A Frost & Sullivan White Paper

An Inescapable Reality: Utilities Need Advanced Identity Governance to Modernize, Evolve

In partnership with

SailPoint

Powering clients to a future shaped by growth

FROST & SULLIVAN

Today's utility industry has seen more changes over the past two decades than in the entire century that preceded it. The industry is being shaped by decarbonization, decentralization, and digitization. Rooftop solar panels, wind power, and on-site power storage are examples of the decarbonization and decentralization trends, whereas digitization is the critical, though often laborious, utilization of vast amounts of customer and operations data.

Utilities have had to evolve from rigid, monolithic, and relatively homogenous entities to flexible and diverse organizations. The old hub-and-spoke model that dominated for over a century, in which one regional power company maintained generation, transmission, and billing of power to homes and businesses, has become a matrix of varying power sources and changing usage patterns. Utility business models have also changed over time, with some purchasing, rather than generating, power; some competing for electricity market share in deregulated markets; and some major investor-owned utilities (IOUs) owning related but distinct entities in both regulated and unregulated markets. All these different facets to the industry have meant that utility business processes and their workforce have had to adapt, which can be a challenge in a historically slow-moving industry. New roles, departments, and even subsidiaries have been created within utility organizations in response to these trends, further complicating the utility business. This growth in external and internal complexity, in a highly regulated industry, has also come at a time of rising cybercrime. Managing people and the data they can interact with becomes critical to operating effectively, efficiently, and securely.

UTILITY INDUSTRY TRANSFORMING FROM ALL SIDES

Utilities manage vast amounts of information. In terms of customers, this includes personally identifiable information (PII) such as banking and credit card details; contact details such as emails, phone numbers, and addresses; personal and business identification numbers; and energy usage patterns, which can indicate when people are home or when businesses are at their busiest. In terms of operational data, utilities are swimming in information — from generation and transmission to internal business processes — all of which are critical in ensuring safe and consistent operations.

The type and volume of information utilities gather has grown tremendously in recent years as a result of the industry's evolution. For example, the number of internet of things (IoT) devices used in the energy industry is expected to increase from 1.1 billion in 2020 to over 2.1 billion by 2025.[1] The information streaming in from these devices, coupled with sophisticated analytics, can reduce equipment failures, allow quicker responses to outages, and enable different revenue models such as time-of-use rates or rooftop solar power integration. This has also meant that customer and operations data is being accessed by a growing number of roles, departments, value chain partners and even devices. To ensure data security, regulatory compliance, and operational excellence, it is increasingly critical to know who has access, to what data, and how they use it.

Utilities have always had a focus on safety and security for their employees and customers. This has expanded from physical security to include a growing focus on cybersecurity. As utilities manage infrastructure fundamental to economic health and national security, they can often be targets of threat actors. The vast amounts of personal information utilities house are also targets for stealing identities, login credentials, and financial information.

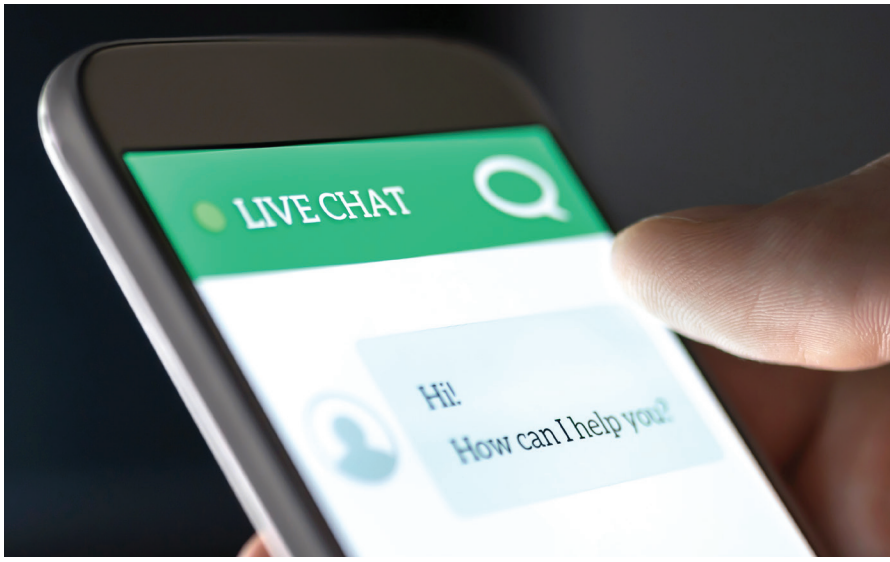
> **“Utilities have always had a focus on safety and security for their employees and customers. This has expanded from physical security to include a growing focus on cybersecurity.**

Strong security standards are a business imperative as well as a regulatory requirement in the utility industry. As the threat of cyberattacks in our increasingly connected world continues to rise, utilities find themselves subject to numerous mandates such as NERC's critical infrastructure protection (CIP) standards and requirements, which, among other things, require frequent checks on a utility's cybersecurity vulnerabilities. Along with the NERC CIP, utilities need to comply with customer data requirements such as federal protections, the California Consumer Privacy Act (CCPA), and the Payment Card Industry Data Security Standard (PCI DSS). Utilities also need to heed the same data security and compliance standards of other businesses in terms of financial auditing and being accountable to shareholders and insurers. Whether driven by mandates, or enacted through smart business management, knowing who has (or should have) secure data access is non-negotiable. This requires ensuring access to that information is managed in a manner that is logical and dependable. A technologically advanced, automated identity governance system can give a utility visibility and consistency in user identification and authentication for data access across the complex organization.

