CYBER SECURITY THAT'S

GOOD FOR PEOPLE & GOOD FOR BUSINESS

The Anatomy of a Privileged Account Hack – how to start your least privileged journey

Scott Shields

thycotic

Protecting privileged accounts has the greatest impact of any cyber security strategy

PRIVILEGED ACCOUNTS

What is a privileged account?

- **Non-human or user accounts** used by IT staff or applications which often have unfettered access to critical data and systems i.e. Domain Admin, root.
- **Exist everywhere** in nearly every connected device, server, hypervisor, OS, DB, or application: on-premises & cloud.
- Represent one of the **most vulnerable aspects** of an organization's IT infrastructure.

HACKER TECHNIQUES

It is critically important to know how cyber criminals target their victims, what you can do to reduce the risk and make it more challenging for the attackers who steal your information, your identity or your money.

thycotic

CYBER SECURITY RISK ACTORS

Script Kiddies	Organized Crime	Insider Threats	Nation States	Terror Groups
				
Curiosity	Financial	Retaliation / Financial	Economic Adv & Intelligence	Destructive

thycotic

32%

OF HACKERS SAY

accessing privileged accounts was the number one choice for the easiest and fastest way to get at sensitive data

ENTER THE MIND OF A HACKER?

thycotic

SELECTING THE TARGET

STEP 1

RECONNAISSANCE

90% OF TIME

HACKERS TARGET
PERSONAL IDENTIFIABLE INFORMATION (PII)

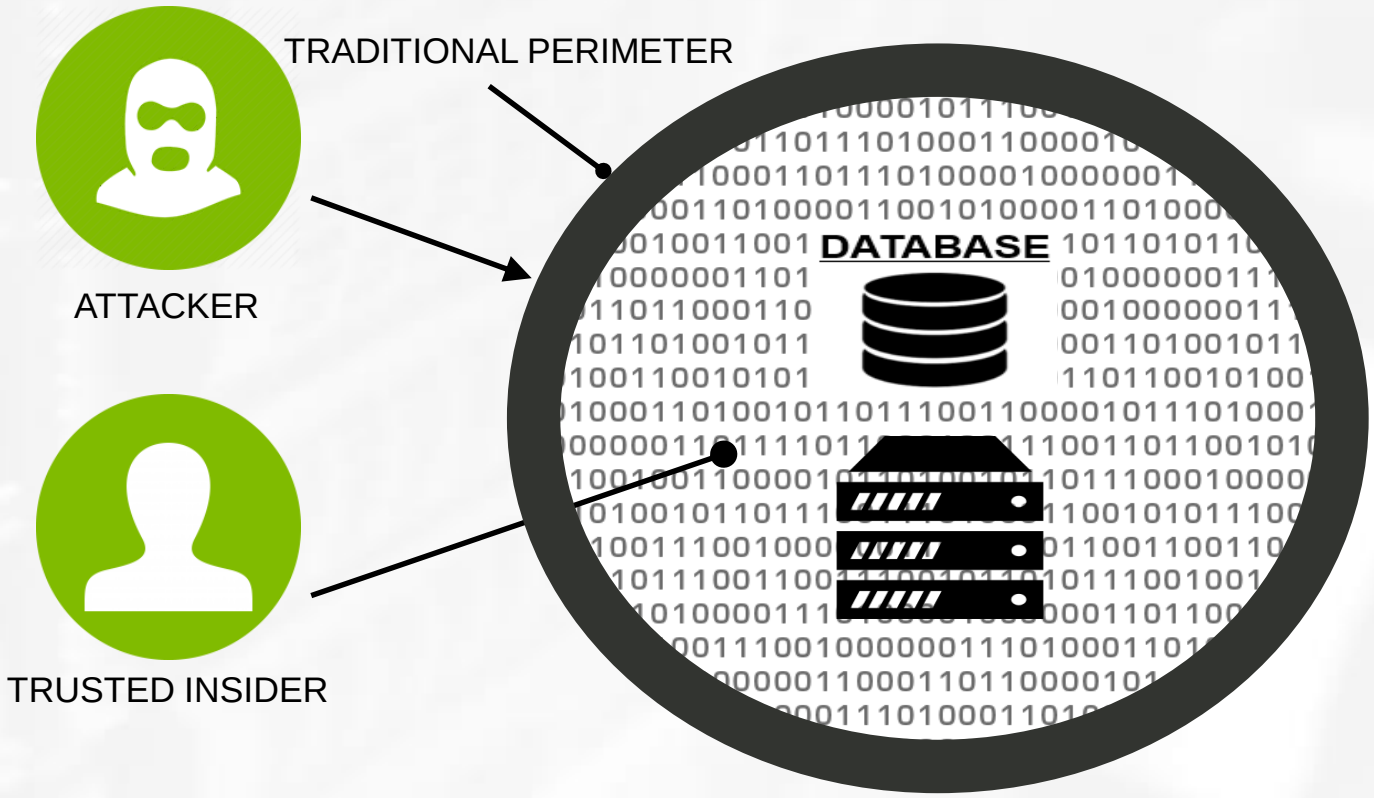
- Full name (if not common)
- Home address
- Email address
- National identification number
- Passport number
- IP address or Mac Address
- Vehicle registration plate number
- Biometric Information
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Telephone number
- Login name, screen name, nicknames

