It’s not if, but when

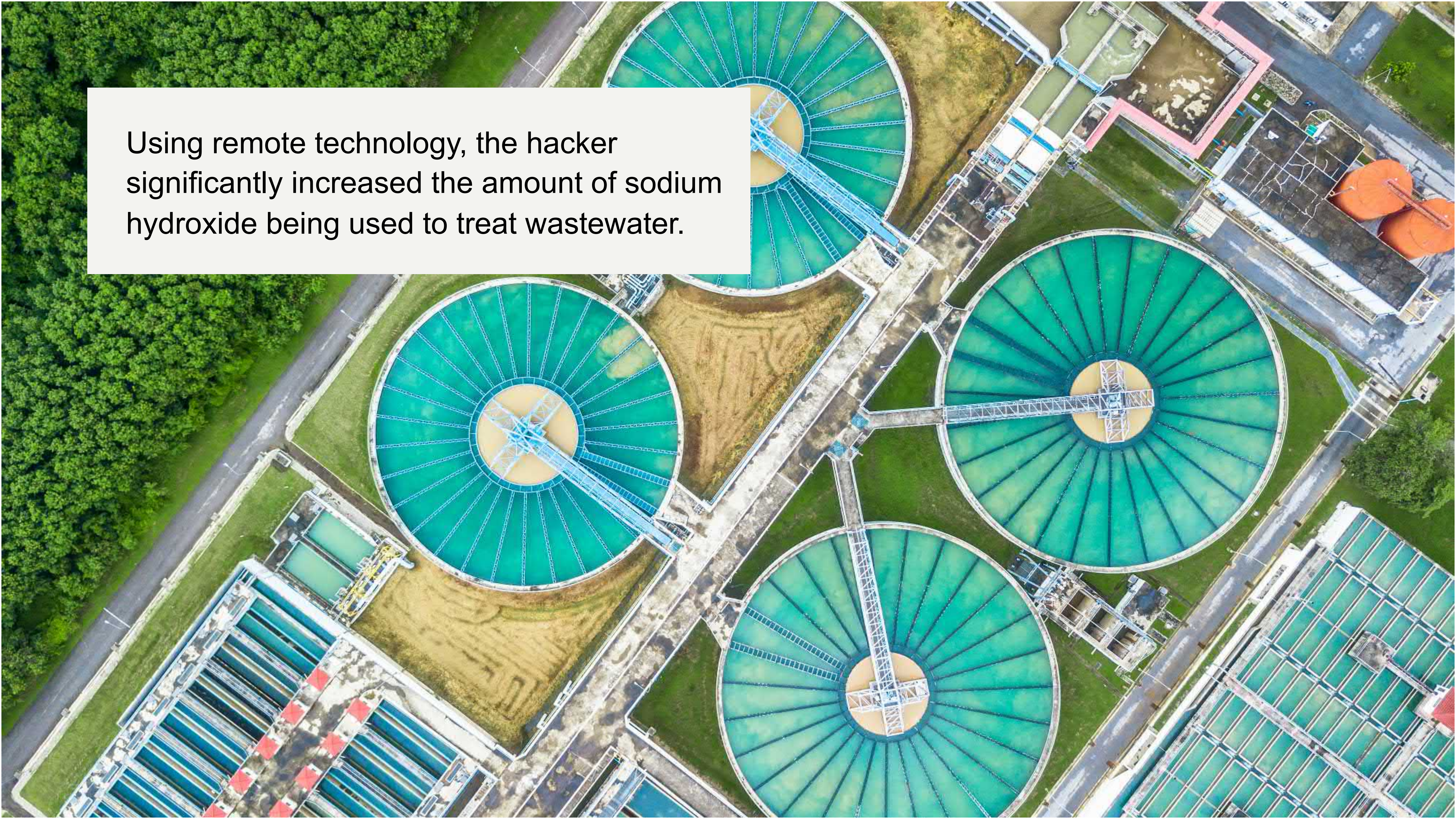
SIEMENS

Every year cyber security thought leaders publish reports that look at different trends. Invariably and universally, critical infrastructure network operators, such as utilities, top their lists of industries that are prime targets for hackers.

