DARKTRACE

WHITE PAPER

How Darktrace Can Complement Industrial OEMs

CONTENTS - DARKTRACE INDUSTRIAL OEMS

What is an OEM?

Many OT networks utilize Original Equipment Manufacturer (OEM) machinery, with components usually procured directly from the OEM vendor or via a system integrator. OEM vendors, such as Siemens, Honeywell, Rockwell, and Emerson, supply equipment for ICS across a wide range of industries—including manufacturing, automotive, gas and energy, and electrical grids.

Maintenance of machinery is often written into the OEM contract and protected under warranty. These agreements are intended to outsource operational risk from the consumer to the manufacturers of the kit. More recently, some OEM contracts include cyber security solutions. Examples include Emerson's NSMs and IPD firewalls for DeltaV systems, and Siemens' Digital Twin, as well as certain solutions provided by Oylo, which was recently purchased by Rockwell.

To their credit, the OEMs have the specialized knowledge to select appropriate cyber security frameworks for their products, and they understand the unique requirements of their customer base, be it regulatory or otherwise.

The overall effectiveness of these solutions, however, hinges upon an organization having single-vendor ICS networks, and also maintaining networks that are well segregated from the Internet or from enterprise networks. These approaches accordingly remain limited in their capacity to address the reality of multi-vendor ICS, the increase in IT/OT convergence (such as IIoT and Cloud solutions), and the use of multiple access points such as vendor-only VPN access.

> Current ICS security technology focuses on reactive defense against known threats with limited capabilities to detect threats based on behavior rather than pre-defined indicators.

CISA, Securing Industrial Control Systems:
/ A Unified Initiative FY 2019-2023

Challenges Faced When Securing OEM Systems

Securing OEM systems involves a number of unique challenges that require a solution that goes beyond securing specific OEM products in isolation:

- Legacy hardware/software: OEM vendor solutions often contain unique operating systems, software, and hardware. Long-running contracts may mean widespread use of legacy machinery that is challenging or impossible to update.
- Proprietary protocols: Proprietary protocols are used by many OEMs. By developing their own protocols, OEMs gain the ability to place restrictions on the use of the protocol, as well as to change the protocol unilaterally. Specifications for proprietary protocols may or may not be published, and implementations are not freely distributed. Proprietors may also enforce restrictions through control of the intellectual property rights, for example, through enforcement of patent rights, or by keeping the protocol specification a trade secret. The use of these protocols provides ongoing challenges to integration with other security tools such as SIEMs or third-party NSMs.
- Security configurations: OEM security configurations are often unique and poorly documented. This lack of visibility can lead to unseen gaps in the broader security strategy, opening up the door to vulnerabilities or leading to a lack of successful coordination when responding to an incident.
- EDR compatibility: The vast majority of ICS equipment cannot be secured using Endpoint Detection and Response (EDR) solutions. Without a detection and response solution in place, an attacker that breaches protections can easily go unnoticed, and an attack likely will go unnoticed until it affects operations to a noticeable degree. Examples include high-profile attacks such as Triton, and advances in C2 methodology and polymorphic malware are driving up the stealth and speed of attacks.

> Cybersecurity is essential to the safe and reliable operation of modern industrial processes.

NIST
/ Guide to ICS Security

- Static defense: OEM vendors are manufacturing experts, but not cyber security experts. Solutions based on a) asset management b) network security monitoring that only provides partial coverage and c) signature-detection are a good starting point for passive defense, but do not protect against the most sophisticated threats, such as novel 'zero-day' malware and advanced persistent threats (APTs), which consistently target critical national infrastructure alongside global suppliers and manufacturers. Given that publicly known ICS attacks such as Triton and Havex started in IT networks and moved laterally into OT, the use of Industrial-specific security solutions does not reflect the true nature of real-world attacks.
- Limited coverage: Starting defense in the control system isn't sufficient. If the attacker has already reached these systems, they have achieved persistence, and so the opportunity to stop the attack from doing damage will have already passed. Security teams accordingly need full visibility of the network, rather than just into OEM subnets.

As with IT networks, OT networks are best defended by combining a foundational set of static defenses with adaptive defense – that is, adaptively identifying deviations indicative of an emerging attack. Adaptive defense can be achieved with Self-Learning Artificial Intelligence (AI), which gains a deep understanding of every detail of your industrial environment to understand normal behavior for all your bespoke OT and IT/OT ecosystems. By knowing what normal looks like, it can detect unusual activity and take targeted action to stop emerging threats.

