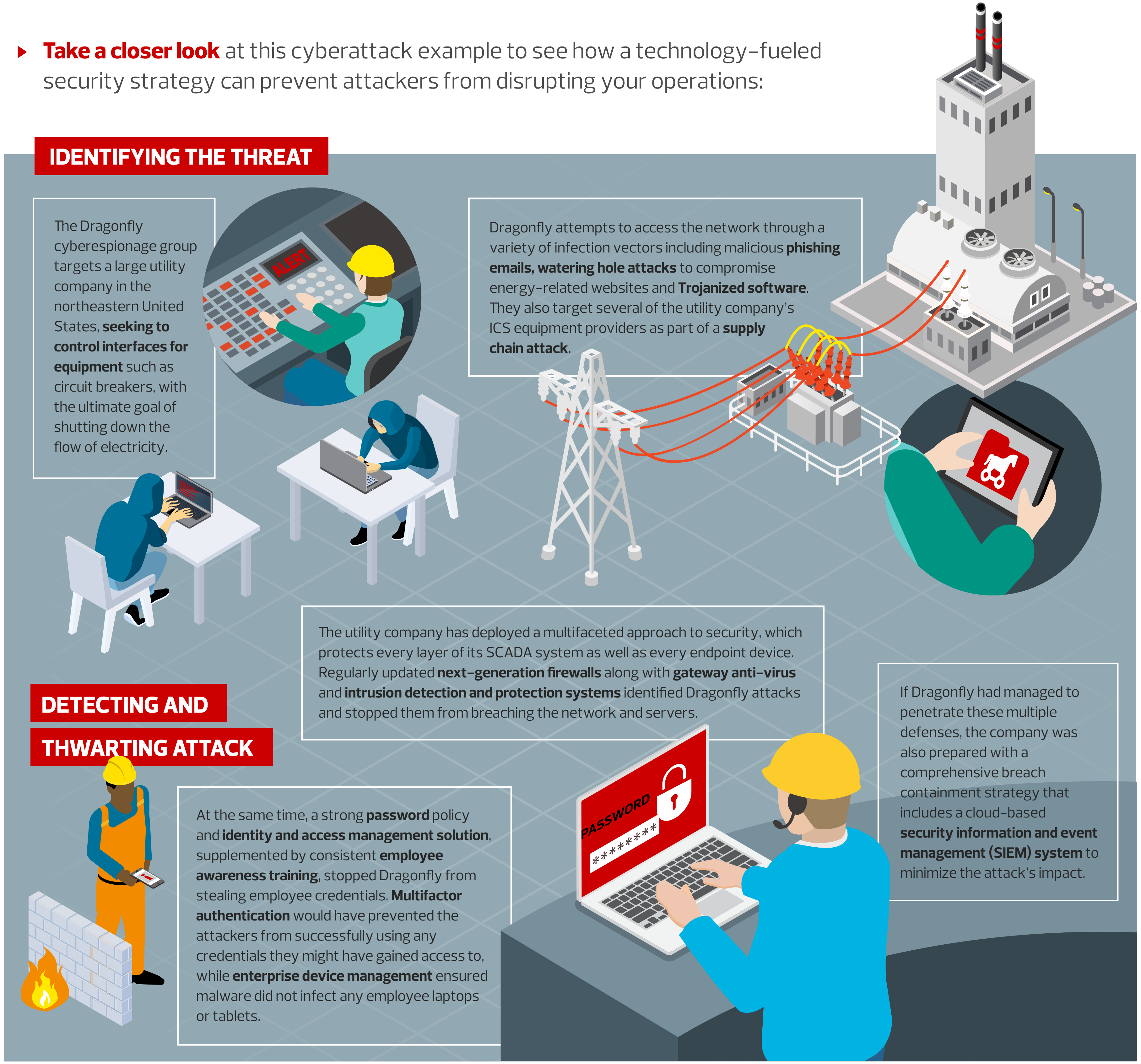
SOLUTION IN ACTION

Protect SCADA Systems Against Escalating Risk

Energy and utility companies must vigilantly defend their critical infrastructures against cyberattack. Threats are becoming more frequent and sophisticated, and SCADA systems increasingly connect with IT networks, IoT, the cloud and mobile devices.

Vulnerability has soared, putting everything from pipeline operations to the smart grid to nuclear facilities at risk of sabotage, disruption or shutdown. To keep cyberattackers at bay, companies must conduct regular risk analyses to identify security gaps as well as implement and update multilayered security components.

▸ **Take a closer look** at this cyberattack example to see how a technology-fueled security strategy can prevent attackers from disrupting your operations:



IDENTIFYING THE THREAT

The Dragonfly cyberespionage group targets a large utility company in the northeastern United States, **seeking to control interfaces for equipment** such as circuit breakers, with the ultimate goal of shutting down the flow of electricity.

Dragonfly attempts to access the network through a variety of infection vectors including malicious **phishing emails, watering hole attacks** to compromise energy-related websites and **Trojanized software**. They also target several of the utility company's ICS equipment providers as part of a **supply chain attack**.

DETECTING AND THWARTING ATTACK

The utility company has deployed a multifaceted approach to security, which protects every layer of its SCADA system as well as every endpoint device. Regularly updated **next-generation firewalls** along with **gateway anti-virus** and **intrusion detection and protection systems** identified Dragonfly attacks and stopped them from breaching the network and servers.

At the same time, a strong **password** policy and **identity and access management solution**, supplemented by consistent **employee awareness training**, stopped Dragonfly from stealing employee credentials. **Multifactor authentication** would have prevented the attackers from successfully using any credentials they might have gained access to, while **enterprise device management** ensured malware did not infect any employee laptops or tablets.

If Dragonfly had managed to penetrate these multiple defenses, the company was also prepared with a comprehensive breach containment strategy that includes a cloud-based **security information and event management (SIEM) system** to minimize the attack's impact.

BEHIND THE SCENES

Well aware that its SCADA system and networks are a prime target for threat actors, the utility company works with its IT partner to periodically **audit its SCADA environment** and network-connected components for any new vulnerabilities. It also takes a proactive approach to malware detection, conducting regular threat checks that **incorporate passive network and endpoint monitoring** to detect botnets and any infected clients.

To protect your critical infrastructure from potentially destructive cyberattacks, you need an integrated security strategy that helps you identify vulnerabilities, defend against threats, and detect and respond quickly should an attack occur.

See how CDW can help you capitalize on the latest technology to better protect your SCADA systems. Request a free security scan at **CDW.com/threatcheck** or contact your CDW account manager at **800.800.4239**.