DeepArmor® Industrial, fortified™ by Siemens Energy

AI-driven Cyber Defense for Endpoint Energy Assets
The Siemens Energy-SparkCognition Partnership

Siemens Energy, a global powerhouse focusing on the areas of electrification and digitalization, and SparkCognition, a leading artificial intelligence company with deep experience in cybersecurity, are partnering on a revolutionary cybersecurity system — DeepArmor® Industrial, fortified™ by Siemens Energy — to protect the energy industry’s endpoint operational technology (OT) by leveraging artificial intelligence (AI) to monitor and detect cyberattacks.

This new collaboration draws on SparkCognition’s award-winning machine learning technology and Siemens Energy’s global cybersecurity and energy equipment expertise to define a new category in endpoint cybersecurity for the energy industry.

From its founding, SparkCognition recognized the growing threat of zero-day attacks to isolated, fixed function assets in the oil and gas industry. This vulnerability led SparkCognition to pioneer the use of artificial intelligence to prevent or mitigate new attacks for remote energy assets — one of the few technologies that can provide defenses against unknown attacks.

Siemens Energy’s heritage as an equipment manufacturer and service provider throughout the energy supply chain brings more than 170-years of expertise creating entirely new technology categories and seamlessly integrating these solutions with existing systems. The company’s expertise in the cybersecurity business comes from its legacy as an integral operator and solutions provider of energy technologies that leverage digitalization and intelligent infrastructure.

Siemens Energy’s promise is complete industrial-grade endpoint protection for the energy sector. Our approach applies SparkCognition’s AI innovations and Siemens Energy’s OT-native knowledge base to the unique needs and normal workflow of each customer site. We design, install, tune, and provide service for DeepArmor® Industrial customers, delivering a deep expertise for a shared cybersecurity journey.

It’s a partnership that will set a new standard for excellence in cybersecurity.
Cyberattacks threaten the reliability of the energy supply chain, and pose a significant risk to the core business for every energy company. The need to defend many facilities that are physically remote makes necessary maintenance difficult and expensive.

DeepArmor® Industrial, fortified™ by Siemens Energy, answers the need to defend current and future critical infrastructure from escalating cyberattacks targeting operational technologies.

Tuned to evolving site operations, the AI-based technology recognizes and reports new devices or behavior changes that characterize insider threats. Its predictive analysis enables DeepArmor® to prevent malicious code from executing, even if that code is not yet part of threat intelligence packages. This solution also recognizes and reports changes to system conditions that characterize a digital-physical attack, either mitigating the threat or making it easier to diagnose. This means DeepArmor® Industrial provides unique, unprecedented protection to edge assets in the field — even if new threats emerge between updates, or attacks arrive at isolated sites before patches can be deployed.

The engineers collaborating on DeepArmor® Industrial design and deploy a configuration that matches the actual workflows of distributed sites and relative risks based on an asset’s value and degree of exposure. The combination of SparkCognition’s artificial intelligence — and Siemens Energy’s expertise in the energy industry’s operating environment — enables resilient defenses that support continued normal operations.

Most current technologies rely on updates. A system updated on Monday is ineffective on Friday against any new attacks emerging on Tuesday, Wednesday or Thursday. Not DeepArmor® Industrial. Its machine learning detection engine uses advanced classification algorithms to predict and prevent zero-day industrial attacks without frequent updates or cloud access, greatly enhancing asset protection. The machine learning models are tailored by Siemens Energy and SparkCognition for the OT environments. They are built using samples of known clean files and malicious files targeting OT environments. The result is the protection layer includes script control, USB control, application control, and model control. Once installed and serviced by Siemens Energy, it remains steadily effective — without regular updates, and in the face of innovative attacks developed any day of the week, month, or year.
The Energy Industry’s Connectivity Paradox

Losing Visibility in the Gathering Storm

A chief information security officer’s phone rings in the middle of the night. It’s bad news. A compressor station is down, no one is sure why, and a thousand miles of pipeline — and all the natural gas inside it — stall. Producers counting on getting their product to market will have to find other routes. Customers in need of just-in-time delivery will end up scrambling. And until technicians can trace and isolate the problem, no one can guarantee other compression stations will remain operational.

