guardsix

Safeguard business

Made in Europe. Open platform. Complete visibility.

OTD BİLİŞİM
GLOBAL VAD

About Guardsix

Safeguarding society in a digital world

Headquartered in Copenhagen, Denmark

SOC Type II attestation

Cybersecurity Made in Europe

Privately held by European investors.

OTD BİLİŞİM
GLOBAL VAD

Why security operations hit the wall

Alert overload and false alarms

SOC analysts face an endless barrage averaging 4,484 alerts per day, 40% of which are false positives1. Critical alerts inevitably get missed.

Understaffed and burning out

69% of security teams are understaffed and struggling, and 71% of analysts are experiencing burnout2. Constant fire-fighting with limited staff has led to alarming turnover rates.

Siloed tools and poor visibility

Disjointed security tools (separate SIEM, NDR, EDR, etc.) don't share data, leaving blind spots in coverage. Lack of correlation means even trivial events can generate floods of alerts.

Manual drudgery

64% of analysts spend over half their time on manual tasks like compiling reports and basic triage instead of true threat hunting. It not only wastes expertise, it saps morale from security teams2.

Rising threats &new regulations

Advanced threats outpace legacy tools

New, sophisticated, and innovative attacks that siloed monitoring can’t catch appear every day.

Regulatory pressure

New laws following the EU’s NIS2 Directive have made security a board-level accountability issue, explicitly imposing liability on management for incidents.

Geopolitical instability

Now more than ever, organizations scrutinize where their most sensitive data is stored and processed.

OTD BİLİŞİM GLOBAL VAD

What could you achieve with straightforward security operations?

Efficiencies

- Automation and native integration to reduce alert fatigue, eliminate manual tasks, and focus on proactive defense

Compliance

- Simplified adherence to frameworks like NIS2 and GDPR
- Audit-ready reports and data handling aligned to regulatory mandates

Risk mitigation

- Real-time detection
- Full visibility across environments
- AI-driven insights to minimize dwell time and stop threats early

Data sovereignty

- Guaranteed access to data
- No one else has access to your data

OTD BİLİŞİM GLOBAL VAD

Why Guardsix?

Enhance threat detection and response

- Full visibility
- Reduced alert fatigue
- Automated incident response
- Threat hunting

Meet compliance requirements

- Pre-configured reports
- Compliance evidence
- NIS2 and GDPR compliance

Achieve data sovereignty and privacy

- European cloud providers
- On-premises solutions
- Cybersecurity made in Europe

Improve efficiency and save cost

- Multitenancy capabilities
- Unified platform
- Predictable licensing

Unlock smarter, faster and sovereign security operations

Close the detection gap

See with just one look if an incident belongs to a much larger attack. Guardsix graphically connects incidents with all their metadata, so you can instantly trace the attacker's activity and predict next steps.

Stay in control of your data

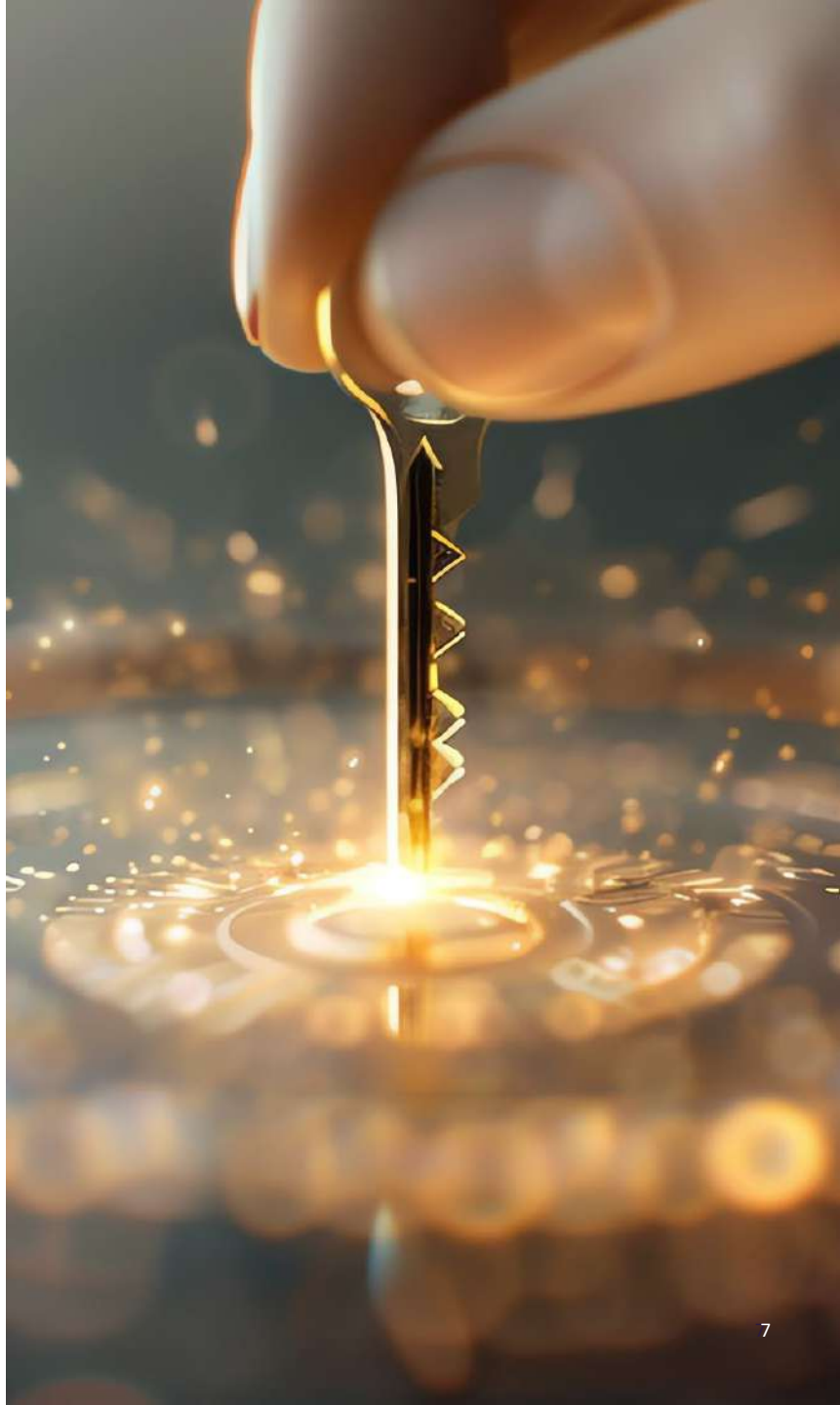
Store data in alignment with your needs for data sovereignty, protection and security.
You can choose an on-premises solution for maximum data control or deploy in a private or public cloud.

