DARKTRACE + XAGE JOINT SOLUTION

DARKTRACE

Enhancing Zero Trust Access Control with anomaly-based threat detection

KEY BENEFITS

- Prevent cyberattacks at every stage of the attack chain, anywhere in the IT/OT Environment
- Gain visibility, access control, and attack prevention in a simple, interoperable platform
- Enrich Darktrace modeling and visibility to accelerate detection
- Better informed anomaly detections to assure timely, precise response
- Inclusion of high-quality Xage data in Cyber AI Analyst investigations

Zero Trust in OT, IT, and Cloud Environments

The zero trust security model is gaining popularity among organizations pursuing digital transformation and adapting to the shift to remote workforces. It shifts focus from traditional network security perimeters to prioritizing identity and facilitating secure, distributed access from any device, at any time.

Implementing a zero trust model in interconnected enterprise IT and Operational Technology (OT) environments is challenging because OT devices are proprietary, highly distributed, and often not inherently designed to interoperate with modern security technology. While cybersecurity and IT teams move to modernize security, OT security professionals are concerned with zero trust initiatives disrupting operations. The joint solution of Darktrace/OT and Xage Security makes it simple and undisruptive to adopt a dynamic approach that assumes breach and verifies access privileges intelligently, while restricting access and operations accordingly.

Now that industrial assets are commonly connected to IT systems, OT security professionals are faced with the challenge of defending against threats that can come in from IT networks, making zero trust security an important aspect of securing OT assets.

With the right solutions in place, OT environments can begin to develop a zero trust security model that helps them protect systems across plants and remote sites by defending against unauthorized access, lateral movement, and speeding up incident response.

xage SECURITY

About Xage Security

Xage is the first and only zero trust real-world security company. Xage's solutions and services accelerate and simplify the way enterprises secure, manage and transform digital operations across OT, IT, and cloud. Xage products include zero trust access management, zero trust remote access, and zero trust data exchange, all powered by the Xage Fabric. Xage also offers Cybersecurity Services, which deliver expert design, implementation, and support services to accelerate the adoption of proactive cyber-defense and underpin secure digital transformation.

Darktrace/OT + Xage Security Enhancing Zero Trust

Darktrace enhances zero trust postures to identify and mitigate unpredictable cyber threats, providing a layered security strategy that adapts to evolving business and workforce needs.

Darktrace integrates with Xage to modernize threat detection in zero trust remote access contexts. Xage enriches Darktrace/OT's analysis by adding identifiable credentials to assets monitored by Darktrace/OT.

How It Works

The integration allows Darktrace to ingest audit logs from Xage which highlight what user credentials were seen on which devices connecting to Xage Nodes. Events produced by Xage logging will be associated with a device of the same IP within Darktrace/OT.

