Endpoint Protection

DeepArmor® Industrial, Fortified™ by Siemens Energy

siemens-energy.com

The threat landscape for critical energy assets is evolving…

Cyberattacks threaten the reliability of the energy supply chain, and pose a significant risk to the core business of energy companies. The need to defend multiple facilities that are physically remote can make necessary maintenance difficult and expensive.

Additionally, these threats are moving beyond information technology (IT) and are now directly targeting critical operational technology (OT) infrastructure. While the widespread adoption of digital technologies has improved safety, enhanced reliability, reduced emissions, and lowered costs, increasing connectivity has expanded the surface across which threat actors can execute cyberattacks.

Energy companies increasingly recognize that their likelihood of being attacked is nearly 100%, and that they must strengthen their agility and resiliency so they can respond when - not if - they are attacked. Attacks targeting OT are particularly important to thwart because they have the potential to threaten uptime and availability, the health and safety of staff and customers, and brand reputation.

The four most critical challenges in securing OT endpoints…

1. Under-maintained assets
Geographic isolation, air-gapping, and legacy assets lead to labor-intensive, expensive, and complex patching

2. Unauthorized use of assets
Fixed function assets should have specific and well-maintained safelists for what applications should be allowed to run

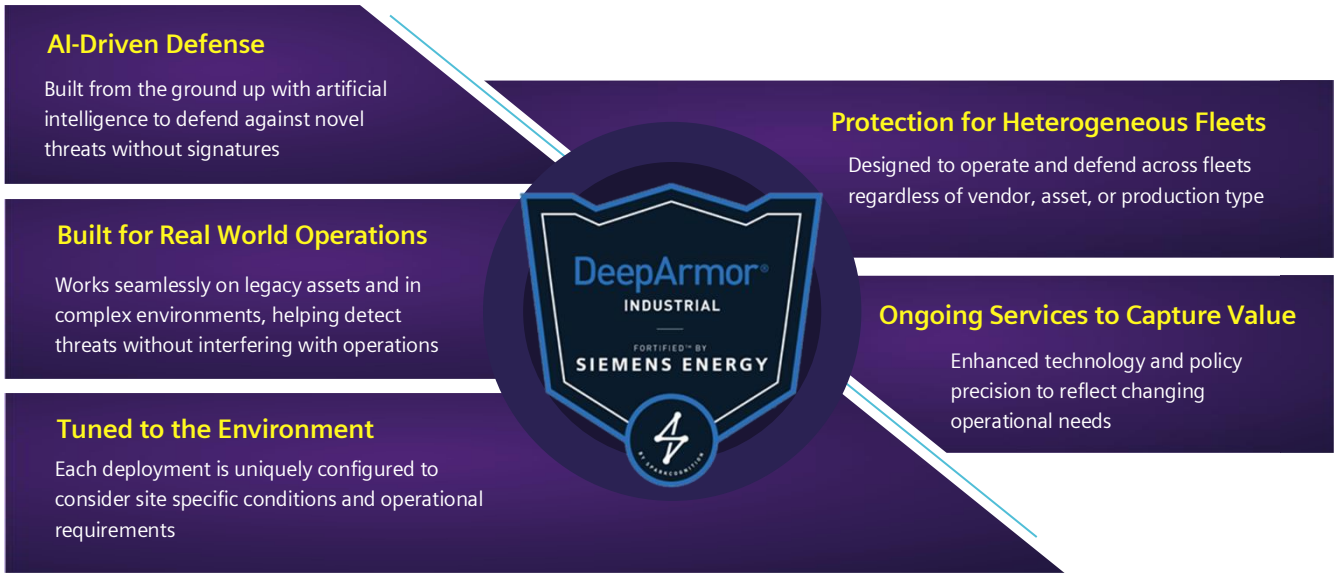
3. Novel threats
Zero-day attacks, which cannot be defended with basic or outdated tools, are crippling energy infrastructure

4. Increasing connectivity
Digitalization may help asset performance, but it exponentially increases the surface area through which threat actors can execute cyberattacks

DeepArmor® Industrial, Fortified™ by Siemens Energy provides a comprehensive answer for vulnerable OT endpoint assets

DeepArmor® Industrial, Fortified™ by Siemens Energy prevents ransomware, viruses, and other advanced malware from executing. It leverages pre-taught machine learning to differentiate between normal operations and anomalies without requiring access to your organization's network or data. This enables DeepArmor® Industrial to protect remote field assets, even if new threats emerge between updates, or attacks arrive at isolated sites before patches can be deployed.

DeepArmor® Industrial, Fortified™ by Siemens Energy is the first next-generation endpoint protection solution designed for OT assets and built from the ground up with artificial intelligence (AI) and the industrial customer in mind. The technology for this solution is provided by SparkCognition, an AI software company with market-leading efficacy. By directly addressing the most critical security concerns in industrial environments, Siemens Energy and SparkCognition are further enabling and accelerating industry-wide digital transformation efforts.



Traditional endpoint protection relies on frequent updating to maintain its effectiveness against emerging threats. DeepArmor® Industrial takes a more resilient approach using AI-based defenses. It can detect never-before-seen malware without the need for known patterns. The ability to deliver consistent and constant protection from malware for a range of endpoints, including legacy and isolated assets, all on a lightweight footprint designed for industry use is what differentiates this product from anything else on the market.

By relying on Siemens Energy, a trusted partner for OT cybersecurity solutions, you will unlock the most value from the technology because we tailor each deployment to your organization's unique requirements. Siemens Energy configures each endpoint agent to be specific to the asset it is protecting. The result is a Precision Defense™ solution designed for complex environments across vendors, asset functions, and operational requirements.

Siemens Energy is committed to working with your organization – guiding you on your journey to enhanced visibility, capable detection, increased security, and improved reliability.

Contact our Global Cybersecurity Portfolio leaders to learn how DeepArmor® Industrial, Fortified™ by Siemens Energy can help your organization secure its OT endpoint assets.

For further information:

Leo Simonovich
Vice President and Global Head
Industrial Cyber and Digital Security
Leo.Simonovich@Siemens-Energy.com

Stephen Hiser
Global Portfolio Manager
Industrial Cyber and Digital Security
Stephen.Hiser@Siemens-Energy.com

Cassandra Ljungmark
Global Portfolio Lead
Industrial Cyber and Digital Security
Cassandra.Ljungmark@Siemens-Energy.com

Published by

Siemens Energy Inc.
Controls and Digitalization
4400 N Alafaya Trail
Orlando, FL, 32826, United States of America