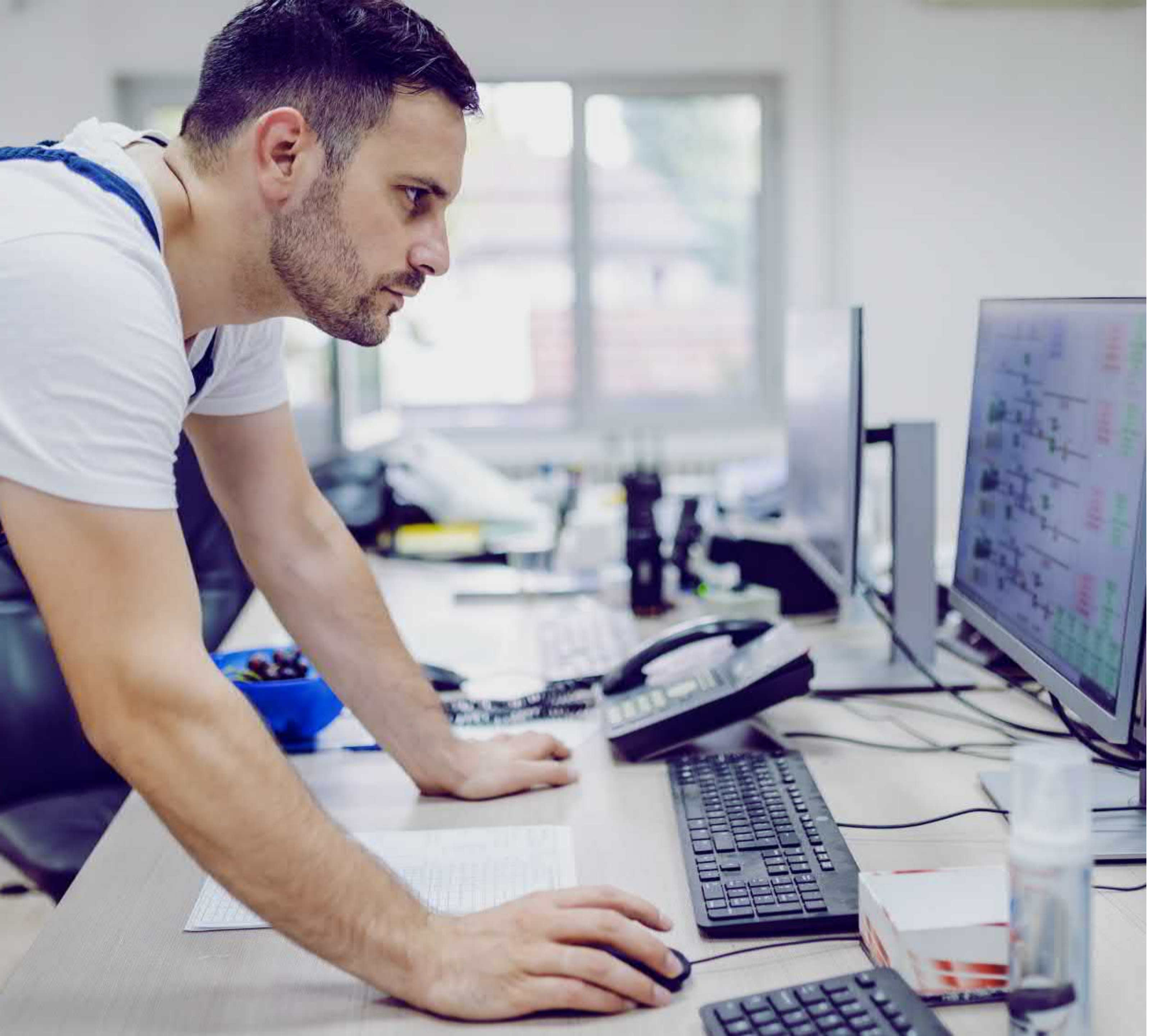
It shouldn’t come as a surprise. If bad actors want to inflict maximum systemic damage to the economy and disrupt all aspects of daily life, utilities are a very enticing target.