Get compliance-ready

Stay prepared for audits, comply with incident reporting mandates, and manage incidents.
You can track policy adherence, generate and export reports and monitor your infrastructure in real-time.

Scalable and future-proof

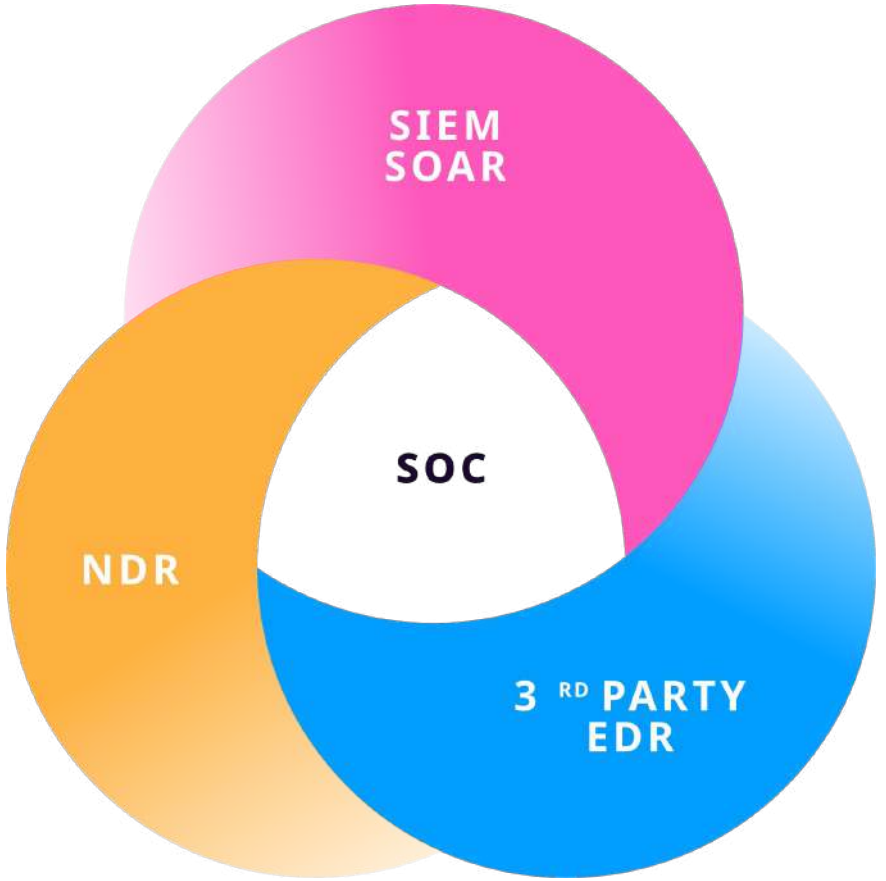
Guardsix scales as your data volumes grow, even with complex and distributed infrastructure. Guardsix integrates with leading security tools, whether cloud or on premise.



OTD BİLİŞİM
GLOBAL VAD

Complete visibility and detection

- Guardsix SIEM offers intuitive, high-powered analytics and incident response workflows.
- Guardsix NDR builds AI models of normal network behavior and spots anomalies across the network



- Guardsix's open platform integrates with major EDR tools to round out SOC visibility

OTD BİLİŞİM
GLOBAL VAD

Guardsix SIEM

High-fidelity alerts, rapid threat correlation, and built-in compliance reporting in one platform.

Centralized log intelligence

Ingest and analyze logs from across your entire IT environment (cloud, on-prem, endpoints, OT systems).

Hundreds of built-in detections

Pre-loaded with detection rules, anomaly use cases, and threat intel feeds curated by experts.