1 Source: Frost & Sullivan IoT data

UTILITY EXPANSION COMPLICATES SECURITY PROCESSES

In addition to a complex regulatory environment and high volumes of data, many large IOUs grew through acquisition and still struggle to have good visibility and consistent practices across operational and customer data, business processes, and departments. Unless a utility has implemented an advanced and automated identity governance system—and many utilities still conduct these tasks manually—the merging and growing of organizations can lead to individuals with similar roles in different departments having inconsistent levels of data access and permissions. There may also be discrepancies as individuals change roles within the business. In these large organizations, it can be difficult to avoid the "entitlement creep" that can occur when an employee changes roles and gains new access and authority, but does not have permissions from the previous role revoked. This can lead to conflicts of interest, such as separation of duty, which can violate regulatory compliance. It can also obfuscate the visibility that management, auditors, and sometimes regulators need on who has access to PII and other sensitive information. Even if some permissions are removed, unstructured data such as third-party file-sharing may fall below the radar on manual identity security processes, though this can be rectified with more sophisticated, automated solutions.



Manual identity security also makes on-boarding and off-boarding more time-consuming and inaccurate, especially if the authorizing manager is not well acquainted with the employee's role or department. Many IOUs have thousands of employees, and trying to manage and govern all their access points manually is destined to lead to inconsistencies and potential security risks, as, across all industries, up to one in five security breaches involve misused privileges.[2]

While people are often top of mind for identity governance, some systems and bots, such as those used for customer service, require identity security as well. Utilities have always been at the forefront of interacting with their customers, as power quality and costs are important factors for any home or business. As utilities work to reduce customer wait times and improve experiences, they are turning to AI-informed systems such as online chatbots to help, for example, reporting an outage or understanding a bill. Hence, these chatbots and related systems need access to sensitive PII and business information, and therefore also need to have strong security and traceability. Advanced identity systems can manage this access effectively, offering 24/7 security, regardless of whether it is a human or automated system connecting with the information.

2 Source: Verizon, Verizon Data Breach Investigations Report

ADVANCED IDENTIFICATION AND AUTHENTICATION ON THE ROAD TO MODERNIZATION

All of these factors—changing organizational structures, massive amounts of data, difficulty modernizing and using information, stringent regulatory pressures—mean that utilities sometimes lack the visibility and management needed to ensure efficient and secure operations. Utility headcounts, short-term contract labor, and access to data by suppliers and vendors have all increased to accommodate how utilities are changing. Managing and governing information access by a growing number of players increase data security risk. Also, compared to many other industries, the utility industry has lagged in digitizing records and moving information to the cloud, in part because of regulatory restrictions, and in part due to the conservative nature of the industry.

However, automation and sophisticated analytics have evolved to create modern solutions that help bridge this gap for utilities, despite the fact that many utilities still rely on outdated, manual methods for identity management. For example, the time needed to bring an employee or contractor on board with manual systems can take hours or even days, whereas advanced automated systems can perform these functions, accurately and comprehensively, within minutes. Just as critical is cutting off access to former employees or contractors whose terms have expired, in a manner that is quick and complete. Manual systems can leave gaps both in time and access that can become a hazard to the organization.

Establishing a reliable and automated identification and authorization system is a foundational element to both strong security and organizational visibility. It can help create consistency across roles in different departments, centralize role management, and ensure role changes are accurately updated. Along with being slow, potentially inaccurate, and inconsistent, manual methods are costly. The time spent for IT teams to respond to help desk tickets, on-board and off-board individuals, and ensure consistency across the business hinders these high-cost professionals from engaging in more valuable activities. As part of the broader picture, identity governance is necessary to further a utility's progress toward its digital transformation. There is also the cost associated with manual process errors that can also lead to regulatory non-compliance and related fees and penalties.

An advanced identity and access management systems' ability to capture and manage unstructured data should also not be underestimated. This became an even greater concern during the COVID-19 work-from-home situation that led to increases in third-party communications and file-sharing, along with a troubling rise in cyber attacks. While line workers and plant operators are still needed in the field, large swaths of the utility workforce, such as finance, marketing, and customer service, have had to transition to WFH arrangements. As with most industries facing these circumstances, many utilities were ill-prepared to accommodate a shift to remote work from a process and equipment standpoint. This has highlighted the need for critical data to stay secure and compliant, which can be accomplished with intelligent user authentication solutions. Risk-averse utilities will want to seek market-tested options to ease implementation across roles and ensure regulatory compliance is comprehensive.

