven Keys

LIMITING PRIVILEGE ESCALATION

In many networks, it's common for users to have access to more resources than they actually—which means attackers can cause maximum damage quickly and even benign users can cause problems inadvertently. This is why granular access controls are so important.

To limit privilege escalation, you must:

- **Leverage** RBAC and native identity stores to define privileged user access rights
- **Adopt** a "zero trust" policy that only grants access to the systems people need for work



- **Implement** filters and white/black lists to enable fine-grained access controls
- **Proactively** shut down attempts to move laterally between unauthorized systems

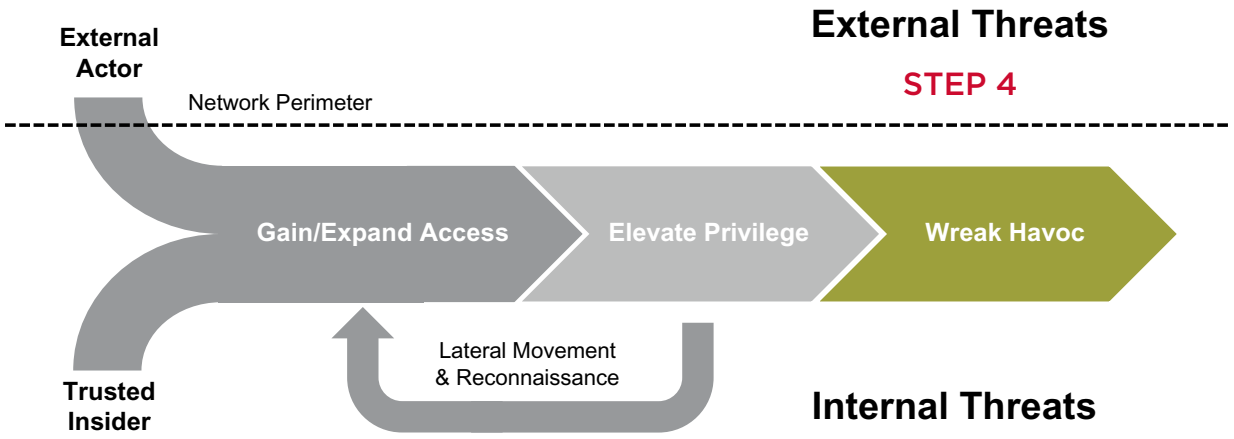
BENEFITS INCLUDE

- **Controls risk** through a least privileged posture
- **Simplifies** privileged user management processes

More than a Feeling

MONITORING PRIVILEGED ACTIVITY

Whether it's a trusted insider who wandered into the wrong area or an attacker with malicious intent, there's a very good chance that at some point users will gain access they shouldn't have. The challenge, then, is to improve visibility and forensics around user activity within sensitive systems.



To deter violations at this late stage of the kill chain, you must:

- **Ensure** that all privileged access and activity is attributed to a specific user
- **Monitor** all privileged activity to proactively detect unusual behavior and trigger automatic mitigations
- **Record** all user sessions so that all privileged activities can be played back in DVR-like fashion
- **Review** and certify privileged access on periodic basis to ensure that it is still required

BENEFITS INCLUDE

- **Forensic evidence** of accidental or malicious actions
- **Reduced risks** through analytics and automated mitigations
- **Improved compliance** and privileged identity governance

About the Symantec Solution

Symantec Privileged Access Management is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity across virtual, cloud and physical environments. The solution provides a privileged credential vault, session recording, threat analytics, host-based access control for mission-critical servers, and application to application password management to address non-human actors, such as applications, configuration files, and scripts.

KEY BENEFITS

- Control privileged access across all IT resources, from cloud to mainframe
- Apply unified cross-platform protection and management of privileged credentials
- Automatically discover and protect virtual and cloud-based resources
- Provide tamperproof audit data and forensic evidence for all privileged user activity
- Segregate duties of superusers with fine-grained control and secure task delegation
- Eliminate hard-coded passwords from apps, scripts, files and support DevOps toolchains

INCLUDED CAPABILITIES

- Privileged credential vault with zero-trust access model
- Threat analytics with machine learning and automated mitigations
- Host-based access control to protect mission-critical servers and containers
- Application to Application Password Management with flexible options
- Audit data and forensic evidence to support compliance and investigations

Are You Doing Enough to Protect Your Business During Cybercrime's Current Boom?

Symantec Privileged Access Management can help you answer that question with a

confident **yes.**

LEARN HOW AT BROADCOM.COM/SYMANTEC-PAM

Symantec™
A Division of Broadcom

For product information please visit our website at: Broadcom.com

BC-0534EN-0120 January 13, 2020