Compliance out of the box

Pre-configured compliance dashboards and alerts mapped to frameworks like NIS2, GDPR, ISO27001, PCI, etc.

Flexible deployment options

Available in sovereign cloud, on-premise, and cloud service.

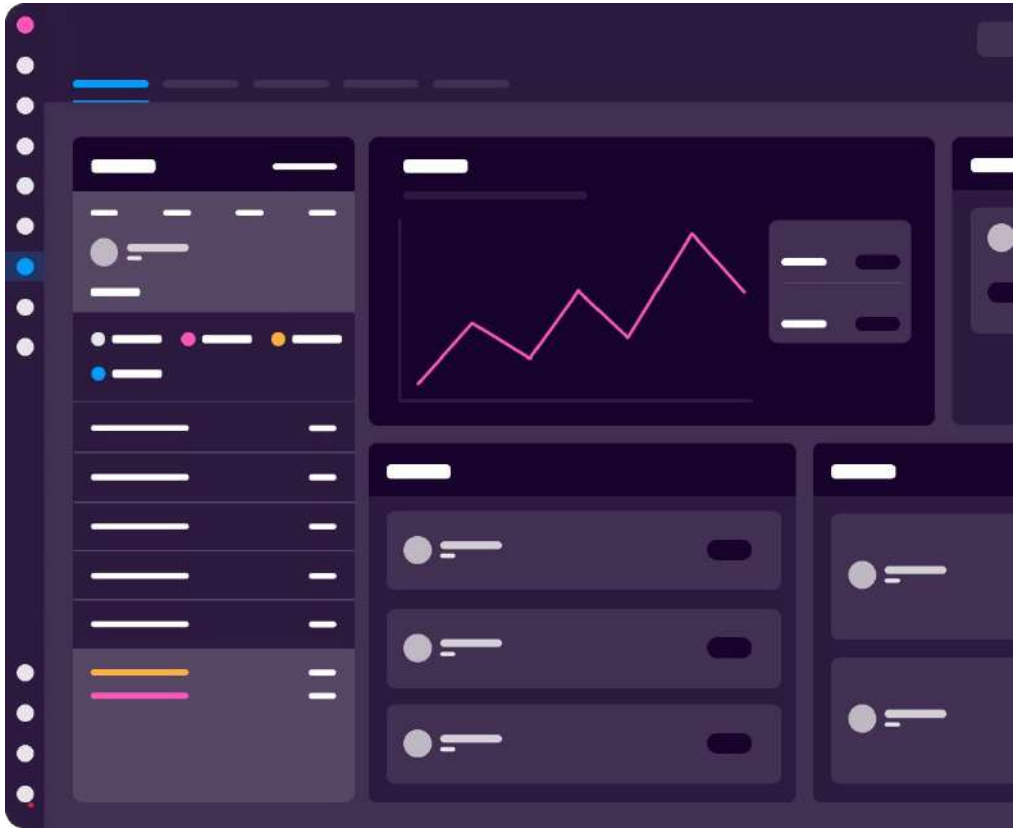
Cost efficient

Efficient data handling that doesn't need an army of admins to stay running, and a predictable pricing model.

OTD BİLİŞİM
GLOBAL VAD

Guardsix NDR

Deep, real-time visibility into network threats that evade logs and endpoints



AI sees threats other tools miss

AI and Machine Learning flag stealthy behaviors like lateral movement and data exfiltration in real time, even if the attacker has evaded endpoint or log-based detection.

Full-spectrum network visibility

Automatically discover and monitor network activity across IT, OT, cloud and SaaS environments.

Real time threat detection and response

Identify and respond to threats within milliseconds via automated responses to maintain uninterrupted business operations.

Reduce false positives and alert fatigue

Guardsix customers see up to a 90% reduction in false alerts.

Guardsix SOAR

Intelligent automation frees up analysts to focus on what truly matters

Orchestrated response at machine speed

Integrated across tools, SOAR playbooks instantly take action when threats are detected. 24/7/365, even when your team is asleep.

Jump start your automation with playbooks

A library of pre-built playbooks for common incidents means you don't have to build everything from scratch.

Consistent, lightning-fast incident handling

Triage incidents before your analyst gets involved, e.g. by identifying malicious IP addresses, hosts or hashes from services like Virus Total.

Analyst oversight and collaboration

Customizable approval gates keep your analysts in complete control even in highly automated playbooks.

Empowering critical infrastructure

NIS2 – ready solution

Compliance-ready

Dramatically simplify NIS2 compliance with pre-mapped controls and compliance use-case packs

24/7 SOC

Around the clock detection and response via automation and efficient workflows for lean teams