If you are a Xage customer and add Darktrace/OT

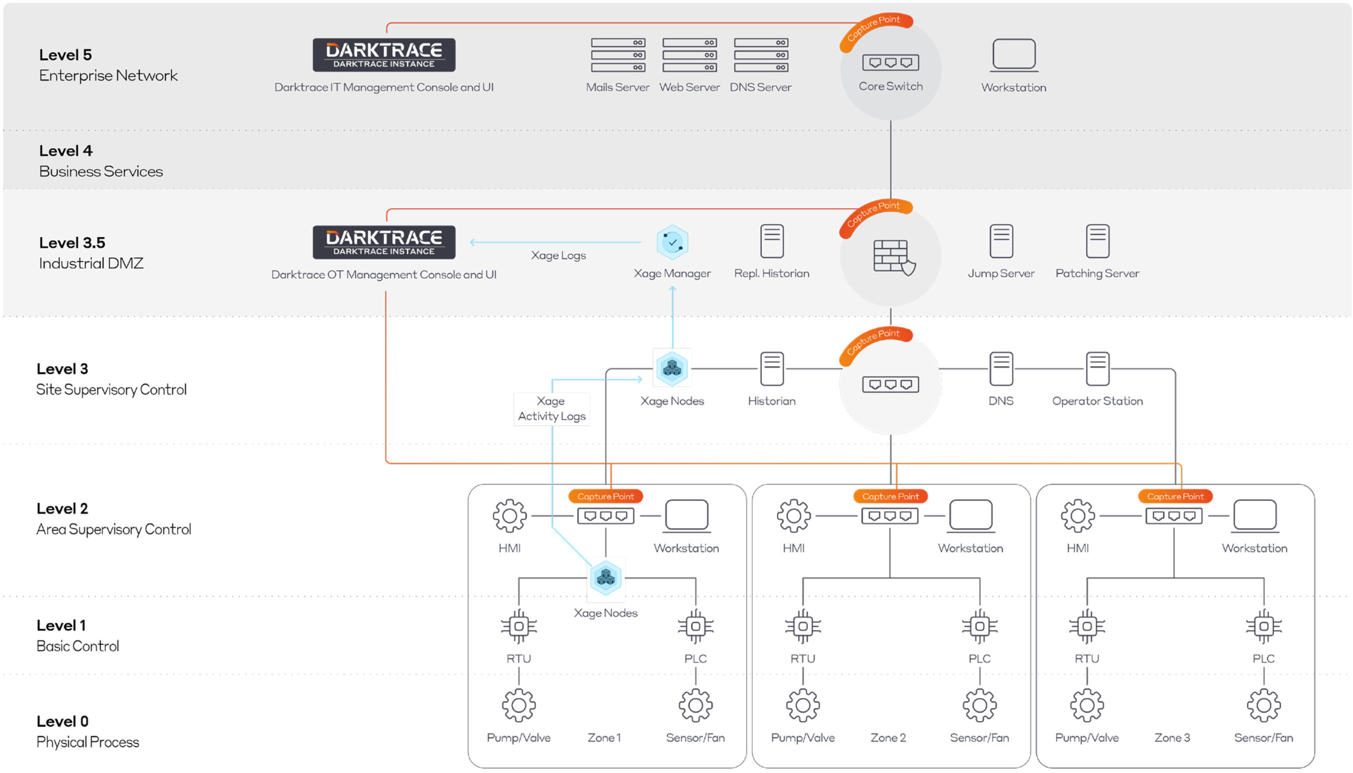
With Darktrace/OT users gain a layer of protection behind Xage in the form of anomaly based detection.

If you are a Darktrace customer and you integrate Xage

Darktrace customers would receive a layer of protection via Xage's zero trust access control, which can enforce granular, instant access restriction to targeted devices and improve Darktrace's tracking capabilities.

Use Case: Stopping an Insider Threat

Darktrace/OT natively detects the lateral movement while Xage Nodes will enrich Darktrace, being able to identify what the user credentials are behind that activity. Darktrace/OT alerts the security team about the suspicious remote user's behavior. Xage and Darktrace RESPOND/OT are then able to react and sever the user's remote access.



Xage fabric collects logs at every level of the Purdue model and collects them at the central Xage Manager (can be hosted in Enterprise or in industrial DMZ).

Xage Broker forwards the Xage audit logs to a Darktrace instance.

Darktrace processes the received logs and enriches its environment with observed credentials to provide more context on the monitored traffic.

About Darktrace Services

Darktrace is committed to ensuring that you receive the maximum value from our world-class Self-Learning AI technology and expert analysts. Our bespoke service options can be customized around Darktrace's Cyber AI Loop to uplift and augment your security teams. Services are delivered by Darktrace's dedicated Cyber Analysts, Cyber Technicians and our 24/7 SOC operation, comprised of experts in threat analysis and risk mitigation. Most importantly, these offerings are crafted based upon our extensive experience working with thousands of diverse customers – it is this expertise that allows us to provide services that are tailored for your organization. **Terms and conditions apply; for additional information about this service, please refer to the service definition.**

Scan to
LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

info@darktrace.com

darktrace.com