This scenario — or something much like it — happened. Earlier this year, the United States Department of Homeland Security confirmed that a ransomware attack using phishing email tactics put a natural gas compression facility out of operation for two days.

Across the oil and gas supply chain, companies recognize cyberattacks as a real and growing threat. A Ponemon Institute study of the oil and gas industry found that 67% of respondents believe the risk level to industrial control systems over the past few years has substantially increased because of cyber threats. The study also found that 61% of respondents said their organization’s industrial control systems protection and security was not adequate.

Outages pose a threat to immediate and future business, making cybersecurity a necessary competency for the energy sector. Customers demand reliability, and will divest from business that can’t reliably defend their infrastructure. Yet companies face physical, financial, and legacy constraints in securing infrastructure. Navigating these complexities to achieve a durable, efficient, and perpetually vigilant cyber defense system takes an intimate knowledge of the energy supply chain — but it gets easier with a spark of artificial intelligence.

The traditional OT security model has been perimeter-based, with an air gap that creates a physical barrier to the outside world. This approach is not foolproof or sustainable long-term due to compromise from USB devices, wireless access points, and the increasing need for remote access and connectivity. Between patches, isolated systems remain vulnerable to new attacks, and a strong perimeter may not prevent attacks from spreading laterally within a compromised network.

That is why Siemens Energy and SparkCognition have partnered to develop AI-based solutions that can operate on isolated energy systems and defend against novel cyber-attacks.
Information Technology (IT) vs. Operational Technology (OT)

**IT**: The servers, computers, and mobile devices that enable business operations in the utility industry in office environments.

**OT**: The machines, systems, and networks used to generate, transmit, and distribute energy.

### Component lifetime
- **IT**: 3–5 years
- **OT**: 10–20 years and legacy systems

### Cyber Market Maturity
- **IT**: Mature stages & advanced cyber knowledge
- **OT**: Early stages & limited awareness

### Key Concerns
- **IT**: Loss of data
- **OT**: Impact to production, health, safety & environment

### Recovery Ability
- **IT**: Recover by reboot
- **OT**: Fault tolerance essential

### Connectivity
- **IT**: Continuous
- **OT**: Intermittent, high delay causes serious concern

### Ability to Update
- **IT**: Straightforward upgrades, automated changes
- **OT**: Typically difficult to patch, changes made by vendors

Comparison of Information Technology (IT) with Operational Technology (OT)
Widespread adoption of digital technologies has helped energy companies improve safety and reliability, while reducing emissions and costs. Yet, increasing connectivity expands cyberattack exposure for the nation’s far-flung power generation, distribution, and critical infrastructure.

The Cyber Threat to Brownfield Assets

Consider compressor stations, targeted in the attack mentioned earlier. Older stations, like other “brownfield assets,” were cutting-edge decades ago, and still rely on a mix of analog equipment and retrofits in today’s digital age. Many of these facilities must be physically distant — the demands of physics dictate their location along a pipeline. Depending on the equipment, they may connect to networks for annual updates, or receive updates from technicians only through site visits. Paradoxically, the same isolation that protects equipment against some types of attack results in longer exposure to emerging risks and increased expense for maintenance. If anomalies develop, diagnosing and rectifying problems may require site visits that take financial resources and personnel away from day-to-day operations.

The Cyber Threat to Digitally Native Assets

Now consider newer equipment — a digitally native compressor station, a smart meter, or an electrical substation. Programmable logic controllers (PLCs) have increasing resemblance to computers, and it’s not unheard of for a technician to solve problems by leaving a laptop on-site to run 24/7. Here, operational technology (OT) is constantly connected to information technology (IT) networks, the edge of the industrial internet of things (IoT). Connectivity allows technicians to monitor metrics, diagnose problems, and push software upgrades without site visits. A cyber breach would offer attackers access to the same tools. The same connectivity that enables rapid updates and efficient management results in exposure to a constant source of attacks.

