CASE STUDY

Energy company implements zero trust strategies with Imprivata Privileged Access Management

imprivata®

Organization snapshot

LOCATION	SIZE	INDUSTRY
Europe, Middle East, Africa	$50M - $250M USD	Energy and utilities

CHALLENGES

- Meet compliance and risk management requirements
- Drive operational efficiencies
- Improve remote access

RESULTS

- Achieved zero trust access
- Greater business agility
- Strengthened supplier relationships

SOLUTION

- Imprivata Privileged Access Management

> **“Imprivata provides high-performance privileged access management both for the inside and the external administrators. It is easy to use, easy to deploy, and enables zero trust.”**
>
> Gartner Peer Insights

Utility, oil and gas, and other critical infrastructure companies are prime targets for cyberattacks. Companies must modernize security practices, secure operational technology, and implement zero trust access policies. Imprivata Privileged Access Management is a comprehensive, easy-to-use solution that improves security and helps companies deliver secure remote access to critical systems and data while meeting audit requirements.

The challenge

Utility and energy industries have embraced digital transformation and modernized infrastructure with a growing number of Internet of Things (IoT) devices. These systems are connected using sensors, big data, and analytics. Remote workers, partners, and contractors must connect to these systems to perform daily maintenance, repairs, and other functions. While this helps drive efficiencies, it creates new security risks.

Companies must manage access for privileged users, machines, IT systems, and cloud software. This includes managing passwords and access to everything from administrative, domain, network, local, Active Directory, cloud, emergency, Internet of Things, and service-to-application accounts.

As cyber threats increase, companies must rethink their privileged access strategies to prevent unauthorized access to systems. If malicious actors gain access, they can move undetected through IT and OT systems and change configurations, control equipment, and potentially harm workers or entire communities they serve.

Solution

To improve their security posture and mitigate risks associated with remote access, one local energy company in EMEA implemented Imprivata Privileged Access Management after carefully evaluating privileged access management (PAM) providers.

When asked why they selected Imprivata, the CXO said the top three factors were overall product functionality and performance, company vision/roadmap and cost. Imprivata Privileged Access Management delivers a robust feature set with high value and lower total cost of ownership due to its modern architecture and cloud delivery model.

The Imprivata solution was implemented on-premises to store and manage privileged credentials and create a secure remote gateway. It securely locks the company's OT and IT systems behind their firewall forcing remote workers, partners, and contractors to use the gateway to access critical assets. Access is then verified, managed, and monitored through privileged credentials.

Imprivata Privileged Access Management is used with secure Active Directory logins, multifactor authentication (MFA), and approval and time-based workflows to safely provide access to only trusted personnel and devices. This allows the company to limit access by account or system, implement just-in-time access, and enforce zero trust policies that 'never trust, always verify' any person or device connecting to their network before granting access.

The solution also integrates with the company's ServiceNow incident tracking system and is used as a convenient way to schedule work orders for IT administrators and to track their progress.

Results

Moving to Imprivata Privileged Access Management and a zero trust policy has improved the company's cybersecurity posture and enabled them to secure endpoints to reduce their risk surface.

The company can now streamline the management and monitoring of all types of privileged accounts, including IoT devices. Remote workers and approved partners have the right level of access to applications and systems. Authorized partners can securely access systems to perform maintenance or other job functions. This improves partner and customer relationships while providing a full audit trail.

To help satisfy compliance regulations and security audits, Imprivata Privileged Access Management isolates, monitors, records, and audits privileged access sessions, commands, and actions. It securely stores and indexes each account access with keystroke logs, session, and other privileged event recordings. This ensures the company can meet stringent compliance regulations.

*Case study details taken from **Gartner Peer Insights** imprivata®

Imprivata, the digital identity company for enterprise, provides identity, authentication, and access management solutions that are purpose-built to solve hyper-complex workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com