On February 5 2021,
a computer hacker attacked a small water utility in Florida, breaching a remote access program shared by plant workers. It made national news.

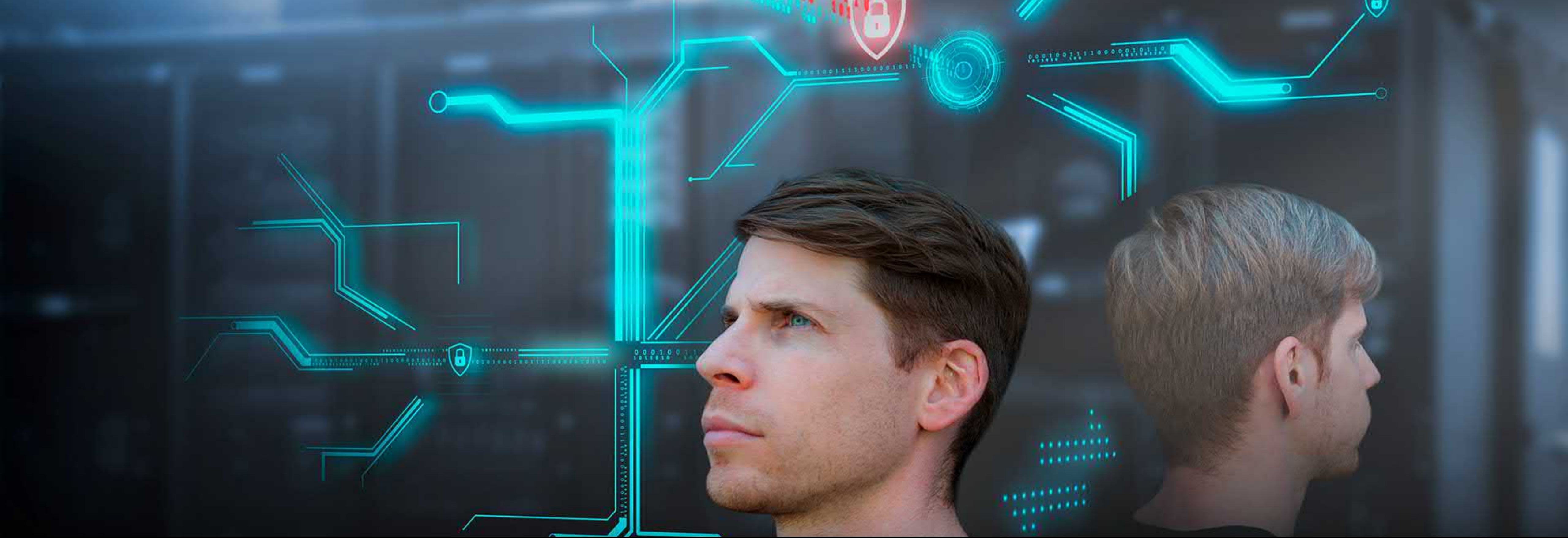
SIEMENS



Using remote technology, the hacker significantly increased the amount of sodium hydroxide being used to treat wastewater.



Fortunately, an employee noticed a cursor moving on his system monitoring screen and reversed the chemical flow before anyone was harmed.



This incident was yet another reminder that we must constantly be on guard and take steps to mitigate attacks before they occur.