Automated identity management systems can increase organizational process efficiency and business governance across several facets within a utility, including:

- Continuity of access across similar roles and positions for the entire organization, regardless of department silo or region. This can even span regulated and non-regulated parts of a business, while still maintaining necessary operational data separation.
- On-boarding employees and contractors with the right access exponentially faster than with manual processes. This includes access that evolves as roles change over time, and can be quickly and comprehensively removed when an employee leaves the organization or a contract expires.
- The ability to find and manage unstructured data as well as structured data across systems and programs. These solutions can also help ensure access to secure, internal data-sharing systems is streamlined so that employees do not feel the need to use external systems.
- Full visibility of access across the organization, including all users, applications, data, and cloud platforms.

> **Risk-averse utilities will want to seek market-tested options to ease implementation across roles and ensure regulatory compliance is comprehensive.**

AN IDENTITY GOVERNANCE UPGRADE IMPROVES AN ALREADY TECH-SAVVY UTILITY

One utility that recognized, acted upon, and reaped the benefits of advanced identity management is the Sacramento Municipal Utility District (SMUD). SMUD, which services California's capital city and its surrounding areas, is one of the largest US community-owned electric utilities. Frost & Sullivan research also confirms that SMUD is one of the most innovative and advanced utilities with numerous forward-thinking programs on smart energy and renewable power.

SMUD recognized that, despite being among the more technologically progressive power companies, its identity governance program needed modernization. SMUD had to contend with a largely manual system that was time-consuming and costly for managing users and their access to structured and unstructured data. It lacked visibility across the organization on who had access to which systems and data, and the process of on- and off-boarding employees was cumbersome and sometimes inaccurate. SMUD also believed that its IT department should have more of its focus on its core competencies, such as its advanced programs on energy storage and distribution, to help it maintain its high levels of customer satisfaction.

SMUD realized it needed a partner to upgrade and chose SailPoint. With SailPoint, SMUD was able to automate processes, thereby improving accuracy, reducing IT department cycle times on tasks such as password management and access requests, and bringing greater visibility and consistency across the organization. Equally critical, the solution has helped ensure SMUD's regulatory compliance and mitigated risk associated with unstructured data, which was found to have greater potential for exposure than previous assessments had indicated.

ENABLING BETTER BUSINESS PROCESSES THROUGH IDENTITY GOVERNANCE

At the end of the day, utilities are about people. It is an industry that employs hundreds of thousands of workers and contractors and services millions of individuals and businesses. Although they are businesses, utilities are first and foremost focused on safely delivering reliable, consistent power. "Resilience" has been the goal for the utilities industry as it continues to face changing business models, an influx of data across its ecosystem, and ongoing regulatory pressures. These rapid changes have meant a traditionally staid and conservative industry has had to pivot to digital transformation to provide high levels of service and comply with regulations, which, in some cases, has been a struggle.

Other key capabilities that utilities should seek with advanced access governance solutions include:

- The ability for the solution to evolve with the business. As utilities need to add roles or even entire new departments or acquire new entities, the solution needs to be able to bring the same level of consistency and visibility across the organization.
- Machine learning (ML) and artificial intelligence (AI)-driven solutions can analyze high volumes of data and quickly ascertain if there are any irregularities that the IT team needs to investigate. This also saves the time and cost that expensive IT teams spend on more mundane tasks, enabling them to focus on higher-value activities.
- AI can learn about roles and data usage over time and make increasingly accurate, data-based suggestions on what access should be granted to whom.
- An advanced solution provides enhanced documentation, ensuring audit trails, compliance reports, and other regulatory needs are comprehensively and reliably met, making the process much quicker, smoother, and more accurate. Instead of teams working weeks to months on gathering, analyzing, and presenting information, traceable reports can be generated within minutes.

Utilities have to manage some of the broadest and most diverse types of data feeds of any industry. This includes institutional information such as managing and maintaining physical assets, business information, and PII customer data. Visibility is typically poor in the utility industry, due to legacy systems from acquisitions, siloed departments and entities, and the slow pace of migrating to digital records in the cloud. Furthermore, utilities need to balance data interconnectedness with appropriate authentication and identification. For example, a major outage, such as one brought on by a hurricane, may involve departments as diverse as finance, insurance, asset management up and down stream of affected areas, customer service, and communication to the public. A strong identification and authentication solution will seamlessly allow the right data to be shared as needed, without unduly exposing PII or institutional information.

NEXT STEPS

- **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
- Visit our **Digital Transformation** web page.
- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

San Antonio
7550 West Interstate 10
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

myfrost@frost.com 877.GoFrost http://www.frost.com

FROST & SULLIVAN

SAILPOINT: RETHINK IDENTITY

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive IdentityTM platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning(ML) technologies, the SailPoint Predictive IdentityTM platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on Twitter and LinkedIn and by subscribing to the SailPoint blog.