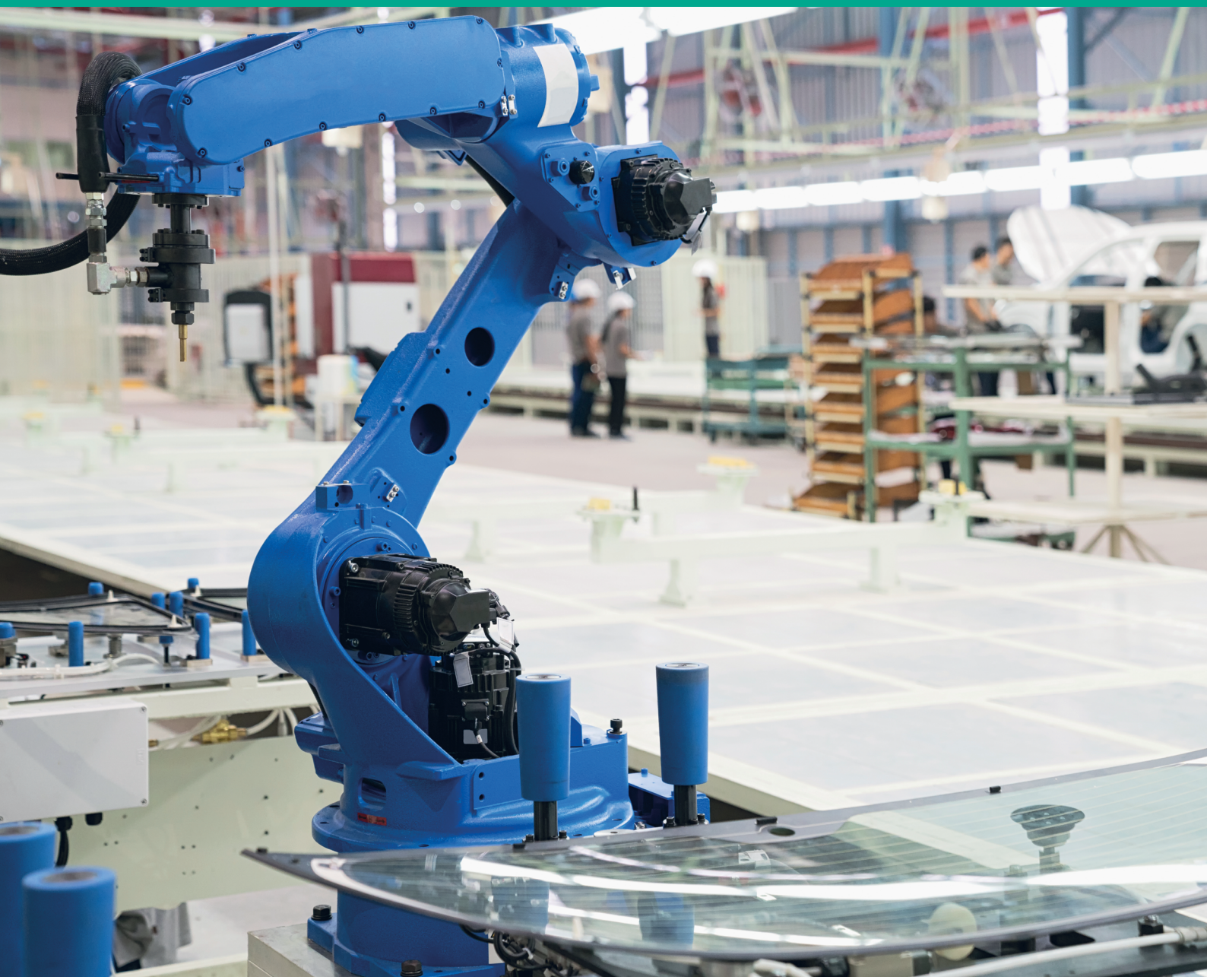

Kaspersky Industrial CyberSecurity защищает AGC

agc-automotive.com

tomorrow-connect.com

Автомобилестроение

- Год основания: 2003
- Доля рынка автостекол: около 23%
- Использует решение Kaspersky Industrial CyberSecurity с 2016 года

Компания AGC поставляет компоненты автопроизводителям, и для нее крайне важна непрерывность бизнес-процессов. Поэтому для защиты AGC выбрала решение Kaspersky Industrial CyberSecurity.

AGC Glass Germany GmbH с 2003 года поставляет автомобильное стекло таким ведущим производителям, как BMW, Volkswagen, Mercedes-Benz, Volvo и Opel. На предприятии компании в Вегберге (рядом с Мёнхенгладбахом, Германия) работают 150 человек. AGC входит в состав Asahi Glass Company – японской группы, являющейся крупнейшим в мире производителем стекла, обеспечивающим 50 000 рабочих мест в 20 странах мира.

