VirtaMove
Migration Intelligence

Cyber Attacks Are Spiking in the Utility Sector:

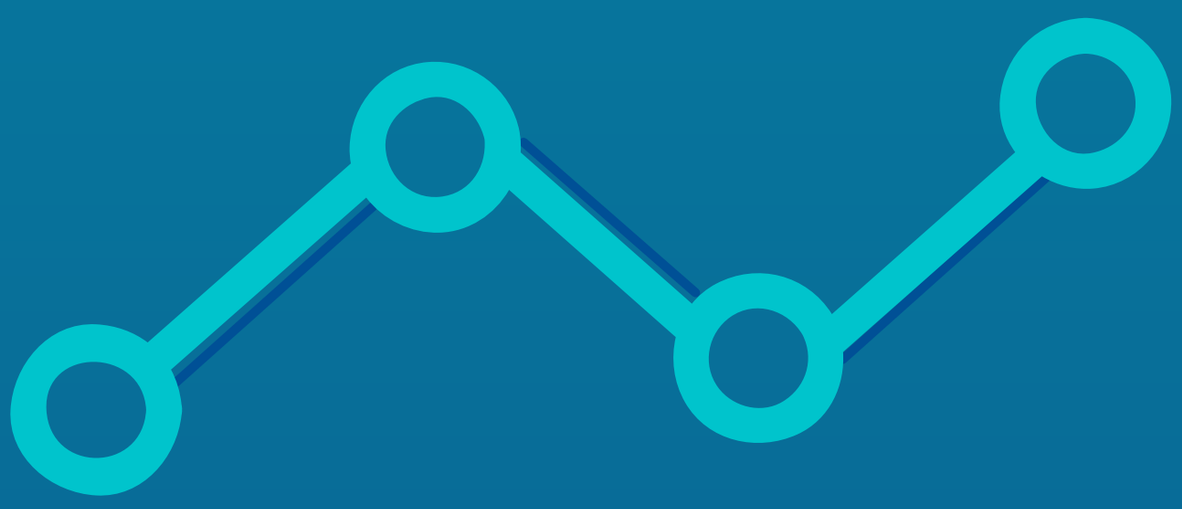
VirtaMove Can Help Address a Key Vector

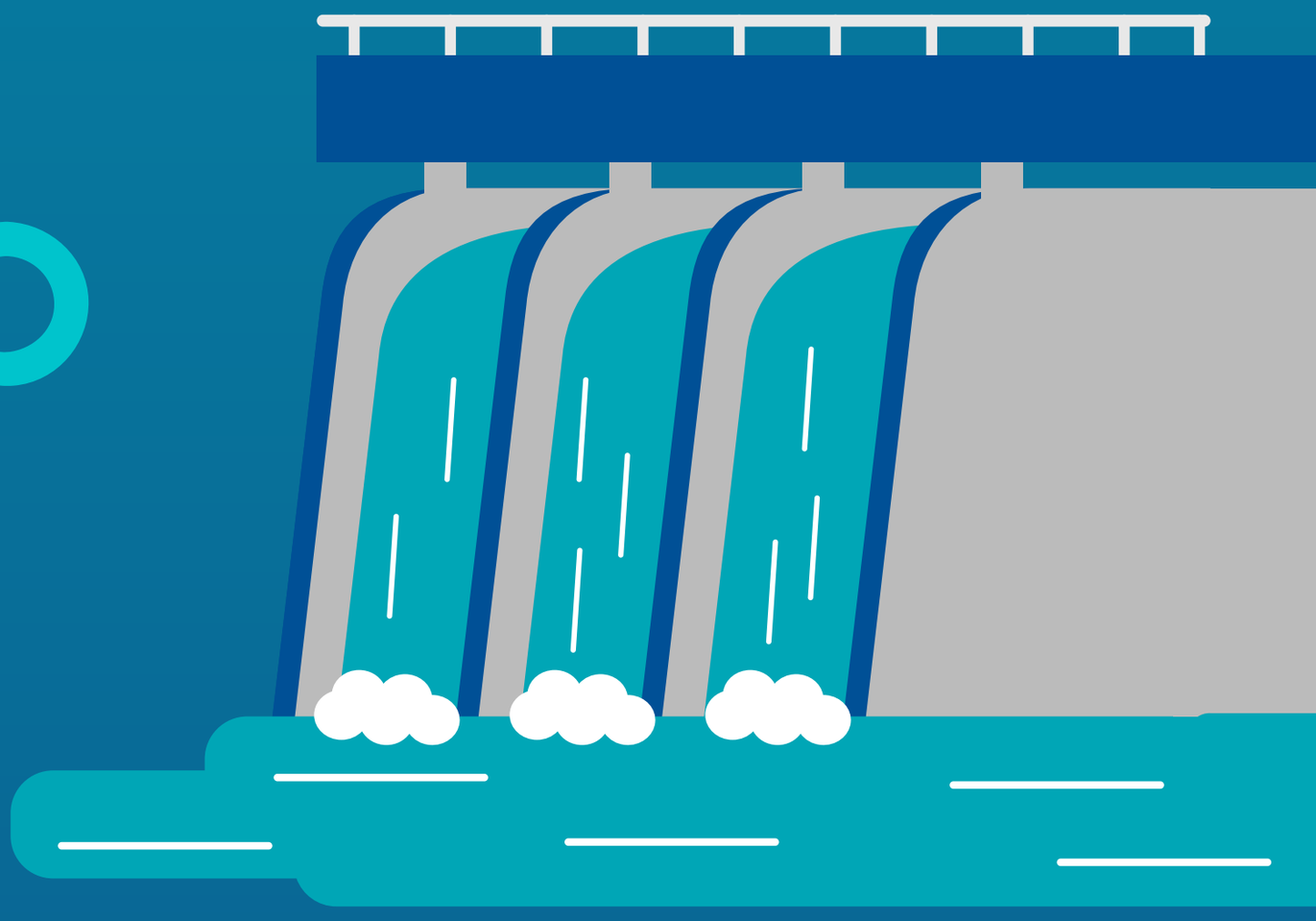
Security experts state that the utility sector, including electric, gas and water companies, has a growing ransomware problem. Ransomware is a type of malware that locks a company's data or computing systems until the victim pays a fee to the hacker, usually in cryptocurrency.