thycotic

TRADITIONAL PERIMETER

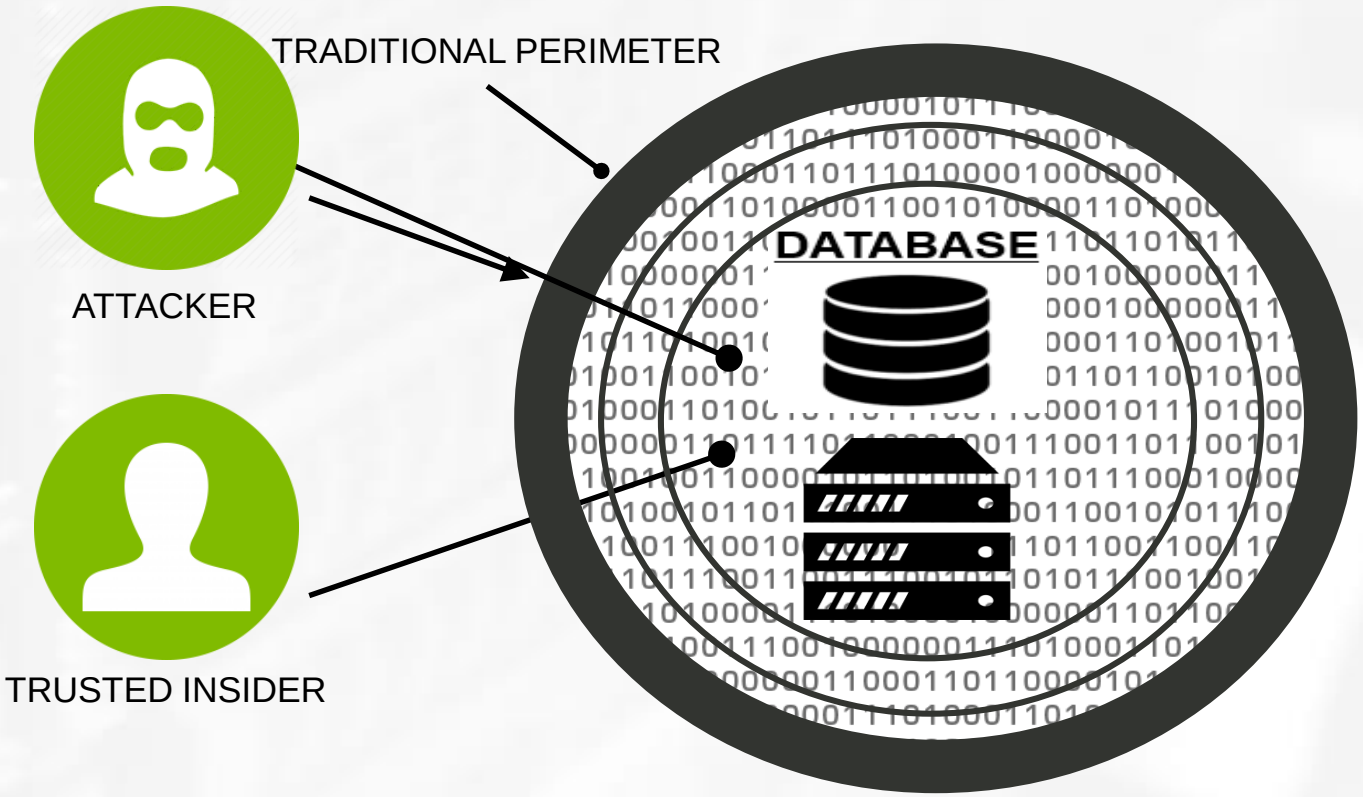
Build a fence around the data. This approach has fundamental flaws

- You can't be 100% sure the fence is working
- Cloud and Mobile computing blurs the perimeter
- Over 60% of fraud breaches are conducted by stolen credentials



ADD LAYERS AND LAYERS?

1. Perimeter control
2. Trusted Insiders
3. Data in Secure vaults
4. Firewalls and Network
5. IDS and IPS
6. SIEM



Gartner Ranks PAM CISO's #1 Security Priority

On Gartner's List of Top 6 Security Projects

THYCOTIC ADRESSES 4

- #1 – Privilege Account Management
- #3 – Anti-phishing
- #4 – Application Control
- #6 – Detection & Response

thycotic

Why can Privileged Accounts be difficult to secure?

Unknown:

- Don’t know where service accounts are used (dependent services)
- Multiple accounts used to run services, tasks, applications on multiple servers, possibly in multiple data centers

Unmanaged:

- Never rotating passwords = manual, tedious process
- Password changes require downtime = need to be done off hours

Unprotected:

- No access control
- No auditing

Secret Server

Privileged Accounts

Domain Administrators
Windows Local Administrators
Domain Service Accounts

RedHat
Debian
Fedora

MSSQL
Oracle
MySQL

AS400 / OS390
z/OS (RACF)
SSH

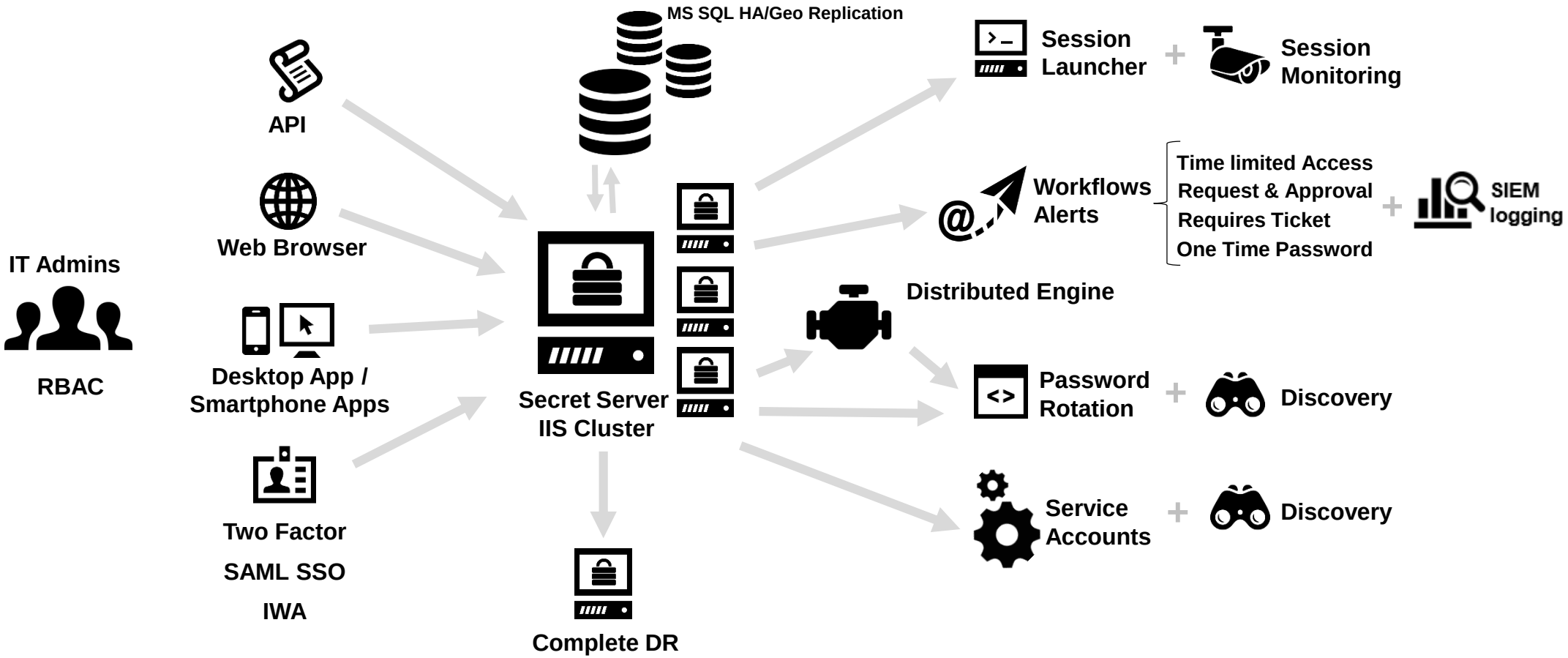
Cisco / Juniper
Checkpoint / Palo Alto
Blue Coat / SonicWall