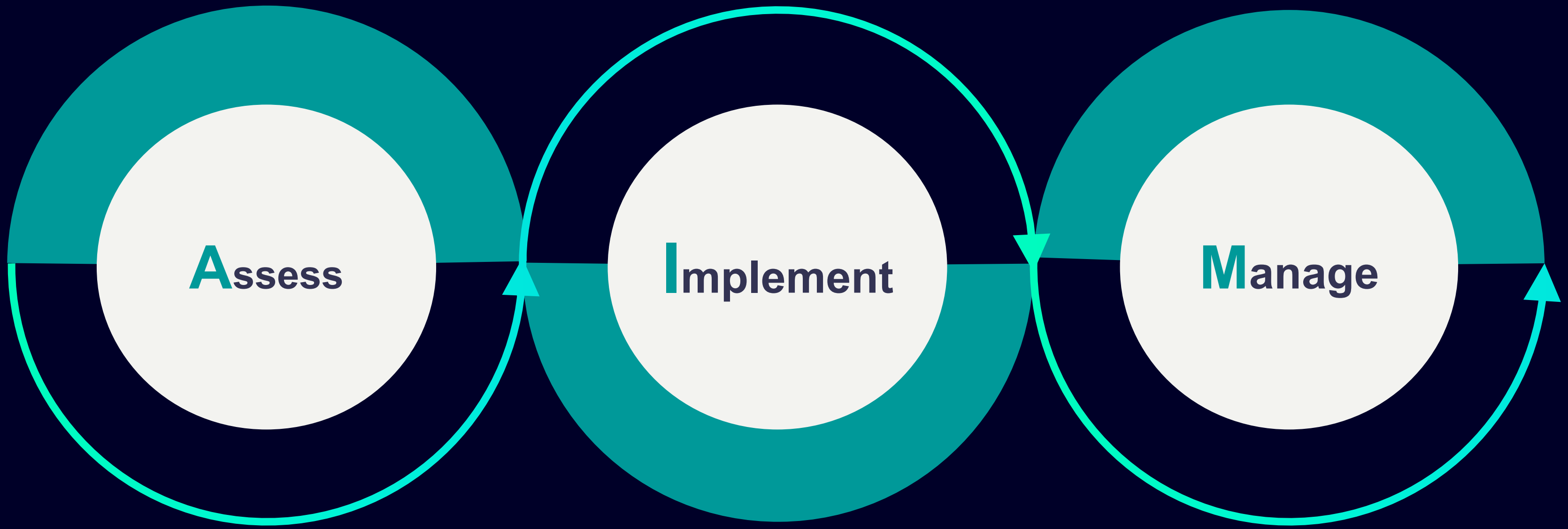
SIEMENS

Dealing with a cybersecurity threat is not a matter of “if” but “when”.

Here are 3 steps operators of critical infrastructure networks can take to harden their cybersecurity defenses.

SIEMENS

Step 1: Follow the A.I.M process.



SIEMENS

Assess

Assess your network from end-to-end, identifying and analyzing all of your IT and OT network assets. This help highlight security vulnerabilities.