Protect IT & OT

Flexible connectors and NDR probes bridge the IT/OT security gap seamlessly

Sovereign solution

Keep your data inside country borders where you have complete control over it

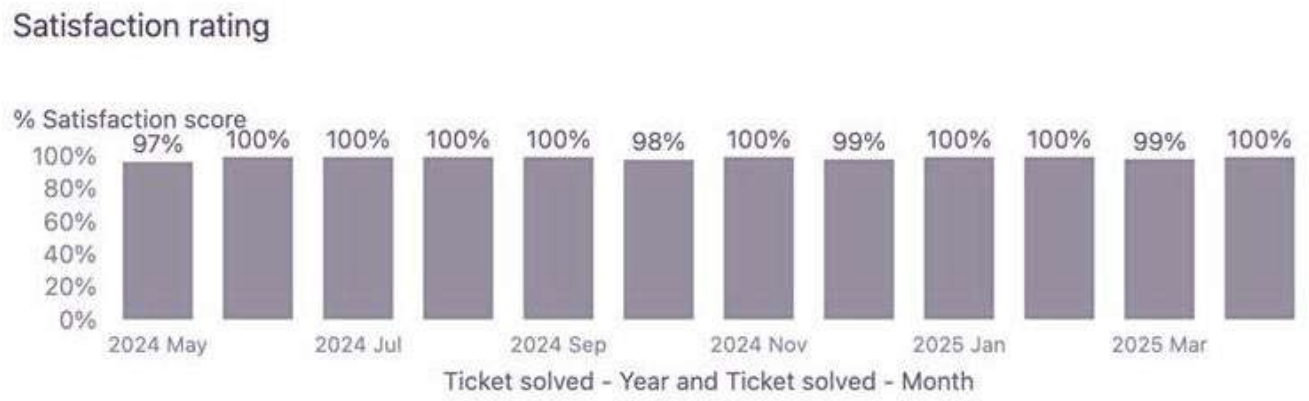
OTD BİLİŞİM
GLOBAL VAD

World class support

"Very satisfied with the customer support.

They explained the underlying issue, and followed up with a way to solve it with a workaround, much appreciated."

Well-resourced support available 24/7



MSSPs

Built for MSSPs

Enhance the differentiation of your service offering with Guardsix

Multi-tenant by design

Automation and native integration to reduce alert fatigue, eliminate manual tasks, and focus on proactive defense

Efficiency = Profitability

Take on more customers and provide better service with the same headcount

Data sovereignty

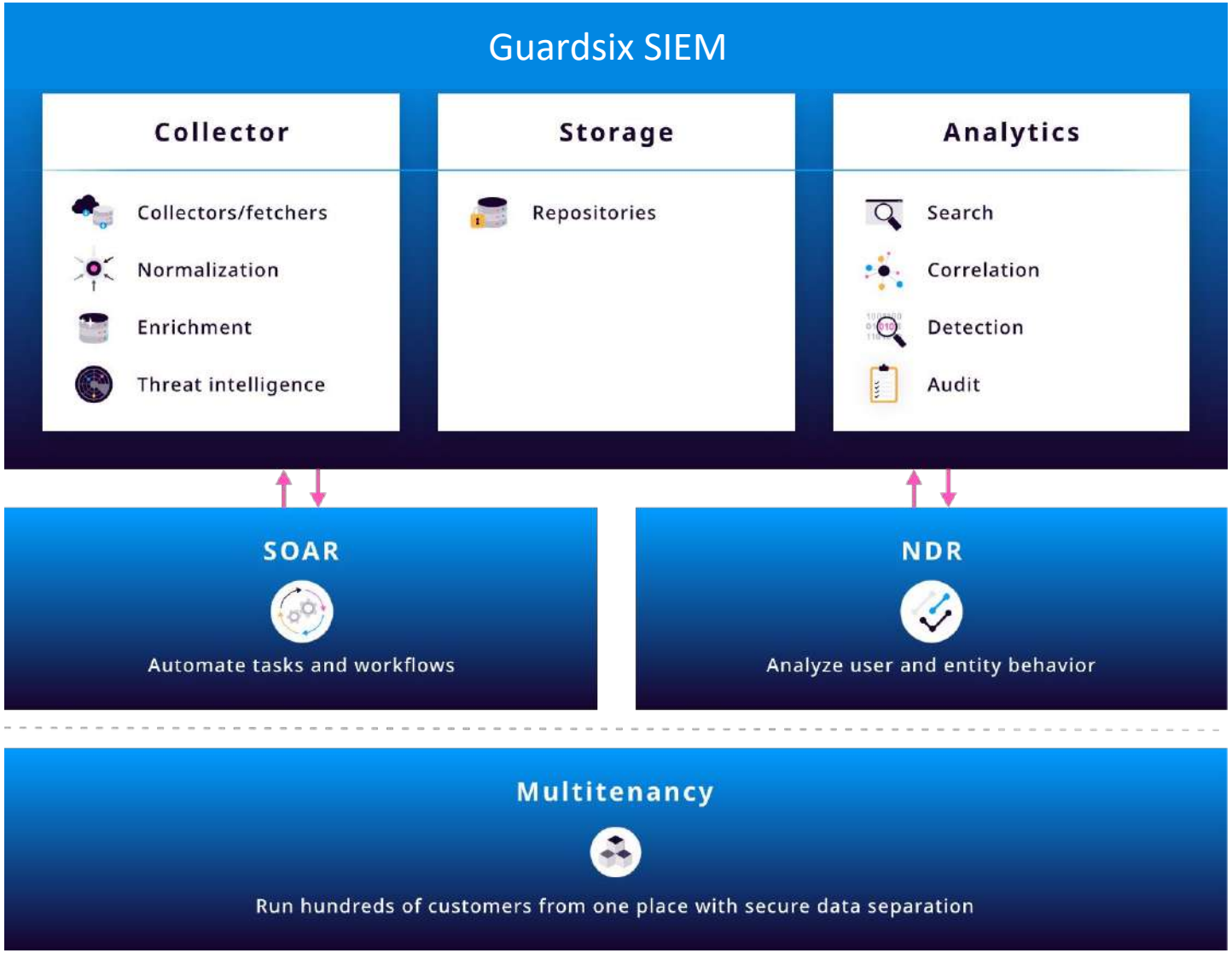
Satisfy clients by keeping data within local European borders.