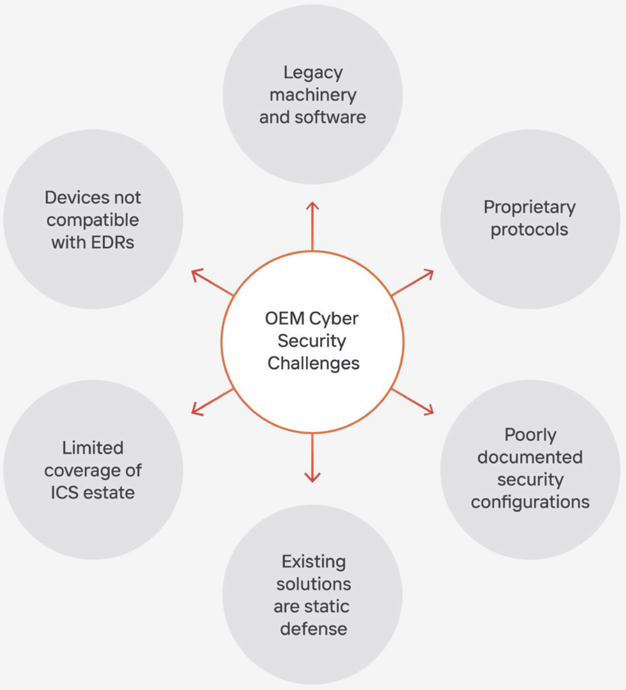

Legacy machinery and software
Devices not compatible with EDRs
Proprietary protocols
OEM Cyber Security Challenges
Limited coverage of ICS estate
Poorly documented security configurations
Existing solutions are static defense

Figure 1: Some of the challenges faced by the cyber security community with OEM networks and devices

Securing ICS Estates with a Flexible Platform Approach

The Darktrace Cyber AI Loop allows security teams to defend multiple parts of an organization's estate, including industrial, enterprise, SaaS, cloud, and email. By processing all traffic and activity on a granular level in a protocol- and technology-agnostic capacity, Darktrace provides full visibility, actionable insights, continuous detection and, where appropriate, autonomous response for diverse and complex cyber-physical ecosystems.

Within this platform, the Darktrace Cyber AI Loop can be configured to defend the entire infrastructure, all the way down to Level 1 devices in the Purdue model, and indirectly into Level 0. It can also be configured to cover just some of an industrial network; for example, it can be set to defend only Purdue model Level 3 devices and above, or just the most critical control subnets within a wider SCADA system. This flexibility allows the Cyber AI Loop to defend an organization's network while being sympathetic to OEM requirements.