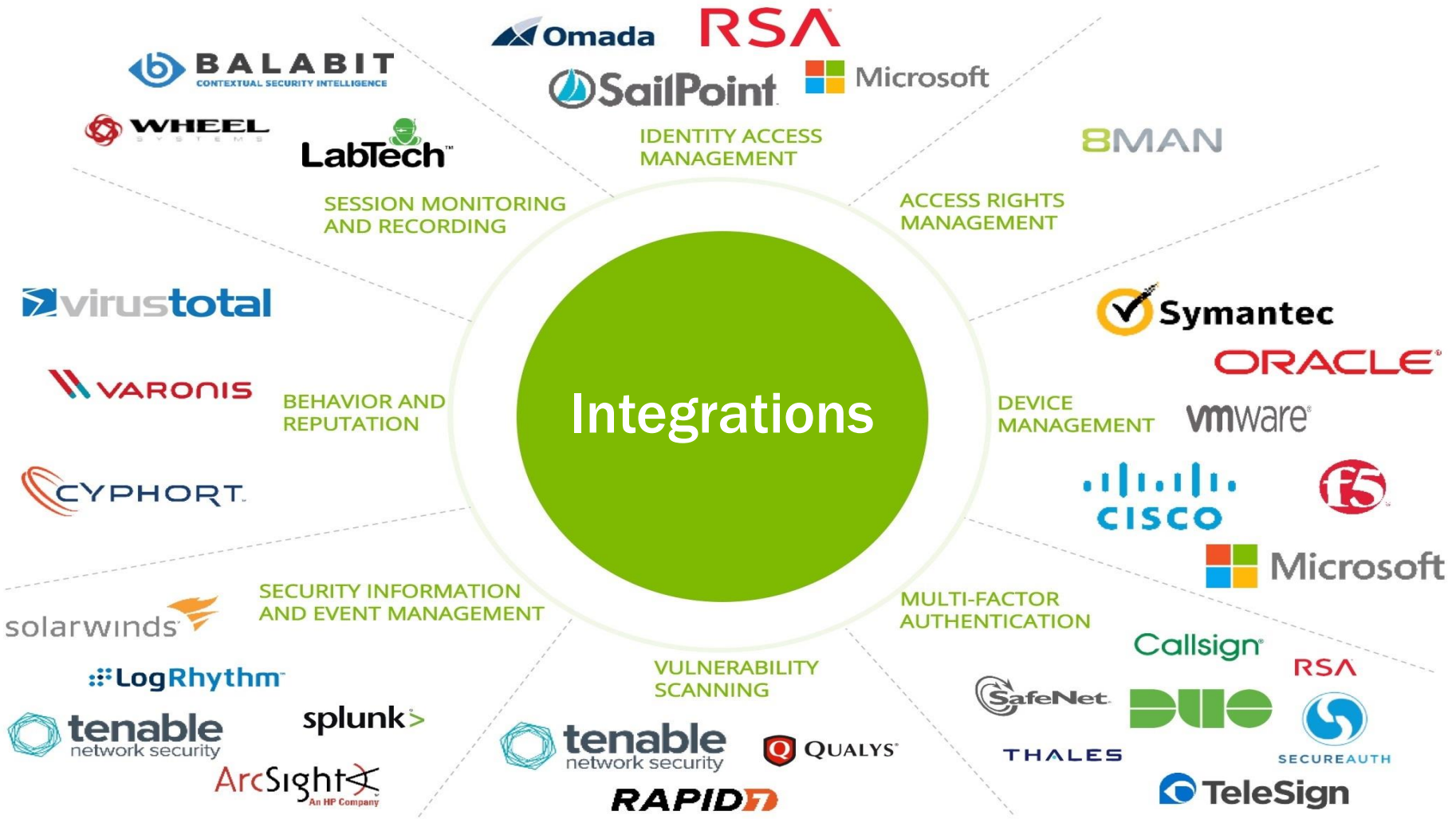
Google / Office365 / Salesforce
SAP / Social Media
AWS / Azure

VMware ESX/ESXi
Dell DRAC / HP iLO
SSH/Telnet Compatible

Config Files
Scripts
DevOps

Secret Server




Integrations
IDENTITY ACCESS MANAGEMENT
Omada
RSA
BALABIT
CONTEXTUAL SECURITY INTELLIGENCE
SailPoint
Microsoft
WHEEL SYSTEMS
LabTech
SESSION MONITORING AND RECORDING
ACCESS RIGHTS MANAGEMENT
8MAN
virustotal
Symantec
ORACLE
VARONIS
BEHAVIOR AND REPUTATION
DEVICE MANAGEMENT
vmware
CYPHORT
CISCO
F5
Microsoft
SECURITY INFORMATION AND EVENT MANAGEMENT
solarwinds
LogRhythm
tenable network security
splunk>
ArcSight An HP Company
VULNERABILITY SCANNING
tenable network security
QUALYS
RAPID7
MULTI-FACTOR AUTHENTICATION
Callsign
RSA
SafeNet
DUO
SECUREAUTH
THALES
TeleSign