Partner-centric support

As an MSSP, you're not just buying a product, you're entering a partnership.

A partnership beyond technology

- Expand services and drive revenue with strategic success plans.
- Uplevel expertise with training in threat detection with Guardsix.
- Get access to marketing funds to support your business plan.
- Share ideas and experiences with other MSSPs across Europe.


Guardsix SIEM
Collector
Collectors/fetchers
Normalization
Enrichment
Threat intelligence
Storage
Repositories
Analytics
Search
Correlation
Detection
Audit
SOAR
Automate tasks and workflows
NDR
Analyze user and entity behavior
Multitenancy
Run hundreds of customers from one place with secure data separation

Customer cases

OTD BİLİŞİM
GLOBAL VAD

Customer Case

OTD BİLİŞİM
GLOBAL VAD

BORYSPIL
INTERNATIONAL AIRPORT

Industry	Transport , Critical National Infrastructure
Location	Kyiv, Ukraine

THE CHALLENGE

Resource heavy setup

The previous SIEM platform was difficult to use and required significant infrastructure and human resources. Its deployment and maintenance needed specialized engineers, which slowed implementation and complicated operations. The licensing model, based on the number of events, made expenses less predictable.

Key problems

- Limited incident visibility and complex data analysis
- High hardware requirements, with multiple servers needed
- Difficulty forecasting costs due to the licensing model
- High complexity for small analyst teams
- Response automation (SOAR) required additional funding

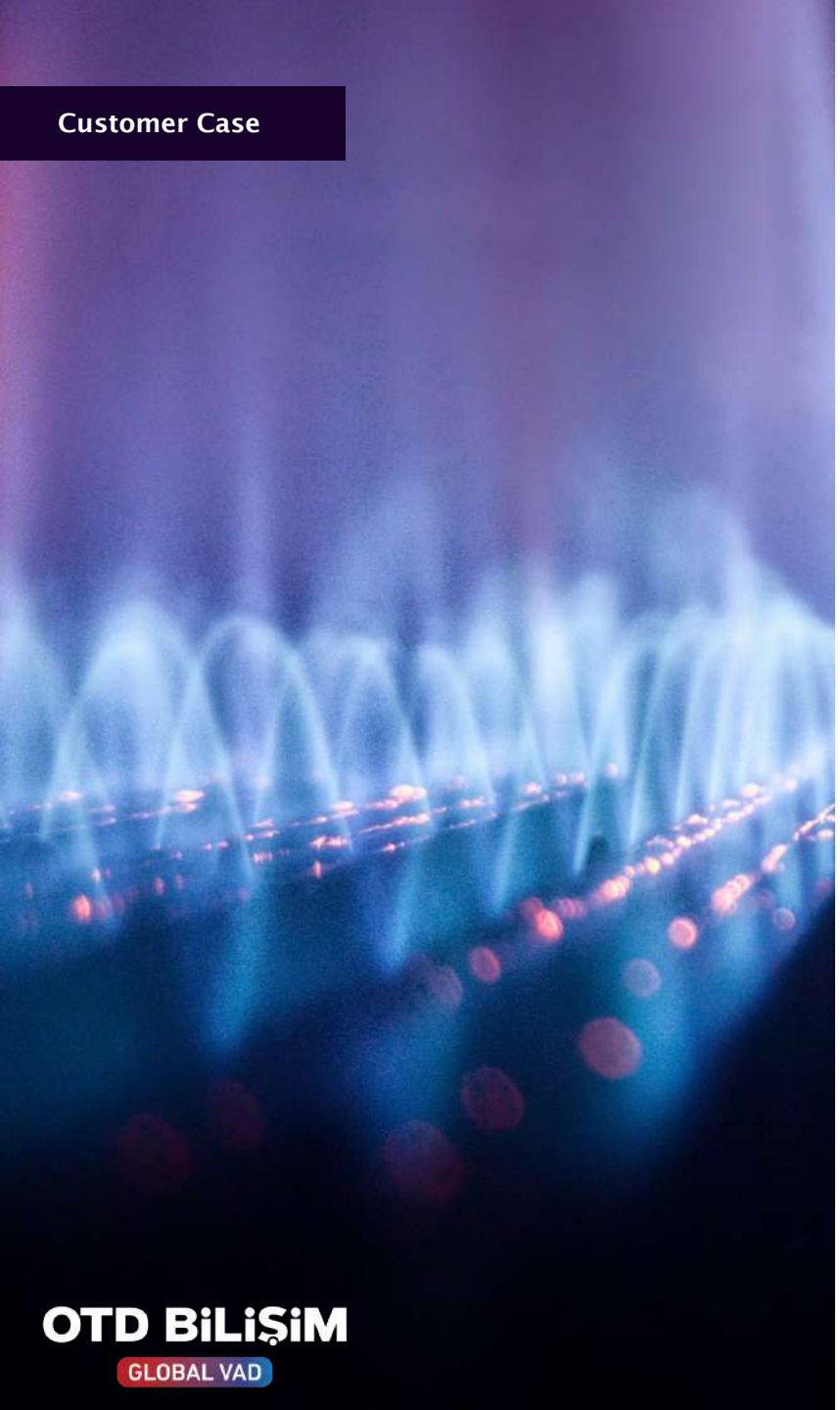
In the context of ongoing military aggression from Russia and increasing cyber threats, the company needed an easy- to-implement solution that would deliver immediate results without overloading the specialists.

