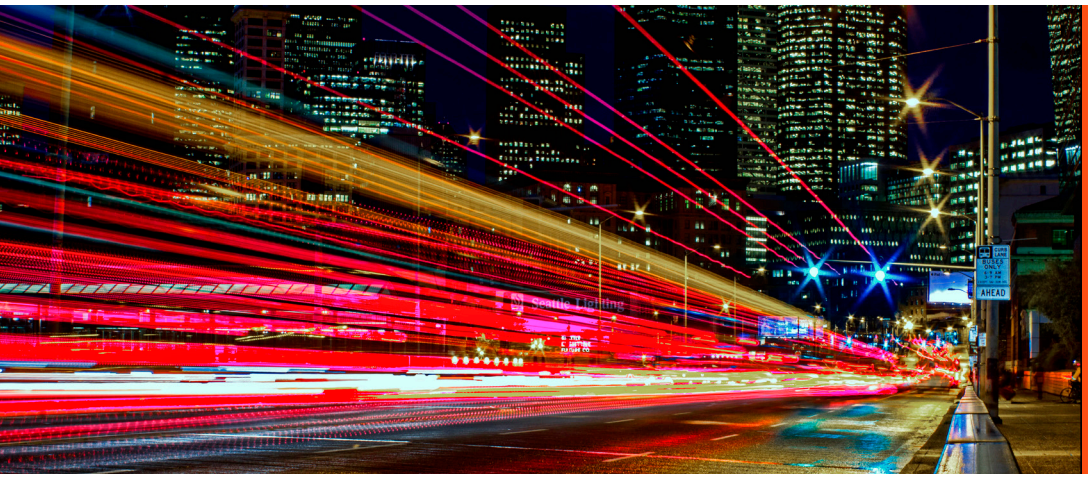
Quest



The average cost of a data breach is

$5.6 MILLION

for the energy sector.[1]

Migrate, manage and secure your public infrastructure environment

Quest software solutions can help you secure your records and systems, maintain compliance, and minimize service disruptions.

THE CHALLENGE

Cyberattacks have become a leading threat to the world's energy sector. It's not just hackers bent on stealing data or encrypting it for ransom anymore; public utilities providers now need to defend against the growing wave of destructive attacks aimed at service disruption or even total annihilation of their IT infrastructures. With these incidents constantly in the headlines, concerns about the vulnerability of the energy ecosystem are being discussed at the highest levels in countries around the globe, resulting in more stringent regulatory requirements and increased oversight of the industry.

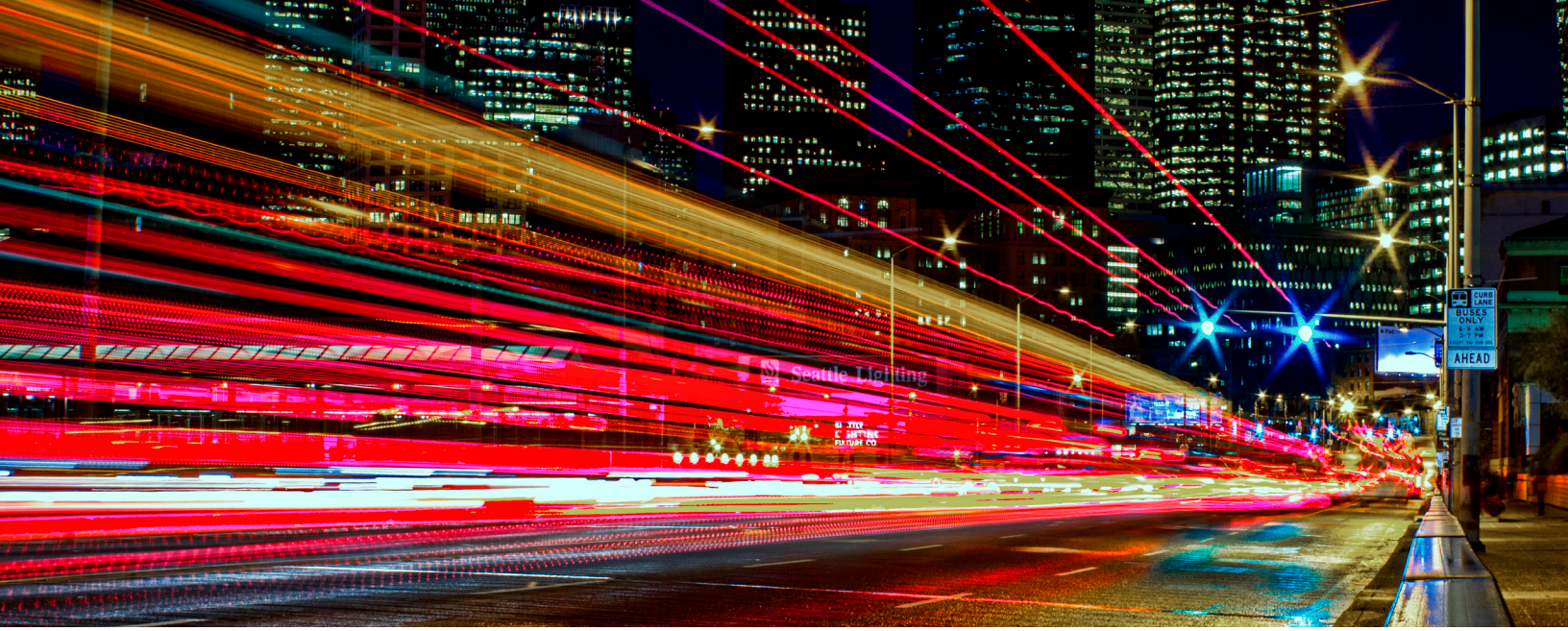
Meanwhile, other modern realities are adding to the burden on IT teams in the energy sector. Mergers and acquisitions are increasing; cloud adoption is projected to triple by 2020; and governments, consumers and environmental activists are pressing for increased efficiency and accountability. As a result, public utility organizations are frequently undertaking ambitious IT modernization and consolidation efforts.