A cyber security report by Siemens and the Ponemon Institute suggested that cyber threats to utility companies are becoming more severe and that 54% of utilities could expect a cyber attack in 2020. The Edison Electric Institute, which represents investor-owned utilities, has stated "an uptick in attempted attacks" in part related to the COVID-19 pandemic. “Utilities are right there at the forefront of risk," said Bob Parisi, a US cyber product leader for a global insurance broker and risk adviser.

Electric utilities throughout the U.S. have seen a steady rise in cyber and physical security related events. In Canada, “cybercriminals are almost certainly improving their capabilities, and are increasingly likely to attempt to access, map, and exploit industrial control systems (ICS) for extortion with customized ransomware,” according to the Canadian Centre for Cybersecurity: “cybercriminals will likely be capable of targeting electricity sector ICS for extortion within the next three years.”

According to Marsh & McLennan, in the past few years, “hackers have increasingly targeted organizations that operate industrial control systems.” As more physical processes come online, “nation states are increasingly turning their sights toward chemical facilities, energy platforms, transportation networks, manufacturing plants, pipelines and water systems.”





What’s at stake?

Cyber attacks and ransomware payments affect the bottom line for utility companies and damage reputation. A shutdown or loss of operational data means disruption. Paying ransom doesn’t always restore data and operations. Attacking critical infrastructure and digital control systems, including safety systems, brings the potential for mass outages, damage to infrastructure and the environment, and injury.

What's at the root of cyber attacks in the utility sector?

According to Marsh & McLennan, "most successful cyber attacks exploit vulnerabilities that were not patched with the latest software fixes." According to a Mission Support Center Analysis Report (Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector), cyber attackers "take advantage of the 'low-hanging fruit' produced by the energy sector's delays in applying software updates and patches for problems that are several years old."

Siemens and the Ponemon Institute also point to "unpatched systems" as a vector. They cite visibility into IT and OT systems as a key component in dealing with cyber threats. They polled utility respondents about being able to achieve a comprehensive and continuous discovery and inventory of digital assets, and ratings were "particularly low." Providing meaningful security on a network is hard to do "when operators do not know what equipment exists within that network."

Keeping up with the latest operating systems and patches can be onerous, particularly for large organizations with complex legacy IT environments.