BENEFITS

- Single-server deployment
- Node-based licensing, allowing predictable budgeting for years ahead
- Dashboards and analytics out of the box for quick data access
- SOAR readiness, for automated response
- Smooth integration with existing multi-vendor security infrastructure.

> The Guardsix SIEM solution impressed us with its ease of implementation and use. From day one, all our event sources were integrated into the Guardsix system without extra effort. Its convenient interface and transparent licensing model make it the optimal solution for our team.

Viacheslav Tretiak
Head of Information Security Department, Boryspil International Airport



Customer Case

OTD BİLİŞİM
GLOBAL VAD

BAŞKENTGAZ
Enerjinin Başkenti

Industry	Natural Gas, Critical National Infrastructure
Location	Ankara, Turkey

THE CHALLENGE

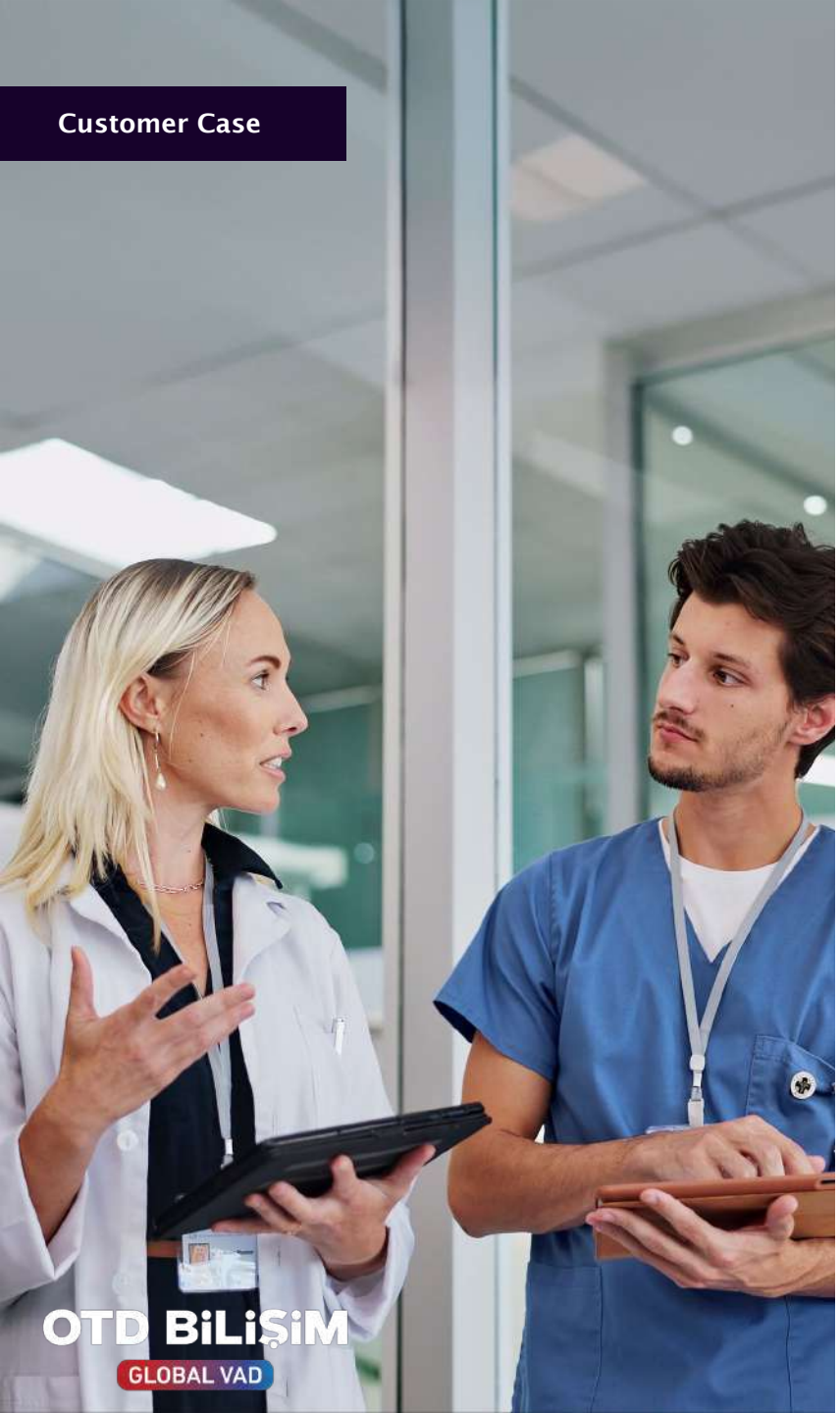
Long term log storage

Başkentgaz wanted to uplevel their log management and security processes. As a publicly traded company undergoing independent audits every three months, ensuring seamless log collection and retention was critical. Başkentgaz also required a solution that could provide long-term log storage while maintaining compliance with security policies. Managing VPN login and logout logs for remote employees was a particular concern, as it was essential to ensure effective access control and prevent unauthorized access.The company sought a scalable SIEM solution that could integrate seamlessly with various critical systems, including ERP, EDR, Proxy, Firewall, and IPS. The lack of a centralized monitoring system made it challenging to quickly respond to security incidents, create custom reports, and efficiently classify and normalize data.

BENEFITS

- Monitor all systems from a single point and respond quickly to security incidents.
- Flexibly create custom alarms, reports, and dashboards in addition to built-in ones, enhancing operational efficiency.
- Classify and normalize data according to user needs.
- Generate daily, weekly, and monthly reports. Integrate with most global products, providing flexibility in product selection.
- Instantly access needed information through fast and easy queries.

> We analyze global cyber threats and create dashboards in Guardsix additional security measures. This gives us extensive capabilities in threat observability.
>
> Guardsix functions like a search engine, making it easy to find the logs we need. The support team is highly competent, not only resolving issues but also explaining solutions, which aids in learning and self-improvement.
>
> Abdurrahman Polat
> Cybersecurity Expert, Baskentgaz



Customer Case

Region Värmland

Industry	Healthcare
Location	Värmland, Sweden

THE CHALLENGE

Protection of patient integrity

With 7,500 employees in hospitals and health care centers, the number of medical record views in Värmland quickly became unmanageable. Since the handling of medical records hadn't evolved significantly since 2006, and the data that needed to be managed from an increasing number of users and patients only grew, the old ways of working were due for an overhaul.

BENEFITS

- Smart reports for medical record views without care relation.
- Smoothless implementation across 16 departments within the region.