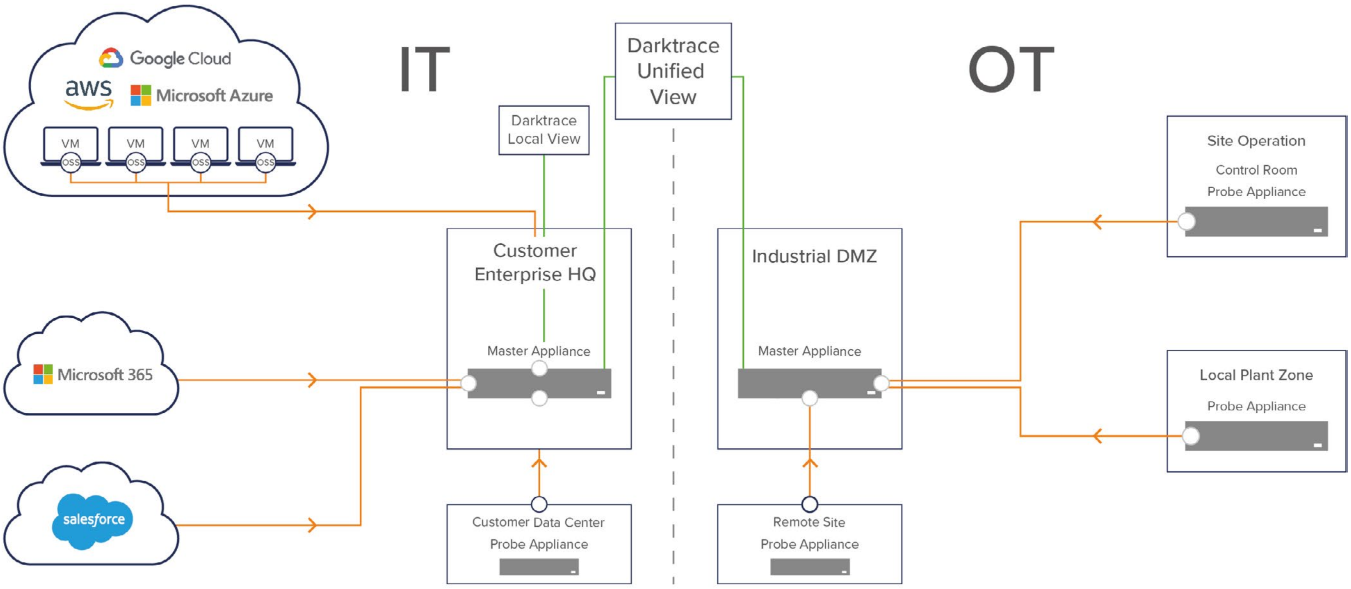


Figure 2: Darktrace defends multiple levels of an organization's infrastructure

How Darktrace Can Defend OEM Networks

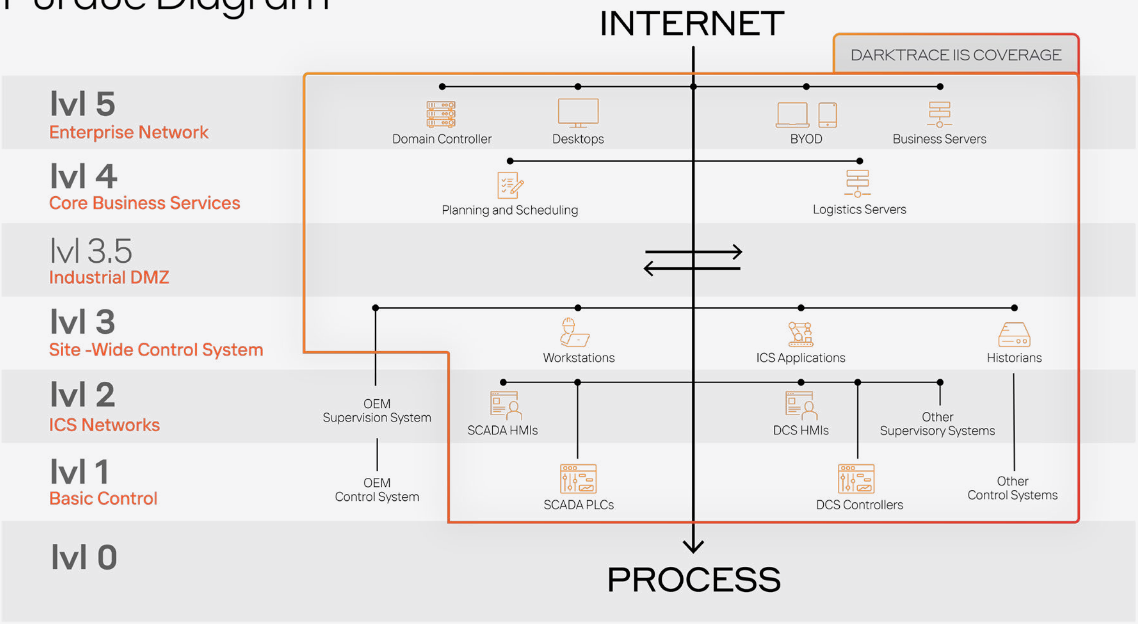
Darktrace can defend OEM networks in many scenarios in which security provided by OEM vendors can't provide comprehensive coverage:

Scenario 1: Network Traffic is not available

An OEM may be unable to provide access to data mirroring. There are several situations that could cause this scenario. Firstly, legacy switches may not be configurable to offer SPAN sessions without risking the integrity of the original traffic and introducing an operational risk. Secondly, an OEM may restrict access to raw network traffic from their subnets as part of the OEM contract and warranty.

In both scenarios, Darktrace can provide coverage at a higher Purdue Level, defending traffic into and out of the OEM ICS networks, functions of the control system that are not OEM specific, and enterprise networks. Darktrace can then expand coverage at the next maintenance window as switches are updated, or when agreements can be made with OEMs to gain access to network traffic. It is important to note that these SPAN sessions are already widely used by OEMs, with SPANs routinely provided to operators for scenarios such as predictive maintenance and safety monitoring solutions.

