

Demonstrated Use Cases with IBM Security Privileged Access Management

Malik Merchant

Privileged Access Management SME and Technical Pre-Sales Leader,
IBM North America

Patrik Horemans

IAM Subject Matter Expert, IBM Europe

Hisham Kamal

Worldwide Sales Leader, Privileged Access Management

3.5%

The % of employees that worked from home prior to Covid-19 (105M Workers)

50+

Unique malware distributed in various COVID-19-themed campaigns

4700%

COVID-19 related spam and malware activities

24 Months

The expected timeframe some form of social distancing expects to remain in place

IBM X-Force Research

XF-IRIS internal data analysis.

Across the IT environment, protecting privileged credentials is mission critical

80%

of security breaches
involve a weak or stolen
privileged credential

85%

of cyber attacks enter
through a compromised
endpoint

Sources:

Forrester : Privileged Access Management Forrester Wave 2018

SANS Institute : Exploits at the Endpoint: SANS 2016 Threat Landscape Survey

Keep your remote workforce secure with IBM Security Privileged Access Management

A central vault ensures.

Automated password
creation and rotation

Session management
controls

Least privilege policies

IBM Security Privileged Access Management can help you quickly enable and secure a remote workforce

IBM Security Secret Server

Discover, manage, protect and audit privileged accounts across your organization.



IBM Security Privilege Manager

Enforce least privilege security and control application rights on endpoints.



PAM from IBM Security can help you quickly enable a remote workforce by securing privileged credentials and endpoints

- Installation in minutes means greater time to value – fast to deploy, easy to use and scalable
- Integrate IBM Secret Server with IBM Cloud Identity for strong multi-factor authentication
- Full-solution in the cloud, on-premise or as a managed service



Largest enterprise cybersecurity provider

Leader in 12 security market segments

8,000+ security employees

70B+ security events monitored per day

Available Resources

IBM Marketplace Pages

- [Control & Protect your organization with Privileged Access Management](#)
- [IBM Security Secret Server](#)
- [IBM Security Privilege Manager](#)

Free Tools

- [Free 30-Day Trial](#)
- [Privileged Account Discovery for Windows Tool](#)
- [Endpoint Application & Least Privilege Discovery Tools](#)

Privileged Access Management as a Service

- [IBM Security Services – PAM as a Service](#)

Planning and Deployment Expertise

- [Get your PAM Program on the Road to Success](#)

Other

- [Whitepaper](#)
- [PAM for Dummies](#)
- [Least Privilege Cybersecurity for Dummies](#)
- [Blog](#)

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.