Implement

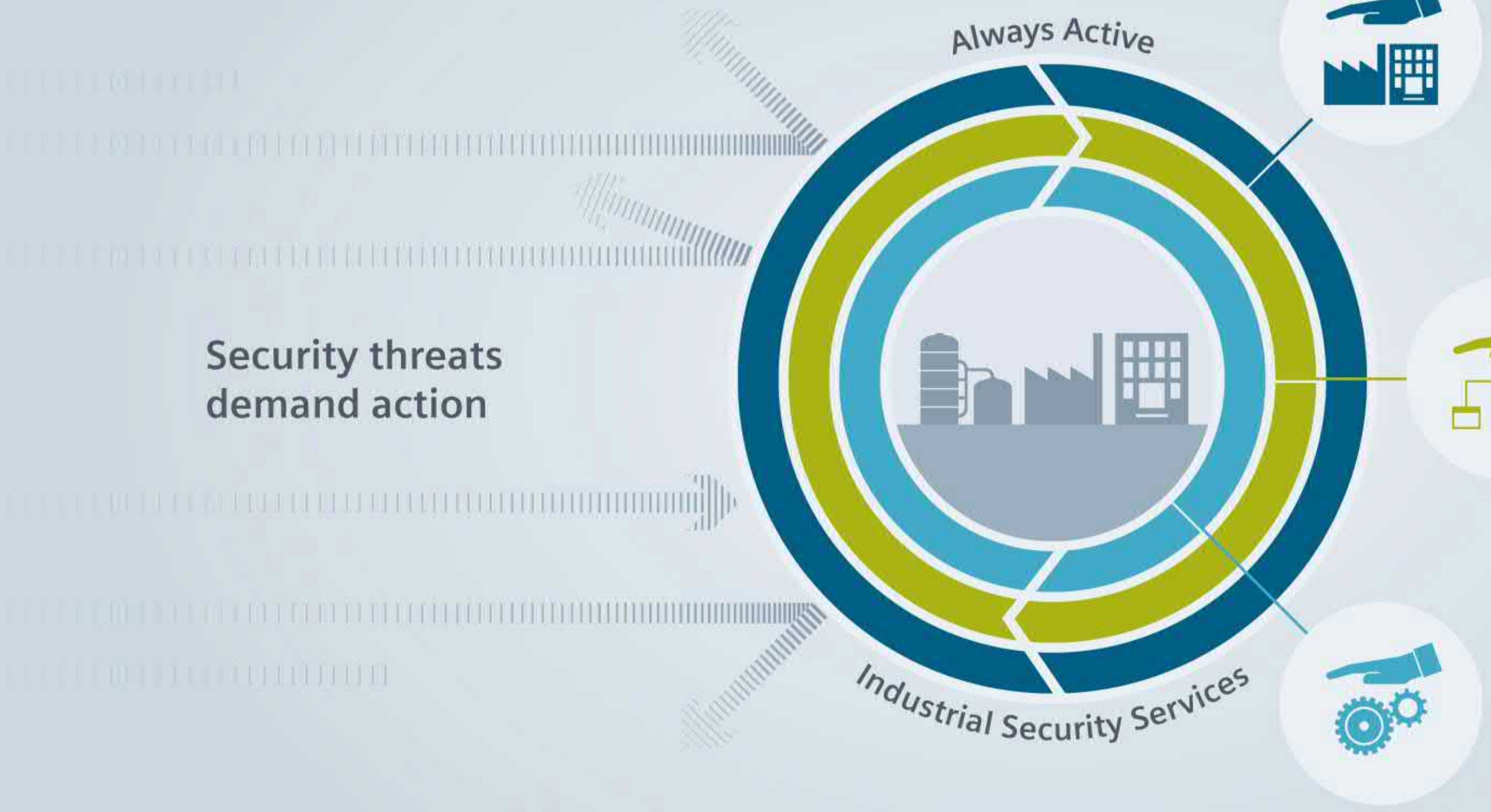
Implement a new security regime where everything you do is secure by design. Pre-configuration, testing and training helps ensure that everything goes as smoothly as planned.

Manage

Actively **Manage** your network. Stay on top of key areas, monitor threats and keep your security up to date.

Step #2: Follow a holistic Defense in Depth strategy that employs multiple layers of protection – physical, network, and systems – with corresponding system support and monitoring redundancies.

Defense in depth



Security threats demand action

Plant security

- Physical access protection
- Processes and guidelines
- Holistic security monitoring

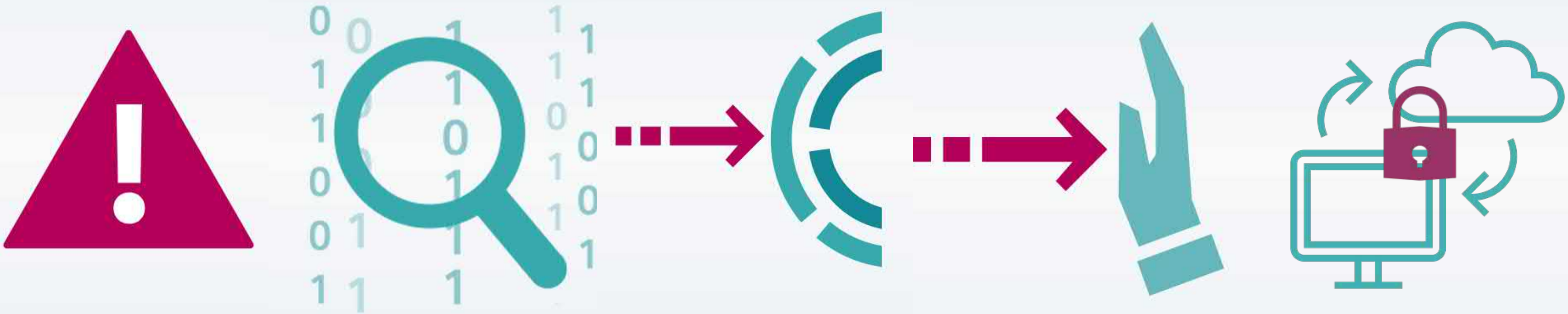
Network security

- Cell protection and perimeter network
- Firewalls and VPN

System integrity

- System hardening
- Patch management
- Detection of attacks
- Authentication and access protection

Step #3: As part of your Defense in Depth strategy, incorporate advanced cybersecurity solutions across your network with the guiding principle being “the right solution in the right place”.