How VirtaMove can help

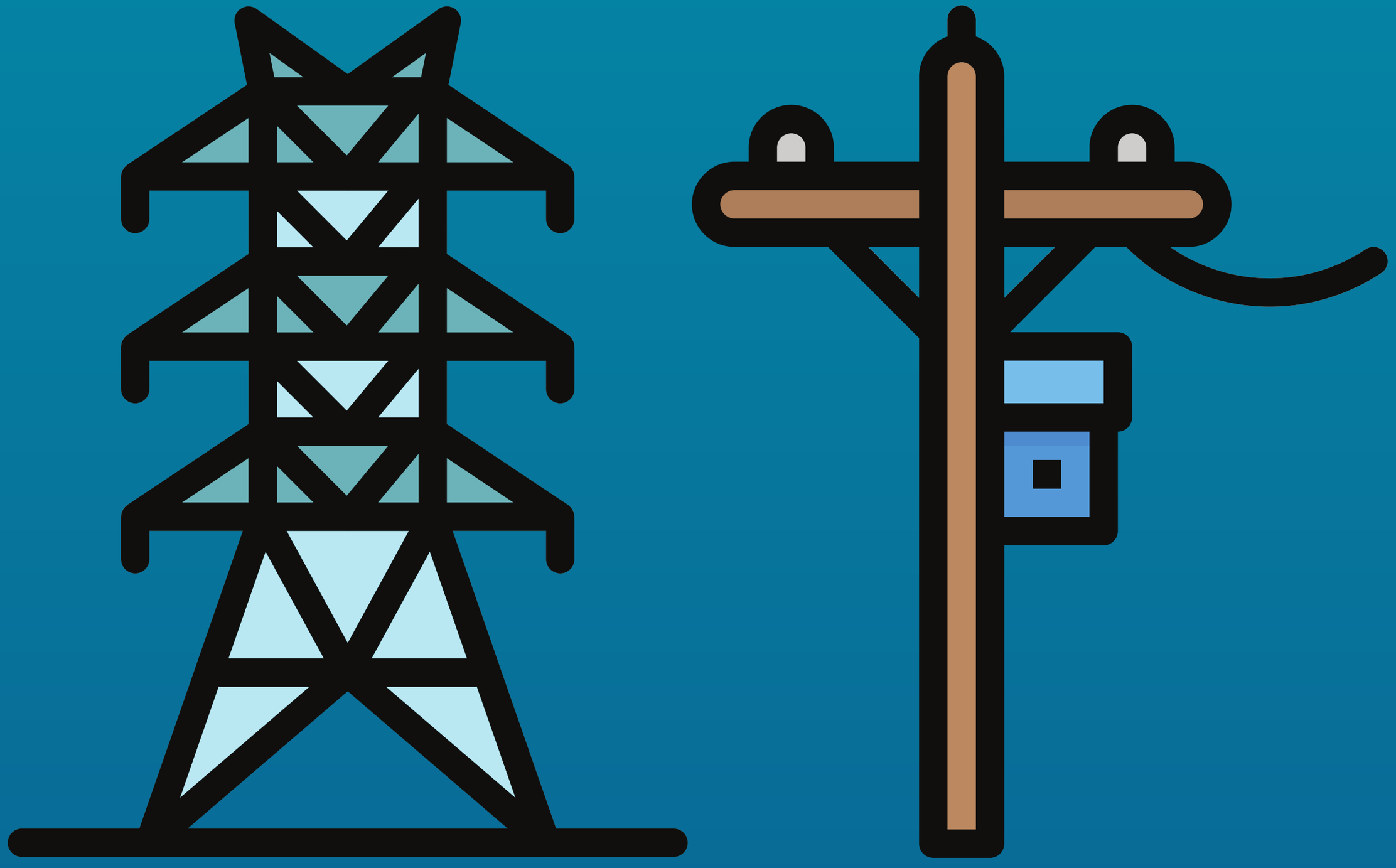
VirtaMove's technology can help the utility sector modernize its IT infrastructure in a timely and cost-effective fashion. Our Migration Intelligence Suite uses automation to discover your digital assets, capture applications along with all dependencies and historical data, and perform a stateful re-install in a modern and supported environment.

Automated discovery and migration allow your company to save roughly 70% of the costs that you would incur with a hand migration. Parallel migrations are possible with automation, meaning that you can modernize more apps in less time. If the scale of the issue is daunting, automation and a proven migration methodology are on your side.

A stateful re-install of legacy applications offers many benefits for a modest infrastructure investment, including closing known vulnerabilities and exposures on outdated, unpatched OS instances and enhanced performance on newer, faster hardware. It also extends the useful life of your apps while allowing concurrent plans and activities, such as IT audits and security and risk assessments.

Contact VirtaMove to schedule a demo or learn more about automated migration. We help companies like yours secure a brighter future every day and we're always pleased to share what we know.

VirtaMove
Migration Intelligence



ABOUT VIRTAMOVE

VirtaMove subscription-based software moves server applications to new cloud or datacenter servers in a fraction of the time and cost associated with traditional migration methods. Install scripts and source code not required. Encapsulating Windows Server and Linux applications in VM/OS-free moving containers, VirtaMove's patented software provides an automated, stateful re-install of most complex server applications. VirtaMove allows you to modernize your infrastructure, moving from an old, unsupported OS to a newer one with automation – modernize and move forward to a new datacenter server or cloud in one step. Reach out to us at info@virtamove.com or check out our website www.virtamove.com to learn more.