The efficiency gains made possible by digital technologies will continue to drive industry trends — but companies that fail to defend the industrial internet of things will be left behind.
Many protective cybersecurity strategies rely on signature-based defenses. This method compares code against known threats, but is ineffective against never-before-seen zero-day attacks. Signature-based defenses rely on constant updates to the list of known threat signatures, and rapidly become outdated on an isolated system. Some innovative attackers now use AI-based or polymorphic approaches designed to fool signature-based defenses by disguising code without changing its effect.
The Endpoint Cyber Threat to the Energy Industry

Whether a company’s infrastructure is old or new, doing nothing risks outages. That risk increases over time, as attackers develop novel attacks focused on OT and find gaps in existing defenses. As new attack methods and specific threats become known, the only way defenders can deploy patches are as part of regular maintenance. Patching is increasingly challenging for physically distant assets — or during crises like COVID-19 or natural disasters — where regular maintenance tasks may lag behind an idealized schedule. The longer the interval between patches, the longer assets remain exposed to known risks.

Balance Sheets vs. Security

Energy asset owners need to reconcile the difference in life cycles between infrastructure hardware and the software that supports it. Infrastructure hardware can have a design life of 20–30 years, while software cycles are closer to 3–5 years. Some organizations may choose to accept escalating risk for aging, depreciated assets, but most companies operate fleets with many serviceable years ahead. To protect these investments, companies need appropriate cyber defenses — and need to plan for maintenance and support for the entire life cycle of the asset.

Today’s OT equipment must withstand frequent attacks arriving via three major threat vectors: mega-attacks, insider threats, and physical-digital attacks.

Bridging the Patching Gap

The first defense against each of these threat vectors is consistent, timely patching, grounded in robust threat intelligence sharing across the energy sector. However, even best-case scenarios will include intervals where patches have not yet reached isolated or intermittently connected sites, and novel threats may breach defenses before they become widely known. Businesses can’t afford to leave themselves vulnerable to outages, yet may struggle to deploy patches on a timely basis. Furthermore, unsupported operating systems in older assets may no longer receive any of these critical security updates.

Mature cybersecurity practices call for frequent software patches and planned defense in depth. Defense in depth hardens infrastructure against attacks that successfully breach initial defenses, building additional layers of protection to help contain and mitigate attacks.

Monitoring tools increase the chance of detection for attacks in progress. Operators with access to real-time site data can identify and investigate anomalies. Automated solutions can provide the perpetual vigilance needed to quickly recognize site conditions or user behaviors that may indicate trouble, and enable early interventions to prevent further spread of an attack.
Mega-Attacks
Attacks like WannaCry and NotPetya show that malware can spread rapidly and destructively within networks. The example of Stuxnet shows that these attacks can be designed to cross air gaps and activate when they reach specific, targeted machinery. Typically, mega-attacks derive from novel exploits, though for companies that fail to patch software, all assets will remain exposed even to known threats.

Insider Threat
Authorized users offer an attack pathway. In the attack on the compressor station, attackers gained entry through an ill-advised or mistaken click on a phishing email, then used this access to identify the specific critical infrastructure to attack. Even assets isolated from the internet are susceptible to insider threats. For example, technicians or contractors visiting sites may need to connect portable devices to perform maintenance. Defeating insider threats requires training personnel on good cyber hygiene, and monitoring sophisticated enough to detect changes in user behaviors, or distinguish between malicious and legitimate commands.