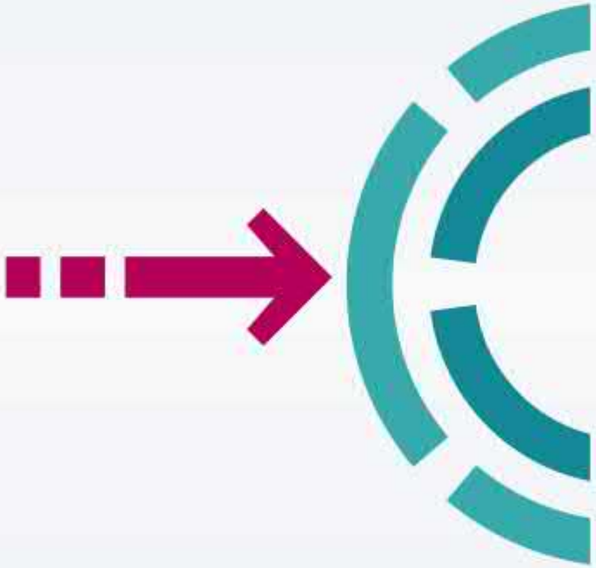
Siemens and its RUGGEDCOM cybersecurity solutions give you the freedom to focus on what matters by providing guidance and consultation with A.I.M. and Defense in Depth.

We can also deliver best-in-class cybersecurity solutions through our partnerships and multi-service platform with the APE1808 (Application Processing Engine).

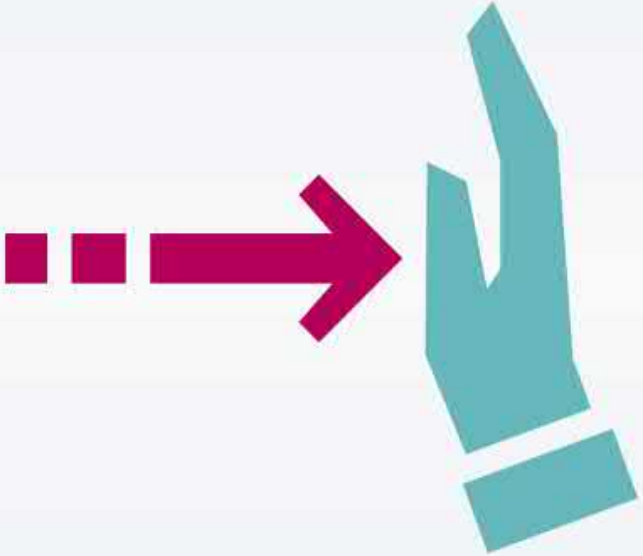
Siemens cybersecurity solutions include both signature-based and non-intrusive, anomaly-based signatureless **Intrusion Detection System (IDS**) software which provides early-warning notifications and alerts on vulnerabilities and sophisticated cyber threats.

We have **Deep Packet Inspection (DPI)** that examine data packets utilizing a non-intrusion methodology focused on OT protocols (such as Modbus and DNP3).