HOW THIS AFFECTS YOU

The communities and businesses you serve are depending on you to keep the lights on. To deliver on your mission, you need to:

- **Minimize disruption to energy services —** To avoid costly and potentially deadly service outages, you need to be able to quickly spot suspicious user activity, including changes to critical Active Directory, Azure AD and Office 365 groups. Ideally, you need a solution that can respond automatically to critical events and protect your most important AD objects from being altered in the first place.
- **Keep sensitive records safe —** You also need deep insight into system configurations and effective permissions, and the ability to spot and block suspicious user activity around critical data. You also need enterprise-quality backup and recovery solutions that enable you to restore normal operations as soon as possible after an attack.
- **Meet compliance requirements —** To avoid steep fines, increased oversight and loss of public trust, you need to be able to maintain continuous compliance with an increasing number of regulatory requirements and to prove that compliance during audit checks. In a complex IT environment with spiraling volumes of data, that requires automation, pre-built compliance reports, and enterprise-wide search capabilities that enable quick response to ad-hoc questions.
- **Keep existing systems up to date and be able to take advantage of new technologies —** Migrations are a fact of life for IT teams at public utility companies. The risks associated with software nearing or past its end of life are simply too great to be ignored, and moving to new platforms is critical for demonstrating leadership in areas such as environment stewardship. To reduce risk and meet deadlines, you need the right tools and expertise.
- **Ensure smooth IT integrations during M&As —** Mergers and acquisitions drive additional migration and consolidation projects. IT teams must regularly integrate diverse systems under tight deadlines, all without disrupting normal operations. Having a proven, repeatable framework and familiar tools is essential for meeting these demands without letting your critical everyday duties slide.

1 Ponemon, 2019 Cost of a Data Breach Report.



Keep records safe, maintain compliance and reduce service disruptions.

A BETTER WAY

What if you could keep sensitive records and critical systems safe, even as cyberattacks become more sophisticated and devastating? What if you could ensure continuous compliance with regulatory requirements, even as standards change and new laws are enacted? What if you could minimize disruption to energy services, even as you upgrade your systems, migrate to new platforms or consolidate multiple IT infrastructures?

WHAT YOU CAN DO ONLY WITH QUEST

Ensure security across your on-premises, cloud or hybrid environment

Consumer energy organizations are a prime target for attackers looking to steal valuable data or wreak destruction. The stakes are higher than in many sectors, since a successful attack can lead to devastating consequences, such as widespread outages, lasting damage to the environment and even loss of life. Improve your security posture with solutions that enable you to maintain continuous control over Active Directory, Group Policy, user permissions and system configurations, and to immediately spot and respond to suspicious user and administrator activity.

Maintain and prove ongoing regulatory compliance with proper governance .

Compliance mandates like PCI DSS and GDPR are growing in number and complexity. Non-compliance can lead to stiff fines,

increased oversight and reputation damage. Quest solutions can help you assess, monitor, govern and control your Microsoft systems to maintain regulatory compliance so you can improve security, minimize losses and maintain trust.

Deliver seamless migrations and consolidations again and again

Today, many organizations face continual IT modernization and consolidation, but in the energy industry, migration stakes are particularly high. The livelihoods and safety of thousands or millions of people might well depend on responsive IT systems. With Quest energy software solutions, you can ensure ZeroIMPACT AD, Exchange and Office 365 migrations that finish on time and on budget.

> Using Recovery Manager for Active Directory, the IT team had the domain operational again within an hour, averting potentially days or weeks of downtime and millions of dollars in revenue losses.[2]

2 Quest customer success story, https://www.quest.com/casestudy/energy-company-is-back-to-work-within-an-hour867300823149/

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

SolutionBrief-EnergyIndustry-US-KA-55353

Quest