Purdue Diagram



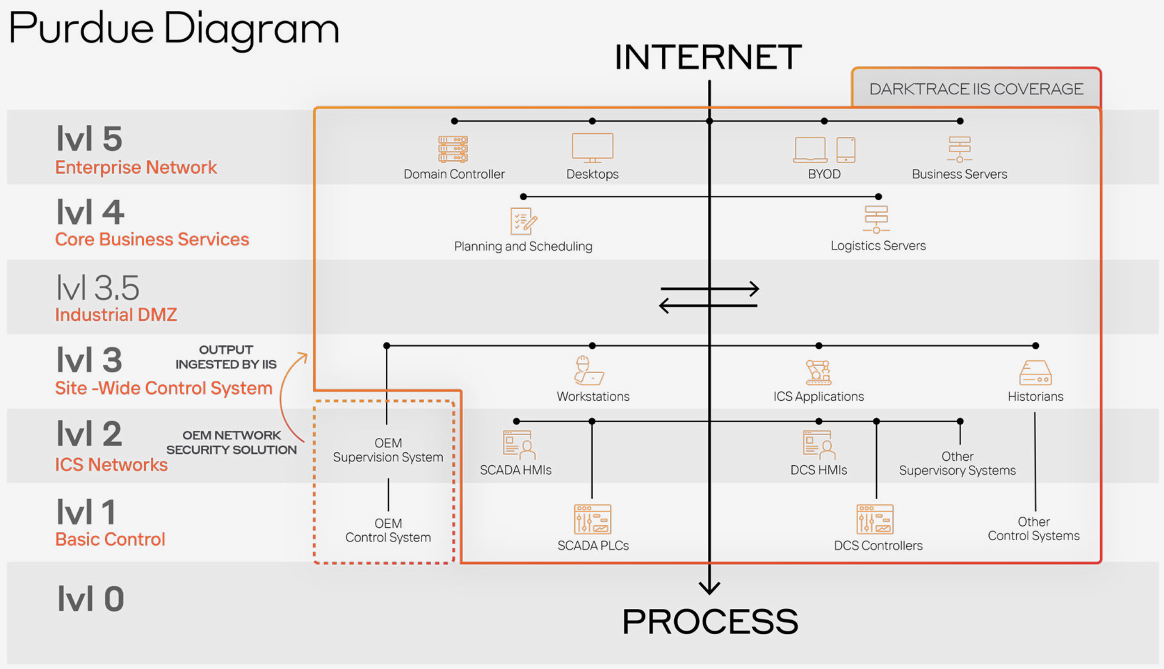
Scenario 1: Darktrace defends the wider ICS estate when network traffic is not available from OEM subnets

Scenario 2: OEM supplied security solution

Darktrace can seamlessly integrate with other security solutions. By ingesting the log-based output of OEM security solutions such as NSMs, Darktrace can perform AI analysis on the data and learn patterns of life. It means the security of OEM subnets can be incorporated into the security of the wider estate while respecting any OEM requirements and restrictions.

Using AI to understand the output of signature-based NSMs can help prevent alert fatigue. Darktrace is able to learn the pattern of alerts, determining which represent false positives or low-level misconfigurations, and highlight the most significant events which may indicate a new compromise or ongoing breach. While not as effective as deploying AI on the raw data, this adds some of the general benefits of Darktrace's technology on top of the OEM's techniques, and it also provides a way to incorporate activity within OEM areas into the larger and more comprehensive reports of Cyber AI Analyst.

An alternative arrangement can share data and workflows between Darktrace and complementary technologies such as PAS CyberIntegrity or SecurityGate. Direct integration between solutions covering differing aspects of an overall cyber security framework saves analysts time and reduces complexity.