PAM IS MORE

THAN JUST A PASSWORD VAULT

thycotic

Why Privileged Accounts Are an Attractive Target

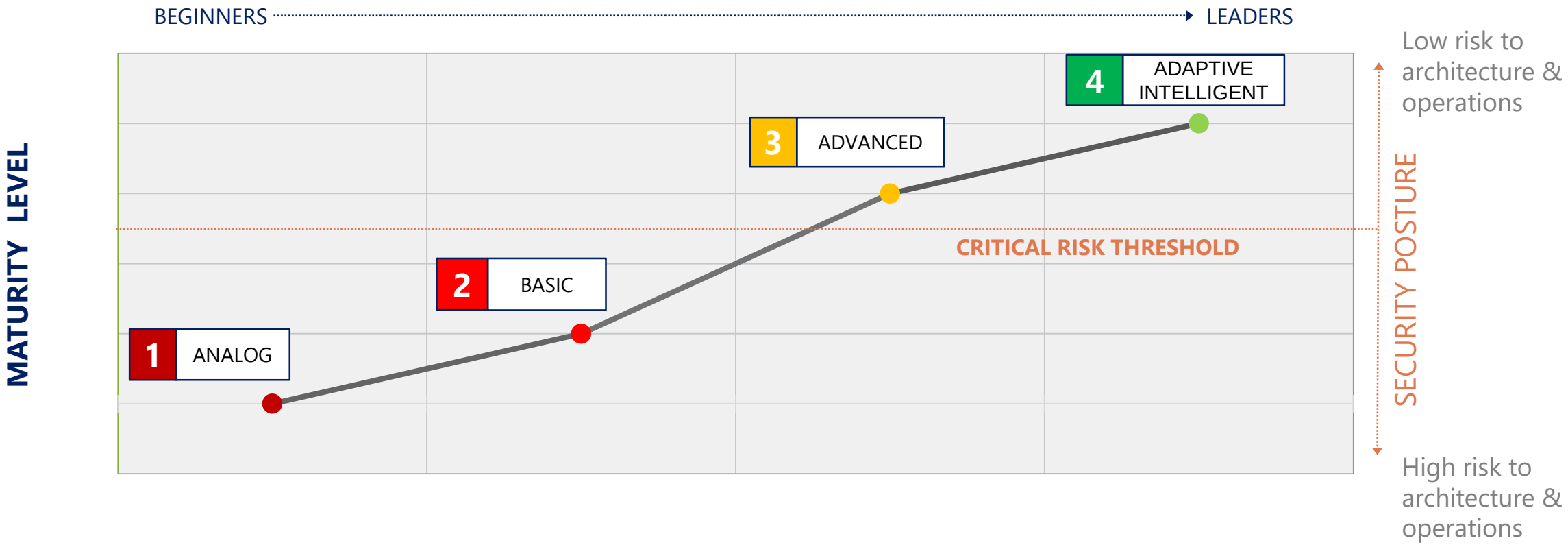
- Privileged accounts exist everywhere and used by IT personnel to access servers, OS, routers, apps, DB….
- *Privileged accounts are often unknown, unmanaged, & unprotected*
- Attackers target privileged accounts to gain access & cause harm
- 200+ days is average time breaches go undetected

