Stay ahead of the threat curve and protect your key assets

Privileged accounts have access to your key assets – your systems, applications and customer data. That makes them a prime target for cyber-attack so they need special attention. Our in-depth understanding of potential threats means we can assess the risks to your information systems. We'll help you evaluate your current position, develop a management strategy and choose the best solution to protect your most important assets. Working with us will reduce the uncertainty and complexity of security and transform your approach.

Although most enterprises have a defined process to manage privileged accounts, they still underestimate potential vulnerabilities linked to privileged accounts. Many have more privileged accounts than nominative accounts and some don't even know exactly how many existing privileged accounts they have. Given any misuse of a privileged account can severely affect your operations and potentially damage your reputation, it's not something you can ignore.

Common issues include sharing and rarely – or never – changing passwords, insecurely storing files on a network or on email and giving users access to too much sensitive information. Often, accounts set up temporarily are not deactivated and forgotten about, while activities and events on privileged accounts are difficult to audit.

Our dedicated identity and access management security consulting team provides both a functional and technical vendor-agnostic solution to protect your privileged accounts while helping you to meet compliance regulations.

We have successfully delivered complete migrations of customer identities into our managed services. Our managed service currently holds more than 40 million customer identities and handles approximately 2.5 million authentication and authorisation requests daily.

Our own identity and access management service holds approximately 180,000 identities which are used globally by our own employees and subcontractors every day again. More than 400 applications and 50+ SAML federations make use of our identity and access management service for the authentication and authorisation of our employees when using applications on our networks or cloud based applications like Salesforce.

Depending on your needs we can offer you complete end-to-end services for implementing a privileged account management solution, or short term engagements. With our global team of identity and access management specialists we are able to support you at any stage of your journey to a successful PAM program implementation or any other identity and access management challenge you might have.

Becoming a proactive security organisation

- **increase operational efficiency** – reduce the cost of manual support tasks and replace old generation tools with new ones
- **enforce information system security** – comply with regulatory constraints and control access to ICT resources
- **improve agility** – easily adapt to other ways of working like mobile, managed services or cloud.

Understanding the risks that come with privilege

Privileged accounts are IT system user accounts which allow users to make significant changes on your systems or applications which affect the integrity and availability of ICT resources. It's clear that special care is required to ensure these accounts are secured properly.

Every organisation uses privileged accounts to support their primary business processes on a daily basis. Examples include:

- **built-in administrative accounts**: these non-personal accounts often provide full access to workstations, servers, network devices, security devices, databases, mainframes, etc. and are typically used by IT staff to perform maintenance
- **emergency accounts**: these provide unprivileged users with administrative access to secure systems in the case of an emergency
- **application accounts**: these are used by applications to access databases, run batch jobs or scripts, or provide access to other applications
- **privileged user accounts**: these are credentials that give administrative privileges on one or more systems, devices and applications. This is typically one of the most common forms of privileged account access granted on an enterprise network. Cloud administrative accounts (like Amazon Web Services and Microsoft Azure) are given particular attention
- **service accounts**: these are used by an application or service to interact with the operating system
- **social accounts**: these are used by the organisation to communicate with the public.

When it comes to understanding the risk to your organisation it is important to determine your current risk profile by asking:

- where are your privileged accounts?
- who owns these privileged accounts?
- who uses these accounts, when, and to do what?
- what is the justification for these accounts?
- is there a security policy defined for these specific accounts?
- is this security policy applied?

Why choose BT?

Put your security consultancy need into expert hands

We are one of the world's leading and most trusted security brands, derived from a set of credentials that have been earned over decades of experience in the field. Our dedicated identity and access management security consulting team will lead and advise on privileged account management or other identity and access management concerns.

Our global Security Consulting capability consists of 500 highly skilled security consultants with a solid expertise in every security domain. Our consultants hold industry certifications like QSA, PCIP, CISSP, CISA, CISM, CGEIT, CRISC, CSSA, CCEP, CCEP-I, CIPP, CIPT and ITIL as well as specialised certifications from security product vendors.

- our consultants are vetted to different security levels and can be assigned according to your specific needs
- we are accredited for performing consulting services on a global scale by Lloyd's Register Quality Assurance for the ISO9001 quality management system
- holding the ISO9001 certification since 2003 shows our long term commitment to continuously improve the quality of our consulting services
- with more than 2,500 security consultants and professionals globally we are one of the largest security and business continuity practices in the world
- we work with 20 partners and over 200 security vendors, as well as joint R&D with a select group of major vendors and innovators.

We operate globally with local presence in more than 180 countries and manage or monitor over 40,000 security devices globally. This global reach also covers 14 global Security Operations Centres (SOCs), 45 datacentres and +250 customer specific operations. All data centres and SOCs are ISO 27001 certified.

What could IAM consulting services do for you?

Visit bt.com/globalservices

Offices worldwide.

Issued: July 2018