- Easy collaboration with other regions (Jämtland, Härjedalen, and Jönköping) that use the same medical records system.
- Knowledge sharing and faster onboarding for other regions through shared use cases and mutual input.

> The strength of the Guardsix solution is that we don't have to spend unnecessary time on investigating false positives and that we check all logs. Not only logs chosen at random. This way, we comply to the legal requirements of effective log auditing

Joakim Bengtzon
IT Security Manager

Customer Case

THE FAMILY BUILDING SOCIETY

Industry	Financial services
Location	Surrey, United Kingdom

TH E C H A L L EN G E

Efficient forensic analysis

The Family Building Society wanted to enable the retention of log data and effective forensic analysis of security and operational events.

At the same time The Family Building Society was going through the process of obtaining the Cyber Security Plus accreditation. To align with the requirements of the program and address the input received from security assessors, they needed a SIEM.

They also had to ensure that they had the necessary resources available to manage the system, the support and documentation to help them through the process, and the freedom to move to a managed service in the future if required.

BENEFITS

- Automated, real-time log analysis, replacing manual processes for faster insights.
- Centralized, optimized access to all log sources for manual inspection and event management.
- Time savings through a unified platform that removes the need to differentiate between log sources.
- Improved threat detection with quick setup of alerts and advanced threat intelligence integration.
- Flexible data ingestion, allowing comprehensive collection and analysis of logs from across the enterprise.

> We now think of Guardsix as a member of the IT Security team. It provides immediate answers to a lot of questions that we would have struggled to answer under a more manual system. We can take logs from everywhere that they need to be gathered and collate and analyze as much as we need, and the process of ingesting data is very open.

Andrew Ballard
Head of Technical Design & Delivery

600+ global customers

MSSPs

CNI

OTD BİLİŞİM
GLOBAL VAD

What our customers say about us

8COM CYBER SECURITY

"The efficient management of customers' SIEMs, the continuous development in close coordination with us as MSSPs, and the flexibility in architecture and data handling make the collaboration with Guardsix especially attractive for us."

Tobias Rühle, 8com (SIEM)

Telia Cygate

"Flexibility in technology is important for us, and Guardsix has always been really flexible in the past, and it is easy to talk to them, which is important."

Martin Spiik, TeliaCygate

METCLOUD
GET CONNECTED • CYBER SAFE

"We have partnered with Guardsix for many years because their SIEM and SOAR technologies ensure adherence to major regulatory frameworks, including the General Data Protection Regulation (GDPR), and the Schrems II ruling. We provide a UK secure sovereign cloud operating in Defence and Critical National Infrastructure sectors and therefore Guardsix aligns perfectly with our data privacy protocols."

Ian Vickers, CEO at METCLOUD

cadesign base

"With Guardsix NDR, instead of looking at hundreds of alerts per month, you can focus on a few chains that highlight real potential threats."