83% of cyber breaches involve privilege accounts

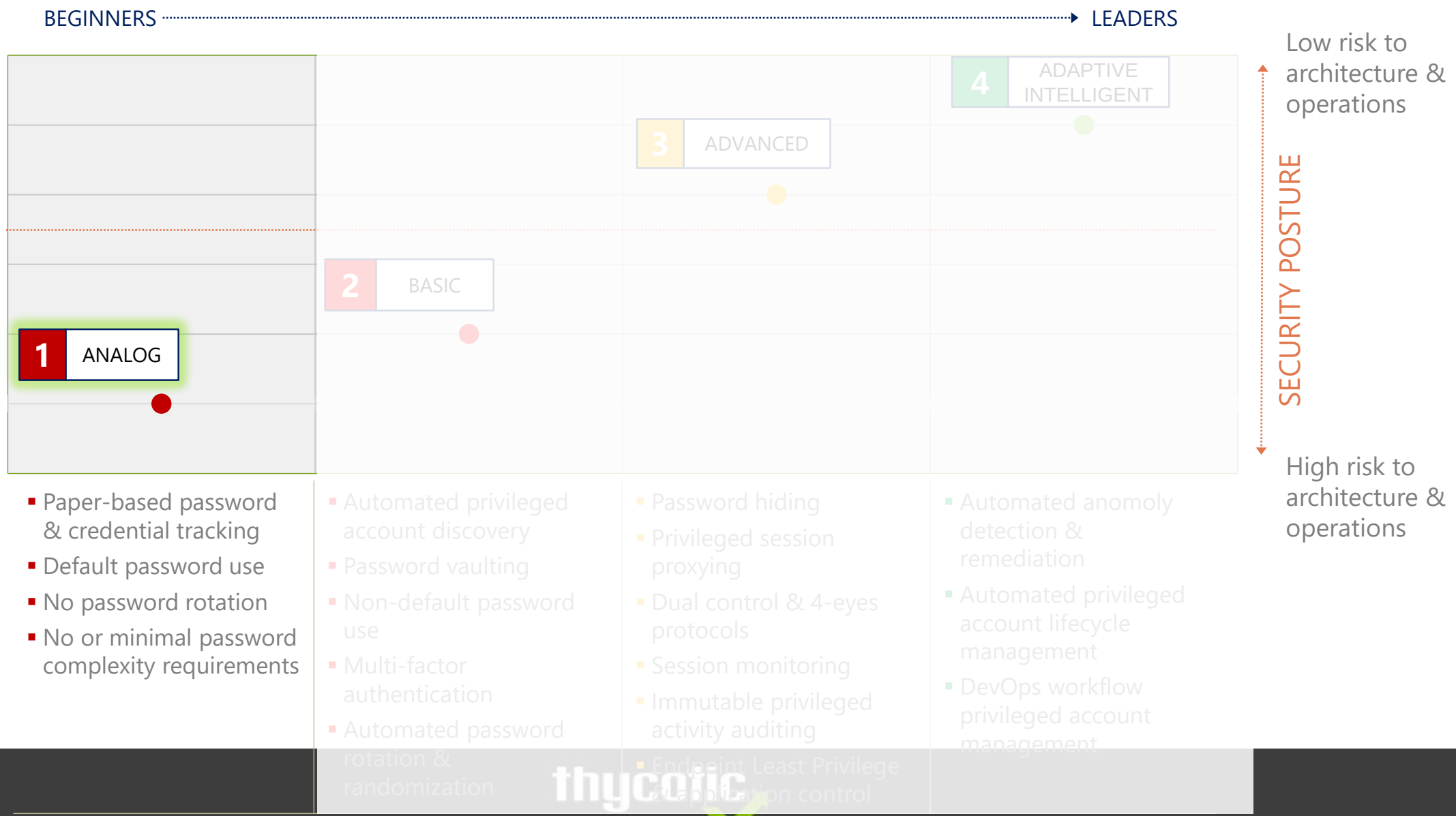
- Verizon 2018 Report

thycotic

thycotic PAM Maturity Model



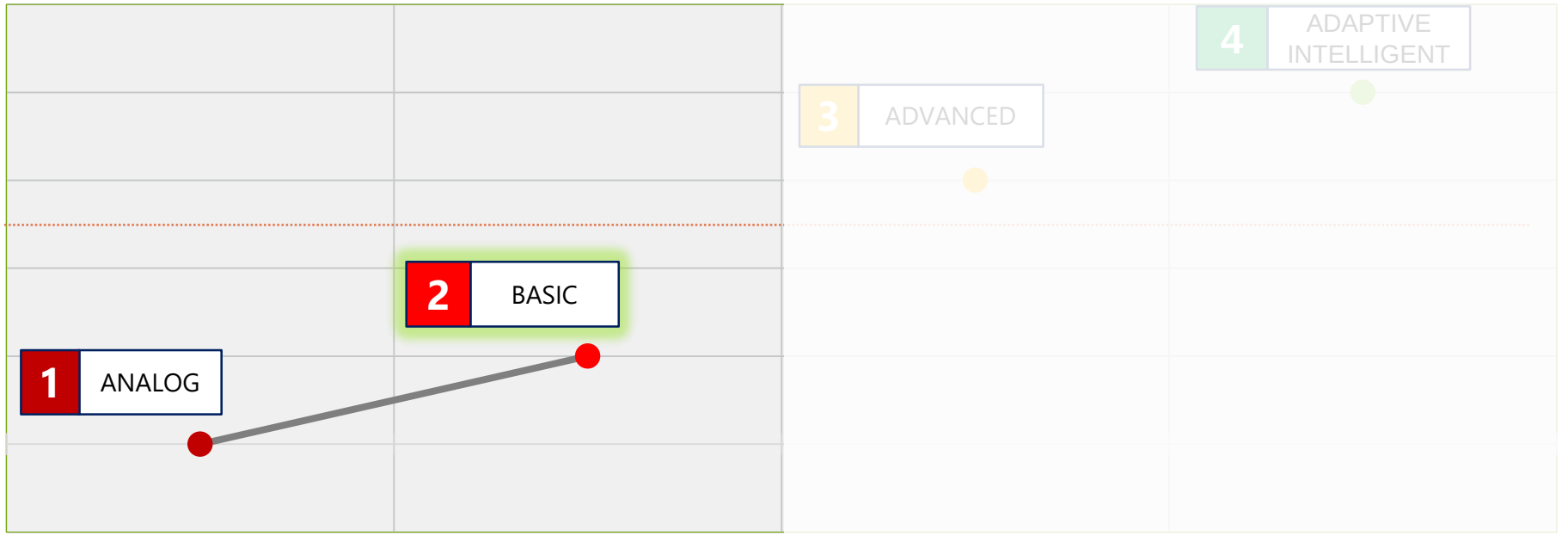
thycotic PAM Maturity Model



thycotic PAM Maturity Model

BEGINNERS → LEADERS

MATURITY LEVEL



SECURITY POSTURE

Low risk to architecture & operations

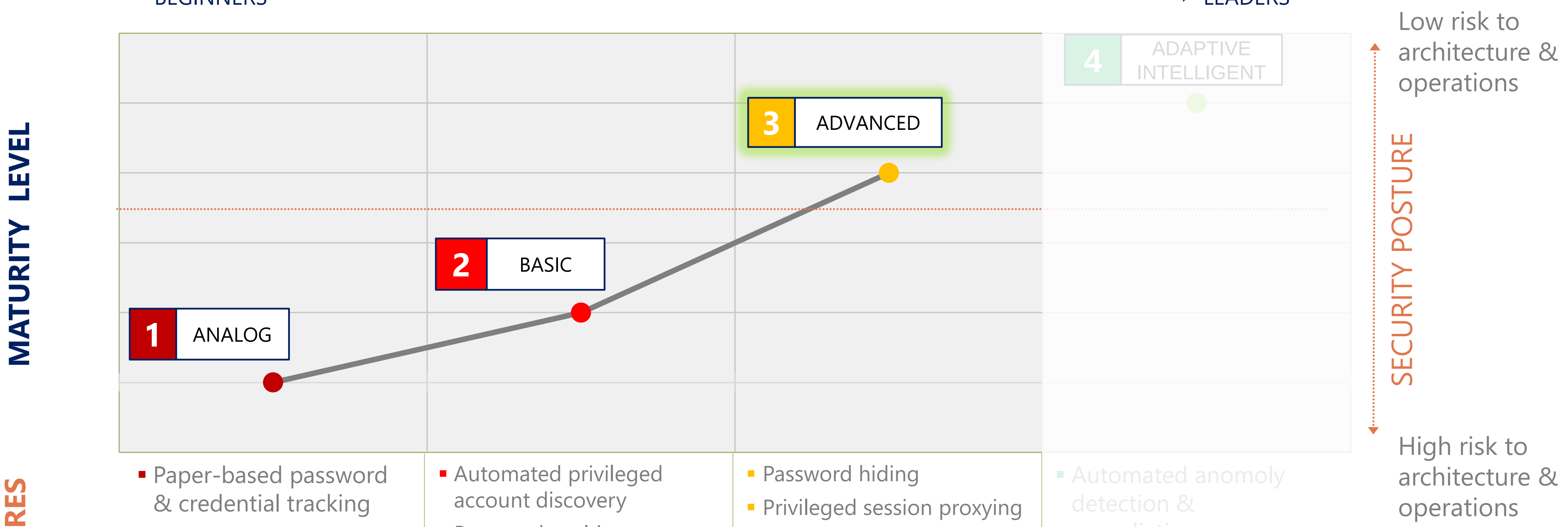
High risk to architecture & operations

FEATURES

1 ANALOG	2 BASIC	3 ADVANCED	4 ADAPTIVE INTELLIGENT
▪ Paper-based password & credential tracking ▪ Default password use ▪ No password rotation ▪ No or minimal password complexity requirements	▪ Automated privileged account discovery ▪ Password vaulting ▪ Non-default password use ▪ Multi-factor authentication ▪ Automated password rotation & randomization	▪ Password hiding ▪ Privileged session proxying ▪ Dual control & 4-eyes protocols ▪ Session monitoring ▪ Immutable privileged activity auditing ▪ Endpoint Least Privilege [illegible] control	▪ Automated anomoly detection & remediation ▪ Automated privileged account lifecycle management ▪ DevOps workflow privileged account management

thycotic PAM Maturity Model

BEGINNERS → LEADERS



FEATURES

1 ANALOG
- Paper-based password & credential tracking
- Default password use
- No password rotation
- No or minimal password complexity requirements

2 BASIC
- Automated privileged account discovery
- Password vaulting
- Non-default password use
- Multi-factor authentication
- Automated password rotation & randomization