Physical-Digital Attacks
A few examples show that attackers can exploit digital pathways to physical systems. In 2015, attackers idled an offshore drilling rig for 19 days by altering its GPS system and thereby causing the entire platform to tilt several degrees from level.
Perpetual Vigilance with AI-Powered Endpoint Protection

The DeepArmor® Industrial Solution — Novel Endpoint Protection

Siemens Energy and SparkCognition’s new solution — DeepArmor® Industrial, fortified™ by Siemens Energy — addresses the energy industry’s challenge of securing vulnerable endpoint OT assets against cyberattacks. Based in artificial intelligence, DeepArmor® Industrial is a perpetually vigilant cybersecurity protection solution for the oil and gas, utility, and critical infrastructure industries, whether assets are isolated in the field or constantly connected.

Unlike existing endpoint solutions, AI-driven cybersecurity provides a layer of defense independent of threat intelligence, and eliminates the need for threat signature updates or specialized analysts to individually secure OT systems. Instead, DeepArmor® Industrial uses behavioral analysis to continuously monitor and detect new threats, resulting in both a first line of defense and immediate protection against previously identified and zero-day attacks on endpoint devices. This enables DeepArmor® Industrial to prevent or mitigate novel attacks still unknown to industry or law enforcement security professionals while reducing security costs to asset owners.

DeepArmor® Industrial can be installed on Monday, receive no updates all week, and remain an effective defense on Friday — even if entirely new threats emerge on Tuesday, Wednesday and Thursday. It sets a standard that other solutions can’t match with its intelligent defense and detection system, customized design, and site-specific deployment model.
DeepArmor® Industrial's AI-based defense system uses a predictive approach to prevent ransomware, viruses, and other advanced malware from executing. All data science models are hosted individually and execute on-device. These models leverage SparkCognition’s unique threat detection IP and methodology, which leads the industry with 99.9% efficacy against zero-day attacks. Because the solution does not use signatures, heuristics, or rules that require constant network connectivity, DeepArmor® Industrial is ideal for isolated networks in OT domains where system updates are performed manually. This improves threat detection accuracy while freeing cyber analyst time to focus on other critical matters.

**Perpetual, Intelligent Defense**

DeepArmor® Industrial offers customers the most compelling and sustainable AI-based approach to prevent industrial attacks in disconnected OT environments, including industrial HMIs, engineering work stations, engineering notebooks, data stores, and historians. It meets the highest standards of North American Electric Reliability Corporation’s Critical Infrastructure Protection (NERC-CIP) reporting and compliance standards.

DeepArmor® Industrial significantly reduces false positives and the costs to update physically distant assets. It vastly improves cyber resiliency from the first day of installation through pre-trained AI algorithms that detect and protect against known and unknown threats.
Siemens Energy–SparkCognition Value

- Surge support to close capability gaps
- Scale and control for fleet management
- Safety and operational risk consideration throughout the project
- Actionable insights to drive compliance and risk reduction

End-to-end deployment guarantee

Integrated solution development

Tailored service fit based on our deep OT and cyber expertise
Designing Defenses Appropriate to Risk and Workflows

To put DeepArmor® Industrial to work, the Siemens Energy service team starts by gaining a deep understanding of the unique organizational and technical needs within customer operational environments, including a network architectural review and design workshop to identify the most effective placement of AI-driven OT endpoint protection.

Tailored Defense Approach

Few sites in the energy sector are homogenous, so Siemens Energy helps customers evaluate assets to prioritize defense based on three broad risk criteria: connectivity, operational importance, and maintenance schedule. Connectivity affects the magnitude of exposure to attack. Operational importance indicates the severity of impacts on the business, if attacks disrupt normal function for that piece of equipment or system. The maintenance schedule indicates the length of intervals between defense updates, or hones the difficulty or expense of updates.