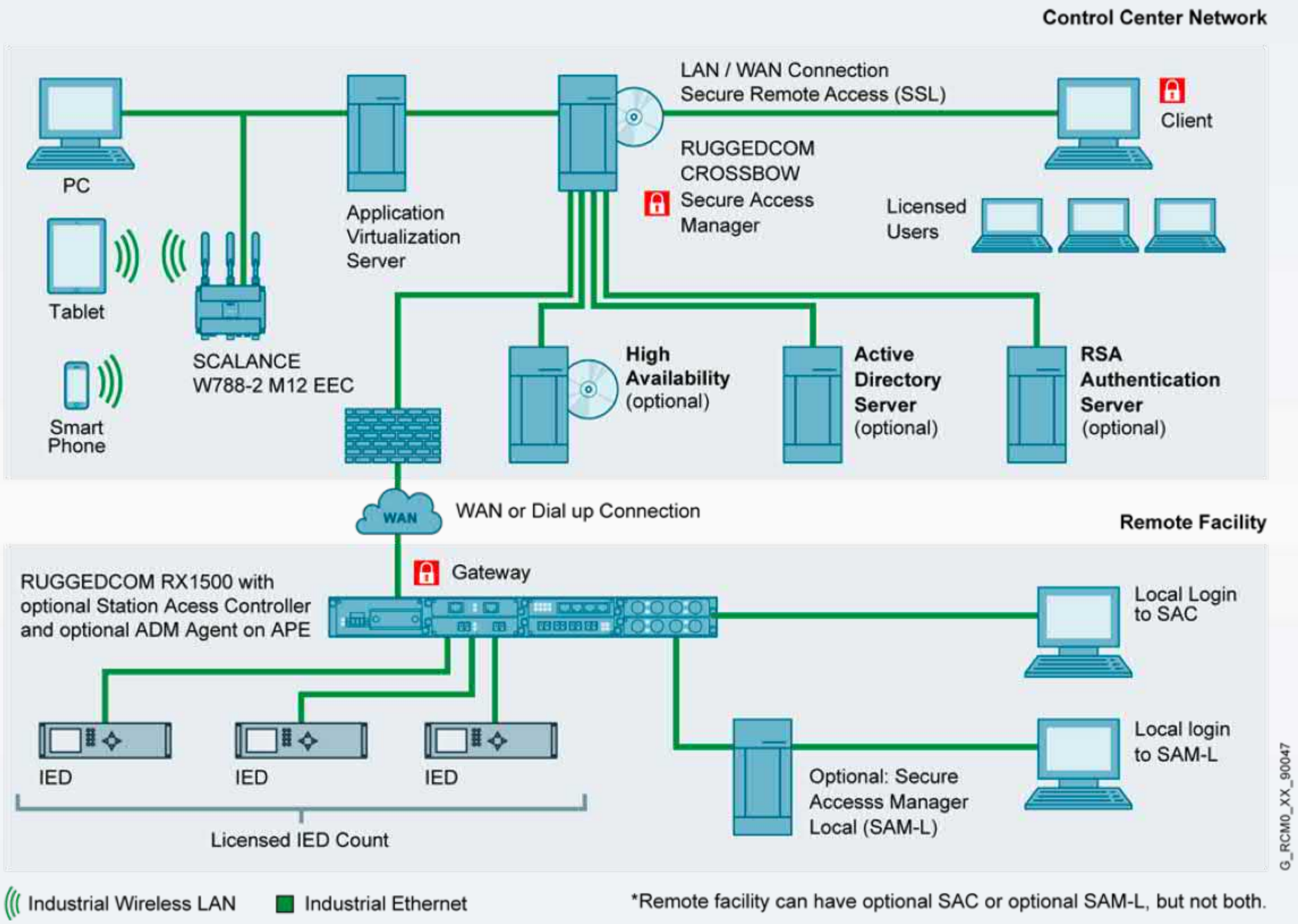
DPI constantly inspects for potential non-compliant or anomaly-based traffic, viruses, spam, intrusions or user-defined criteria giving better visibility into the traffic traversing the network and notifying the operator of any potential threats.



Combining RUGGEDCOM's switching and routing platform with leading **Next Generation Firewalls (NGFW)** functionality on a single, integrated appliance, provides for additional integrated DPI/IPS functionalities, offering additional security.).