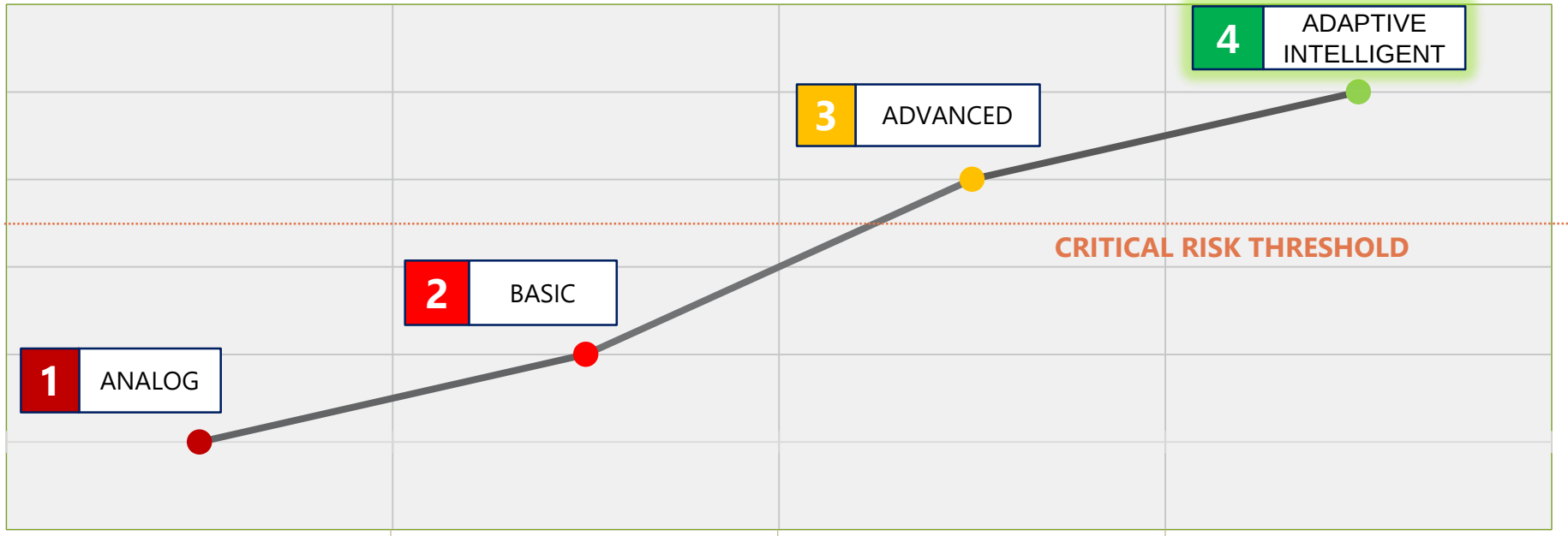
3 ADVANCED
- Password hiding
- Privileged session proxying
- Dual control & 4-eyes protocols
- Session monitoring
- Immutable privileged activity auditing
- Endpoint Least Privilege & application control

4 ADAPTIVE INTELLIGENT
- Automated anomoly detection & remediation
- Automated privileged account lifecycle management
- DevOps workflow privileged account management

thycotic PAM Maturity Model

BEGINNERS ····· LEADERS

MATURITY LEVEL



Low risk to architecture & operations

SECURITY POSTURE

High risk to architecture & operations

FEATURES

- Paper-based password & credential tracking
- Default password use
- No password rotation
- No or minimal password complexity requirements

- Automated privileged account discovery
- Password vaulting
- Non-default password use
- Multi-factor authentication
- Automated password rotation & randomization

- Password hiding
- Privileged session proxying
- Dual control & 4-eyes protocols
- Session monitoring
- Immutable privileged activity auditing
- Endpoint Least Privilege & application control

- Automated anomoly detection & remediation
- Automated privileged account lifecycle management
- DevOps workflow privileged account management

There’s a faster, easier way to privilege security

LET US SHOW YOU HOW IT WORKS

thycotic

Secret Server

The only fully-featured PAM solution both on-premises and in the cloud

Cloud Benefits

Always available

Geo-redundancy, continuous backups, auto-scaling

Highly secure

SOC 2 audits, AES-256 encryption, built-in intrusion/malware/DDoS protection

No hardware or software to buy or maintain

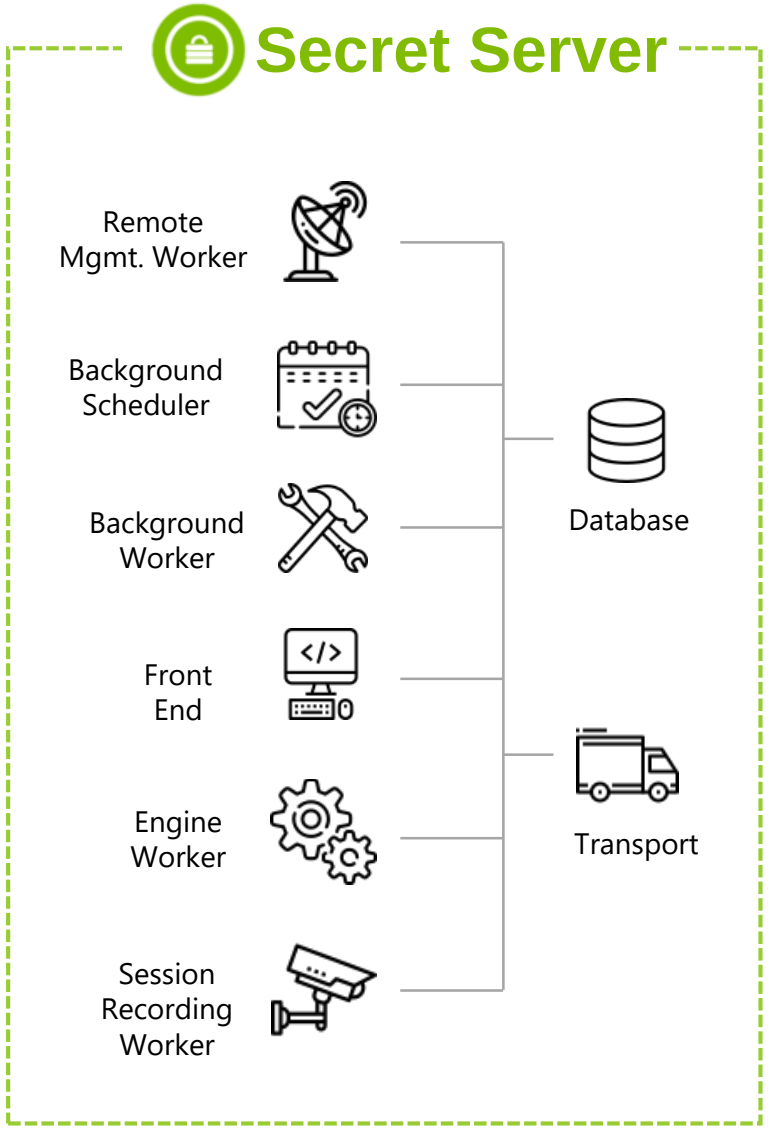
Self-updating and maintenance-free; no need to manage and maintain infrastructure

Hit the ground running

Easy to set up, rapid time to value; get results right away after logging into our browser-based console for the first time

Pay as you go

Total control over licensing costs via flexible, subscription-based price model



Ultimate goal

No more local administrators

Lightweight, clientside service -> Granular Policies ->

Elevate *applications*, instead of users

THE THREAT: Local Privileged Accounts

Local admin accounts on endpoints can be used to access other computers, domain resources, and critical servers unless a least privilege security model is implemented

They **exist everywhere** because it's easier to give standard domain user accounts more rights than they actually need, resulting in humans with privileged access.