AGC Glass Germany GmbH обрабатывает стекло для автомобилей, изготовленное на других предприятиях группы, в соответствии с конкретными потребностями клиентов: например, устанавливает на стекло системы обогрева, датчики дождя или уплотнители. После этого компонент поступает на производство различных автомобилестроителей.

«Мы выбрали своим партнером „Лабораторию Касперского“, поскольку оказалось, что Kaspersky Industrial CyberSecurity можно развернуть без прерывания наших операций, и к тому же это решение совместимо с нашими системами управления и с Tomorrow Connect.»

Ян Хоубен, директор завода
AGC Glass Germany GmbH

Стабильность процессов – приоритет компании

Для предприятий с крупносерийным стандартизированным производством, таких как AGC Glass Germany, стабильность процессов имеет критическое значение. В случае задержки производства или, еще хуже, полной остановки производственных линий клиенты могут потребовать не только возмещения за аннулирование заказа, но, во многих случаях, и уплаты значительных договорных неустоек. Для предотвращения таких ситуаций AGC использует платформу Tomorrow Connect, соответствующую стандартам промышленности, и инженерные приложения для нее (eApp), что позволяет собирать информацию о стабильности процесса и отклонениях от заданных значений в режиме реального времени.

Это решение разработано партнером «Лаборатории Касперского» Tomorrow Labs в сотрудничестве с институтом Fraunhofer IPA и машиностроителями. Платформа собирает, связывает и визуализирует данные оборудования и ERP-систем на разных площадках предприятия, объединяя таким образом информацию из различных отделов в масштабе компании, что позволяет добиться прозрачности и автономности производства.

Безопасность
Сочетает общие технологии кибербезопасности и методы, разработанные специально для промышленных сред

Управление рисками
Предотвращает ситуации, в которых требуется уплата договорных неустоек

Контроль
Выявляет неавторизованные устройства, обеспечивая максимальный контроль промышленных сетей

IT-безопасность для промышленных систем управления

Несмотря на все преимущества, объединение такого большого количества производственного оборудования в единую сеть приводит к возникновению новых уязвимостей. В случае атак возможны значительные финансовые и репутационные потери.

В прошлом атаки компрометировали отдельные компьютеры в офисах предприятий, а теперь злоумышленники способны повреждать целые производственные системы или даже постепенно снижать качество продукции – и при худшем раскладе это обнаруживает только конечный клиент. Для снижения этих рисков компания AGC решила защитить свое производственное оборудование при помощи Kaspersky Industrial CyberSecurity.

150
Сотрудников

10
производственных линий под защитой

Kaspersky Industrial CyberSecurity

Решение Kaspersky Industrial CyberSecurity разработано специально для защиты критически важных инфраструктур и промышленного оборудования.

Решение использует широкий ряд общих методов борьбы с угрозами, таких как защита от вредоносных программ, создание белых списков и управление уязвимостями. Кроме того, оно обеспечивает контроль доступа к устройствам, благодаря чему клиенты могут отслеживать подключения к портативным устройствам хранения данных и периферийным устройствам.

«Решение „Лаборатории Касперского" видит, когда сотрудник подключает к нашей сети флэш-накопители, – поясняет Ян Хоубен. – Оно проверяет подключенное устройство по списку авторизованных флэш-накопителей, которые сотрудники имеют право использовать».

Эти стандартные возможности дополнены технологиями, разработанными специально для промышленных сред: такими как проверка целостности и семантический мониторинг команд управления процессами. Кроме того, Kaspersky Industrial CyberSecurity может работать в специальном режиме мониторинга, позволяющем обнаруживать кибератаки, операционные ошибки сотрудников и аномалии в промышленных сетях.

Десять производственных линий под защитой

Каждая отдельная производственная линия на предприятии AGC защищена решением Kaspersky Industrial CyberSecurity. Решение отслеживает события на всех уровнях сети и проверяет все действия. Kaspersky Industrial CyberSecurity немедленно оповещает компанию о любых аномалиях в производственном процессе.

«Решение Kaspersky Industrial CyberSecurity состоит из модулей, что позволяет адаптировать его к нашим особым потребностям и специфичным инфраструктурам, – добавляет Ян Хоубен. – Решение обеспечивает кибербезопасность на всех уровнях сети, не нарушая непрерывности наших технологических процессов».

Kaspersky®
Industrial
CyberSecurity

Подробнее о решении: www.kaspersky.ru/ics

#KasperskyICS

www.kaspersky.ru