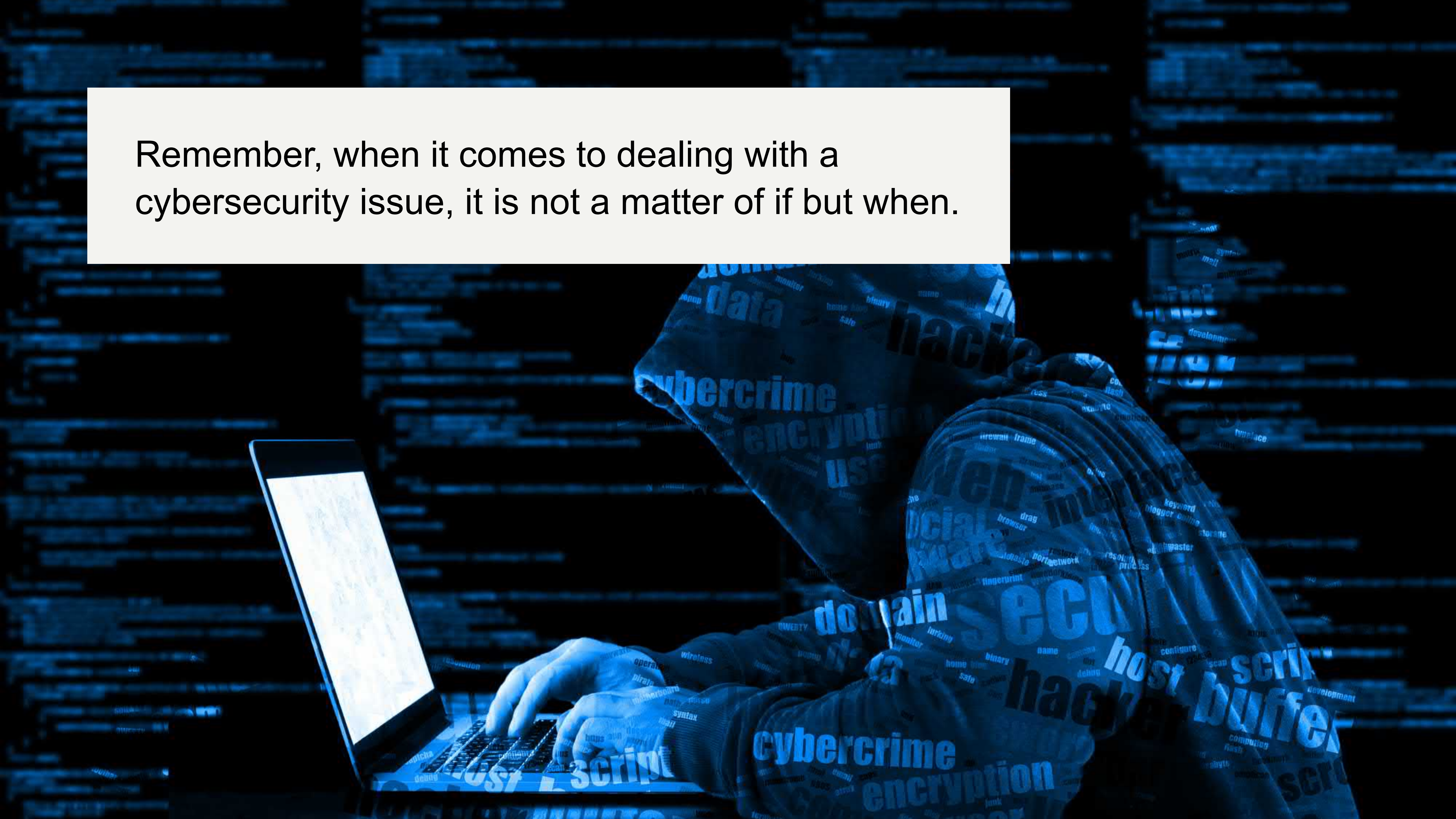


An **Intrusion Prevention System (IPS)** is another capability available on RUGGEDCOM hardware if equipped with a NGFW solution. Located between the WAN and LAN, IPS denies traffic that represents a known threat based on specific security profiles.



Additionally, having a **secure remote access tool** that provides a **protocol break** between the users and the devices enhances your overall Defense in Depth approach.

Remember, when it comes to dealing with a cybersecurity issue, it is not a matter of if but when.



If safeguarding your network, ensuring compliance, securing your bottom line and achieving your business goals are areas of concern….think Siemens and RUGGEDCOM.

SIEMENS

SIEMENS

usa.siemens.com/ruggedcom