The issue is rarely addressed on **employee computers**, leaving companies vulnerable to privileged account escalation and pass-the-hash attacks

According to Microsoft

- ***96% of critical vulnerabilities affecting Windows operating systems could be mitigated by removing admin rights***
- ***60% of all Microsoft vulnerabilities could be mitigated by removing admin rights***

THE Microsoft Solution: UAC

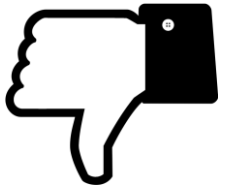
Microsoft recommend that no users should log in to endpoints with local admin rights. Instead they should be issued with two sets of credentials:

- **Standard User**
- **Local Admin**

Users should log in with their standard user account and will receive a UAC prompt whenever admin privileges are required.

OR

Remove admin accounts from end users and keep support teams with administrative accounts



Limitations of UAC

- **2 sets of credentials to remember**
- **Users just log in with the admin account or create a new account/s**
- **Limited application support**
- **If leaving support team with Admin accounts this puts HUGE workload on them**

Meet Privilege Manager

Privilege Manager empowers organizations to successfully remove admin rights without impacting user productivity

How?

Elevate (add admin rights) to specific applications *(Never the User!)*

Replace Windows UAC with flexible, customized messaging

Block known-bad applications outright

Whitelist known-good applications and prevent unknown applications from executing

And much more…

Privilege Manager

Implement and enforce least privilege policies for Windows and Mac

MANAGE ACCOUNTS

DEPLOY AGENTS

DEFINE POLICIES

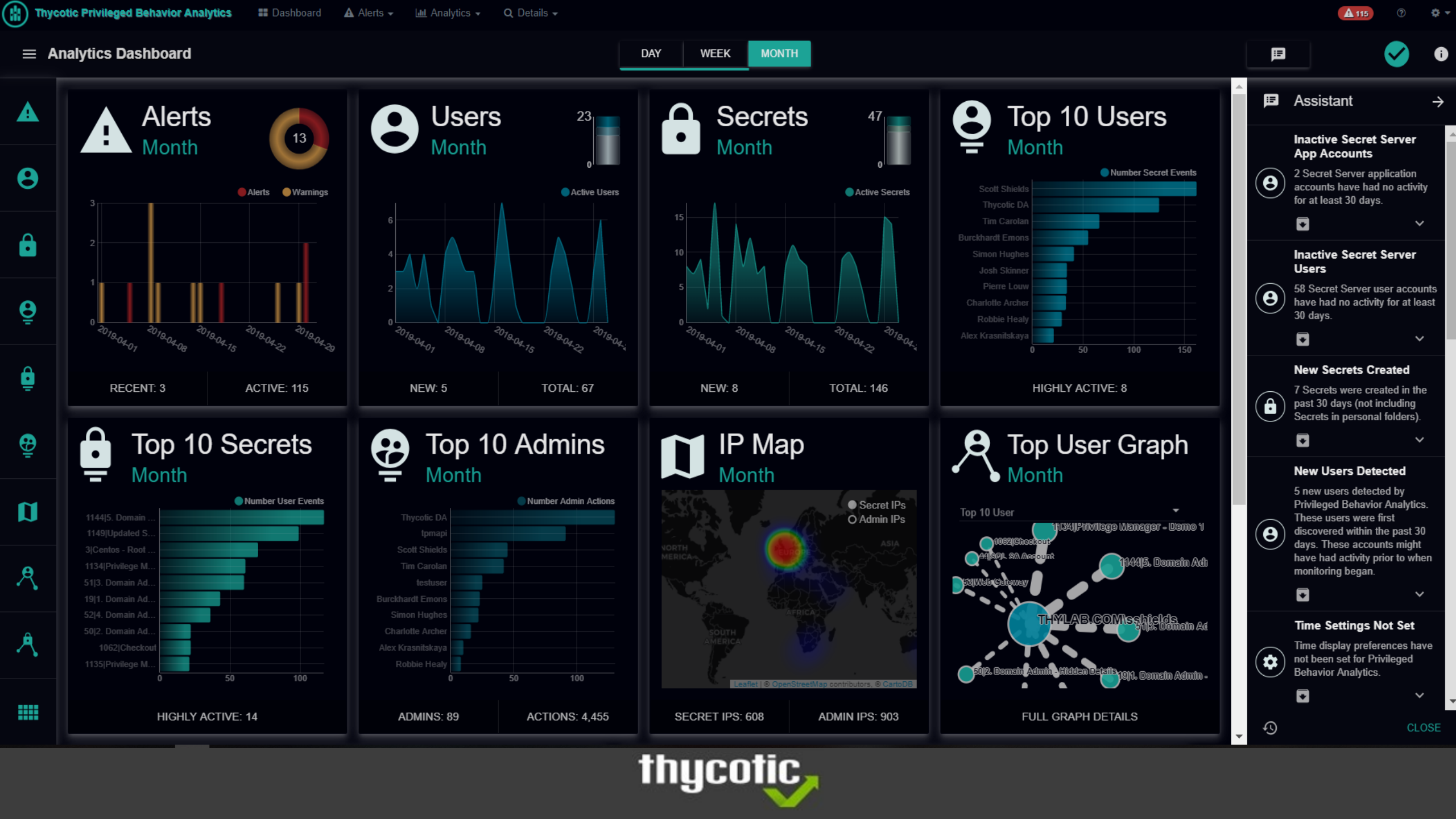
ELEVATE APPLICATIONS

IMPROVE PRODUCTIVITY

Privilege Behaviour Analytics (PBA)