Siemens Energy keeps these considerations in mind when designing a deployment approach that best fits a customer’s endpoint protection needs. By examining the observed vulnerabilities, workflow, and maintenance practices specific to our customer’s sites and systems, Siemens Energy ensures applicable defenses appropriate to the risk represented by each piece of equipment which will vary based on its role and configuration within a site. For example, consider two identical servers purchased from the same manufacturer. The first gets installed at a small remote site, where it logs the activities of a pumping station. The second gets installed at a company’s flagship facility, where it supports a human-machine interface (HMI) critical to managing several parts of the plant. In this example, very tight restrictions on which applications can execute on the server would help secure the small site, but tight restrictions would disrupt workflows at the facility where the server provides HMI support for many tasks.

Deploying DeepArmor® Industrial

Based on the site-specific designs, Siemens Energy implements and configures Deep Armor with technicians validating that the system functions as intended. This phase typically takes place in parallel with planned maintenance, to minimize operational disruptions and maintain business continuity.

As an OT cybersecurity service provider, Siemens Energy understands the disruption to business that accompanies system shutdowns and interval patching of isolated OT assets. DeepArmor® Industrial is easily paired with additional Siemens Energy services to form a comprehensive patch and protect program. This comprehensive protection program can include access to Siemens Energy’s helpdesk, OT cybersecurity contextualized reporting, and updates and upgrades.

Siemens Energy’s deep understanding of the energy supply chain coupled with DeepArmor® Industrial’s protection provides customers a clear picture of their risk profile — both in terms of the identified vulnerabilities at their sites, and the operational impact that a successful attack could have exploiting these vulnerabilities. That analysis enables leaders to prioritize high-risk, high-value targets for defense, and to select defense architecture and technology appropriate to the site.

Siemens Energys’ support doesn’t end with the installation of DeepArmor® Industrial. Siemens Energy provides ongoing services necessary to continue capturing value from the deployment. Siemens Energy OT experts will review DeepArmor® Industrial alerts to provide contextualized reporting specific to the customer’s unique environment, helping understand the risk in their environment and identify actions to improve security.

AI Security for Human Intelligence

DeepArmor® Industrial, fortified™ by Siemens Energy, delivers a market-defining solution for today’s cybersecurity environment as attacks on the energy sector increase in frequency and sophistication. While the AI-based solution offers an unprecedented level of protection to the energy industry’s endpoint assets, nothing can replace human expertise. Many are struggling to adapt to the new normal which is why DeepArmor® Industrial’s service model focuses on building partnerships, implementing solutions, and planning with customers against the backdrop of constant siege.
Deploy DeepArmor® Industrial software to customer devices onsite through hands-on installation and configuration.

Conduct design workshop and review site workflows, planned maintenance, relative operational impact, and site connectivity to plan a deployment that meets customer needs.

Conduct design workshop and review site workflows, planned maintenance, relative operational impact, and site connectivity to plan a deployment that meets customer needs.

Service

4

Provide ongoing contextualized reporting based on DeepArmor® Industrial output data and deliver helpdesk and product support as needed.

Tune

3

Validate successful installation, customize as necessary, and confirm functionality based on initial requirements from design workshop.

Install

2

Deploy DeepArmor® Industrial software to customer devices onsite through hands-on installation and configuration.

Design

1

Complete End Point Protection Through the End Point Lifecycle
The AI Solution to Protect the Energy Industry’s Future

A chief information officer gets an email in the middle of the night. It’s a slightly puzzled report from the security operations center.

At one of the compressor stations, DeepArmor® Industrial detected an anomaly, interrupted the execution of the malicious code, prevented the system from being wiped, and flagged the incident for analysis. A technician returned to the site and realized they had inadvertently loaded malware onto the system during the previous day’s update. They immediately revert to an older software patch, and identify the malware that had infected their device. The technician notifies his colleagues to check for the newly identified malware, and shares the threat intelligence with the industry. Future patches will include defense against this new threat.
Contact Siemens Energy to learn more about how we can help provide unmatched OT asset endpoint protection with DeepArmor® Industrial and our entire portfolio of solutions.


For further information:

Cassandra Ljungmark
Global Portfolio Lead
Cassandra.Ljungmark@Siemens-Energy.com