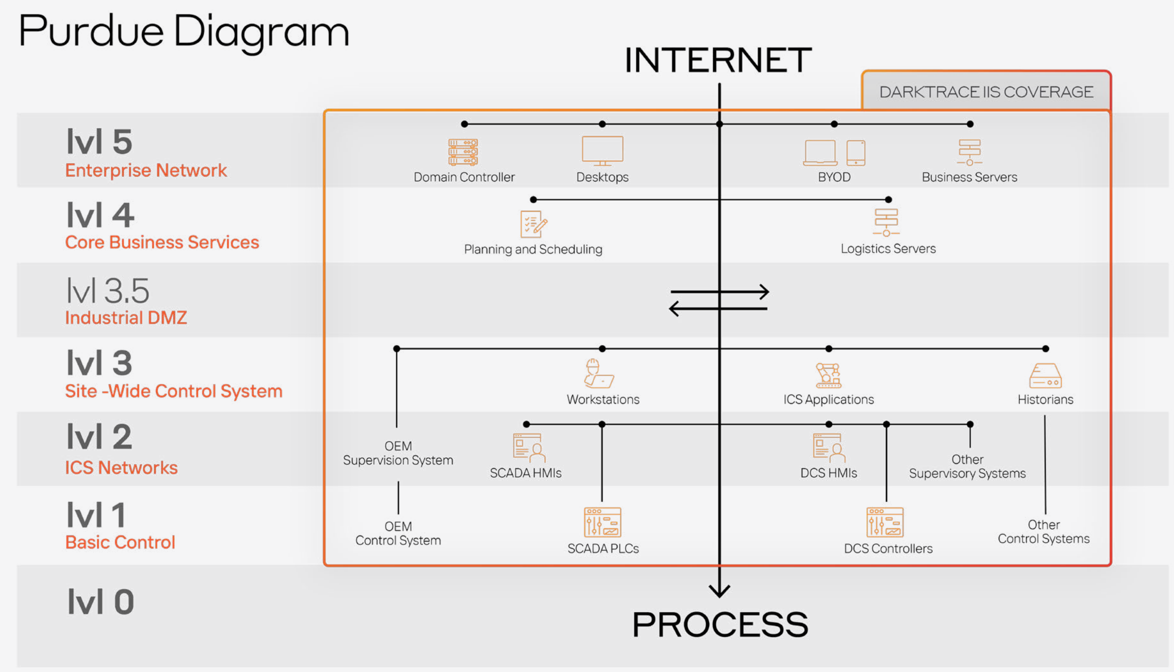


Scenario 2: The Darktrace Cyber AI Loop ingests output from OEM security solutions in order to defend the whole estate

Scenario 3: Proprietary protocols

Darktrace passively monitors network communications, a process which is automatically configured to be protocol- and vendor-agnostic. If an OEM using proprietary protocols is able to provide raw network traffic SPAN'd from a managed switch, Darktrace is able to build a pattern of life based on metadata. This data includes parameters such as time of connections, duration of connections, data transfer volumes, TCP ports, and connectivity patterns.

The challenge of proprietary protocols is similar to the challenges faced by recent masking techniques used by malware authors with encrypted C2 channels and lateral movement connections. Darktrace is well equipped to overcome these challenges, as demonstrated by its recent detections of the Sodinokibi ransomware strain. Depending on the OEM, some level of information from inside proprietary protocols may also be permitted and available for deeper analysis. By building a pattern of life based on metadata, however, Darktrace is easily able to complement Rockwell, Honeywell, Yokogawa, Schneider Electric, Emerson, and Siemens solutions.



Scenario 3: Darktrace defends the whole ICS estate, using metadata to build patterns of life for subnets which utilize proprietary protocols

Conclusion

As demonstrated throughout this report, OEM vendor requirements in ICS networks can result in unique cyber security challenges. Fortunately, the Cyber AI Loop accommodates these demands, providing capabilities such as passive monitoring of proprietary protocols, ingestion of OEM security solution output, and visibility of connections in and out of subnets when internal network traffic monitoring is not possible.

By complementing OEM security strategies that are put forth by the vendors, solutions provided by Darktrace Self-Learning AI allows for full coverage of the cyber-physical ecosystem, significantly reducing the risk of attackers reaching sensitive parts of the ICS network.

> Enterprises that require a cybersecurity solution for IT, OT, and physical environments will find Darktrace an effective tool for real-time advanced threat detection.

Earl Perkins
/ Managing VP, Gartner

KEY TAKEAWAYS

- Multiple factors compound the challenges of securing OEM systems
- OEM-supplied security solutions lack AI's adaptive defense
- Darktrace Self-Learning AI can complement OEM security in a variety of contexts
- By doing so, Darktrace augments the broader ICS security strategy

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,100 organizations globally from advanced cyber-threats.

Scan to
LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com

darktrace.com