Innovative **machine learning technology** automatically identifies and alerts for suspicious Privileged Account access and activity based on individual behaviour baselines

thycotic


Thycotic Privileged Behavior Analytics
Dashboard
Alerts
Analytics
Details
115
Analytics Dashboard
DAY
WEEK
MONTH
Alerts
Month
13
Alerts
Warnings
2019-04-01
2019-04-08
2019-04-15
2019-04-22
2019-04-29
RECENT: 3
ACTIVE: 115
Users
Month
23
0
Active Users
NEW: 5
TOTAL: 67
Secrets
Month
47
Active Secrets
NEW: 8
TOTAL: 146
Top 10 Users
Month
Number Secret Events
Scott Shields
Thycotic DA
Tim Carolan
Burckhardt Emons
Simon Hughes
Josh Skinner
Pierre Louw
Charlotte Archer
Robbie Healy
Alex Krasnitskaya
HIGHLY ACTIVE: 8
Top 10 Secrets
Month
Number User Events
1144|5. Domain ...
1149|Updated S...
3|Centos - Root ...
1134|Privilege M...
51|3. Domain Ad...
19|1. Domain Ad...
52|4. Domain Ad...
50|2. Domain Ad...
1062|Checkout
1135|Privilege M...
HIGHLY ACTIVE: 14
Top 10 Admins
Month
Number Admin Actions
Thycotic DA
tpmapi
Scott Shields
Tim Carolan
testuser
Burckhardt Emons
Simon Hughes
Charlotte Archer
Alex Krasnitskaya
Robbie Healy
ADMINS: 89
ACTIONS: 4,455
IP Map
Month
Secret IPs
Admin IPs
Leaflet | © OpenStreetMap contributors, © CartoDB
SECRET IPS: 608
ADMIN IPS: 903
Top User Graph
Month
Top 10 User
1062|Checkout
1144|5. Domain Adı
THYLAB.COM\sshields
50|2. Domain Admin - Hidden Details
19|1. Domain Admin -
FULL GRAPH DETAILS
Assistant
Inactive Secret Server App Accounts
2 Secret Server application accounts have had no activity for at least 30 days.
Inactive Secret Server Users
58 Secret Server user accounts have had no activity for at least 30 days.
New Secrets Created
7 Secrets were created in the past 30 days (not including Secrets in personal folders).
New Users Detected
5 new users detected by Privileged Behavior Analytics. These users were first discovered within the past 30 days. These accounts might have had activity prior to when monitoring began.
Time Settings Not Set
Time display preferences have not been set for Privileged Behavior Analytics.
CLOSE
thycotic

Privileged Behavior Analytics

Integrate enhanced reporting, threat detection, and incident response

thycotic

PRIVILEGED ACCOUNT MANAGEMENT
SECRET SERVER

ENDPOINT APPLICATION CONTROL
PRIVILEGE MANAGER

ANALYTICS
PRIVILEGED BEHAVIOUR ANALYTICS

thycotic

WE EMPOWER SECURITY CHAMPIONS

FINANCIAL SERVICES

BankUnited

WELLS FARGO

TECHNOLOGY

IBM

Adobe

SAAB

SAP

ENERGY

Chevron

bp

HEALTHCARE

Biogen

KAISER PERMANENTE

BlueCross BlueShield

EDUCATION

JOHNS HOPKINS UNIVERSITY

OHIO STATE

University of San Diego

PUBLIC SECTOR

SEAL OF THE STATE OF INDIANA 1816

MINNESOTA

UNITED STATES SENATE

SERVICES

Deloitte.

pwc

CBRE

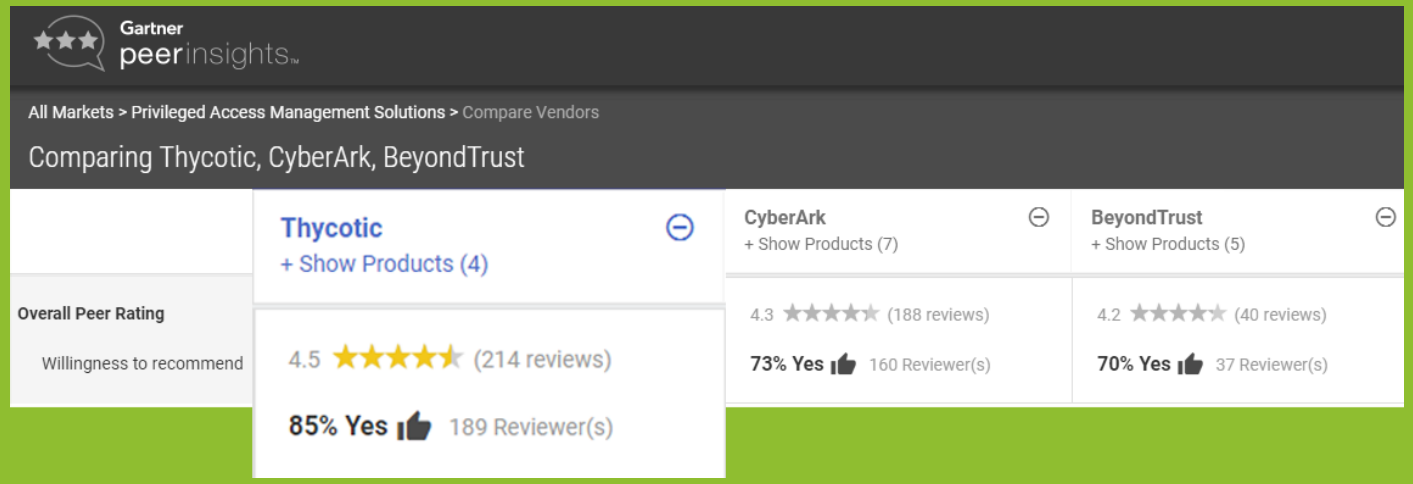
ENTERTAINMENT

Hard Rock

zynga

thycotic

RATED #1 in GARTNER PEER REVIEWS



Performance & Ease of Use

We are very pleased with Secret Server performance and ease of use, especially compared to the CyberArk product it will replace."

CISO, FINANCE INDUSTRY

Requires Less, Covers More

Thycotic is 100% better than CyberArk at a fraction of the cost. And requires a smaller footprint and covers more compliance requirements."

IT SPECIALIST, SERVICE INDUSTRY

Adoption Skyrockets

Adoption has been organic without a need to strongly push the tool. It's intuitive, requiring very little training to get our teams up and running."

INFOSEC MANAGER, SERVICE INDUSTRY

thycotic

FREE TOOLS

No cost. No kidding. FREE forever!

FREE Security Policies Template for Privileged Passwords

DOWNLOAD NOW

FEATURED

FREE Vulnerability Benchmark for Privileged Passwords

DOWNLOAD NOW

FEATURED

FREE Discovery Tool for Windows

DOWNLOAD NOW

thycotic

Free Trials

FEATURED TRIAL:

SECRET SERVER

Secret Server enables you to store, distribute, change, and audit enterprise passwords in a secure environment

START MY FREE TRIAL

Free Resources

THANK YOU