



DATA SHEET

Cyberthreats: Prevention and protection for utilities

An integrated approach to identifying risk and protecting and defending the grid

The security imperative

Cyberattacks – from untargeted ransom-ware to sophisticated national breaches – can threaten the performance of the grid or impact individual privacy. The consequences for utilities, their customers and related economies can be serious.

Cybersecurity is a high priority for most businesses nowadays, but organizations delivering critical services – such as utilities – face more challenges than most.

A reliable and stable power supply is core to energy grid operations. In response to a breach, utilities cannot simply shut down or isolate systems. Their primary concern is keeping the system running without interrupting supply.

Improved integration between utilities' energy operations and IT can help them to discover and exploit data intelligence and better meet the new challenges of a complex energy grid.

However, security concerns hold utilities back. The imperative to keep the lights on can make them hesitant to push forward with integration initiatives and expose grid operations to IT.

While this cautious approach is understandable, the disruptive challenges of the new energy system demand action. Energy executives need to find a happy medium, balancing benefits with potential risks.



What we bring

Defending the utility grid needs the right technology, processes and, above all, people.

OMNETRIC is dedicated to improving energy providers' performance by integrating their energy operations with IT to support business goals. We have been recognized as a leader in the IDC MarketScape: IT and OT Integration Service Providers for EMEA Utilities 2017 Vendor Assessment.*

To utilities' cybersecurity challenges, the OMNETRIC team brings:

- CISSP qualified cybersecurity experts with deep understanding of the specific needs of the energy grid and access to power engineers and product specialists.
- Many years' experience in IT, security and energy grids.
- The rare combination of deep experience with operational technologies across transmission and distribution and IT consulting and systems integration expertise.
- Access to the research and market analysis of our shareholder Siemens – and our other ecosystem partners – to bring the latest product insights to our methodology.

* Doc # EMEA40142616, February 2017

Goal: Sustainable protection

We support utilities to explore existing and future security risks, implement and integrate security solutions and operate and optimize their systems' defense and processes through a range of measures (see figure 1 below).

We propose solutions across technical, organizational and process contexts. While we can help with point solutions such as specific hardening controls, cryptography systems for smart meters and log integration, our aim is always sustainable protection.



Figure 1: An integrated approach to cybersecurity

How we help utilities respond to cyberthreats

- **Security governance:** Getting cybersecurity considerations integrated into all business decisions.
- **Risk management:** Identifying and understanding cybersecurity risks and putting in place the best controls to mitigate them.
- **Protection solutions:** Selecting and implementing the right security controls, such as firewalls and identity management, to stop attackers breaching systems.
- **Verification:** Testing security controls to ensure optimal operation.
- **Security processes and procedures:** Ensuring the ongoing effectiveness of the security measures in place.
- **Monitoring and intrusion detection:** Detecting policy failures and security breaches.
- **Incident response:** Putting a plan in place for dealing with security incidents.
- **Incident recovery:** Restoring measures after an attack and learning lessons from what went wrong.

Getting the best results

The effectiveness of a security strategy is enhanced when:

The right talent is in place

Utilities should hire defenders and a range of other talents relevant to the cybersecurity threat – IT experts and engineers as well as security experts with utility backgrounds all have their place. These professionals understand operations related to running the grid, as well as the complex underlying systems.

Security is on the corporate agenda

Security decisions are about balancing risk, so need to be made in collaboration with informed, senior leaders who can see and assess the complete picture. The involvement of senior leadership is critical to ensure effective prevention and protection measures, as well as the mobilization and focus of the right people in times of crisis.

Security is baked into the core solution

Security needs are best assessed while solutions are architected, rather than later when the solution is in operation. If core energy technology can be implemented into a secure environment, that addresses the people, process and technical aspects of security, risks are minimized. If security is not baked into the solution from the outset, a security breach down the line can be more difficult, costly and disruptive to address, and the remedial efforts generally less effective.

How to get started

To help utilities identify and evaluate security issues, we offer a Cyber Maturity Assessment – an approach to help establish the current security position of a utility's energy solutions and enable better decisions about where to target security investments.

Our aim is to help utilities get out of the fire-fighting trap and into strategic improvement. Our assessment methodology is based on ES-C2M2 and can assess maturity against standards such as NERC CIP, ISO 27001, ISF Good Practice and NIST 800.

The changing security landscape

Digitization:

Placing essential equipment and assets under physical lock and key used to provide adequate protection. Today, a growing number of devices, unprecedented connectivity between the grid and other systems, and distributed energy resources demand new approaches.

Dispersed influence and control:

Devices now operate beyond the sub-station and are often – in the case of smart meters for example – physically accessible by people outside the utility. More people, organizations and devices in the equation, particularly those outside the utility's firewall, mean more risk. Greater automation makes it harder for operations staff to spot unusual behaviors or anomalies, increasing the risk further.

Availability of tools:

With the required tools readily accessible via download, a growing list of threat actors (hackers, terrorists, criminals...) are equipped to attack the grid.

Requirements and regulations:

Regulators are moving with the times to respond to customer concerns. The GDPR – General Data Protection Regulation – for example is improving safeguards on personal data across the EU. The development of the North American NERC CIP regulations continues and more countries are implementing local regulations. These regulations at country or state level are shifting the security landscape for utilities.

Get in touch

We have the sector knowledge, the engineering, data and security skills and experience to deliver security solutions that meet the needs of energy sector organizations. We understand the challenges of working with critical infrastructure and the importance of grid reliability and efficiency. We are also aware of the impact of security threats and the speed at which new threats are emerging.

Contact us

Business requests:
request@omnetric.com

Marketing and corporate communications:
pr@omnetric.com

Careers enquiries:
www.omnetric.com/vacancies

About OMNETRIC

OMNETRIC is dedicated to helping energy providers reap the benefits of the digital energy system by integrating their energy operations with IT to support their business goals.

Our global team of engineering, IT, security and data experts brings extensive industry experience to help customers discover and exploit data intelligence to capitalize on industry change, and realize new business models.

Helping customers since 2014, we are an inventive, technology services company. For more, visit www.omnetric.com.

OMNETRIC is a Siemens company.