Jesper Skovdal, Cadesign Base

What our customers say about us

Gartner Peer Insights™

“One of the advantages of being a Guardsix member is that the customer receives SOAR, a tool that automates the routine tasks of a SOC analysis. SOC analysts no longer need to verify low-level alarms and cleaning records now that SOAR is available. Instead, the SOC analysis may apply critical thinking to tackle difficult issues while SOAR handles the simple ones.” Gartner Peer Insights

STRAUSS

“Using Guardsix fundamentally changes the way you work with log data in your infrastructure. With Guardsix log data becomes a useful tool. It allows us to take control and get a meaningful, constant output that enables us to spot potential problems and react promptly.
Before things turn into a real threat.”

Markus Buss, Engelbert Strauss (SIEM)

Gartner Peer Insights™

“Guardsix has a very strong SIEM solution and is so easy to engage with both in the prospective phase and for users when needing support, technical or otherwise.
This is a company it's easy to do business with.”

Gartner Peer Insights

Gartner Peer Insights™

“Good SIEM Solution, good out of the box SIEM Alert Rules, plenty vendor integrations, good support, free log normalization for new vendors.”

Gartner Peer Insights

OTD BİLİŞİM GLOBAL VAD

guardsix

Guardsix safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Guardsix makes security operations easier, giving organizations the freedom to progress.

OTD BİLİŞİM
GLOBAL VAD

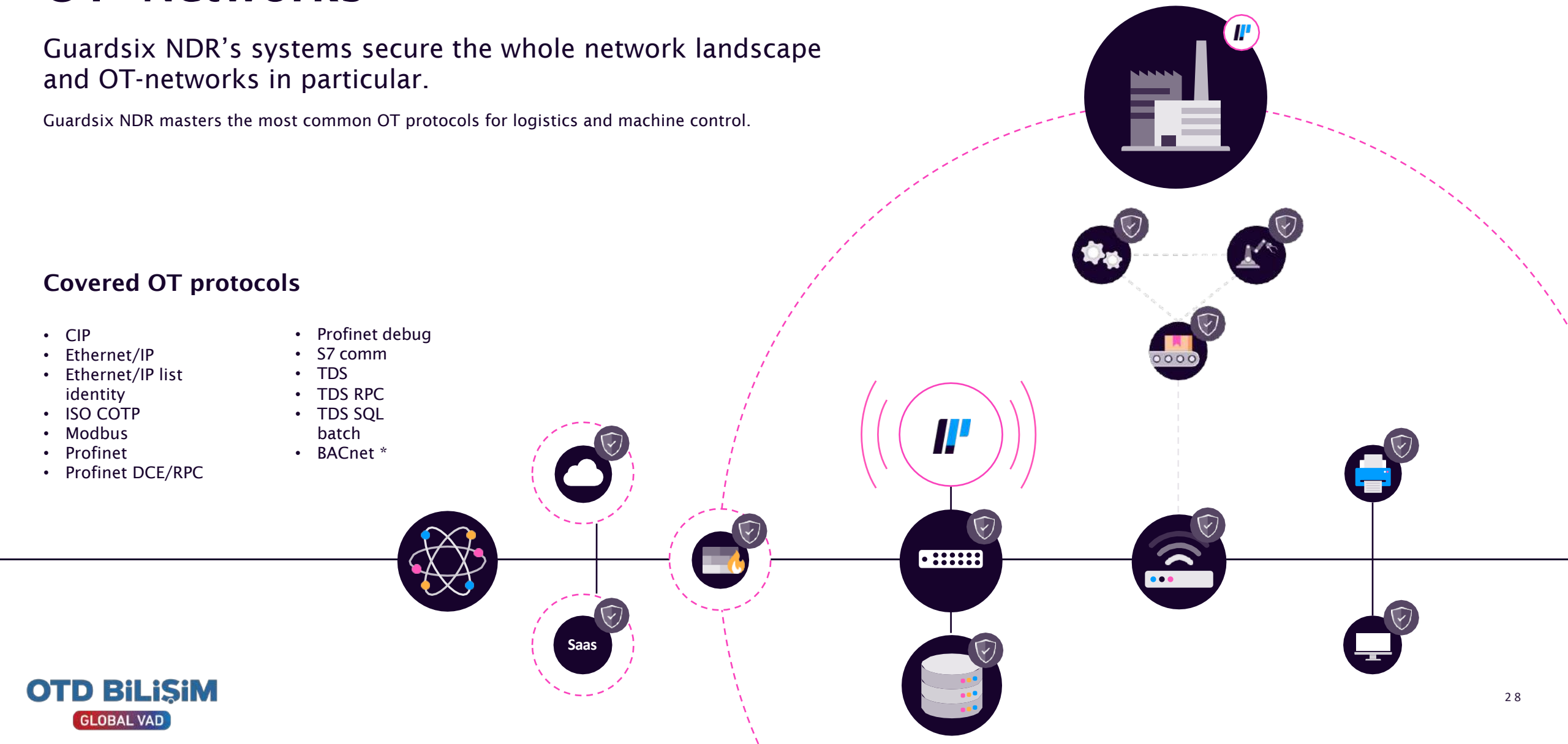
OT- Networks

Guardsix NDR’s systems secure the whole network landscape and OT-networks in particular.

Guardsix NDR masters the most common OT protocols for logistics and machine control.

Covered OT protocols

- CIP
- Ethernet/IP
- Ethernet/IP list identity
- ISO COTP
- Modbus
- Profinet
- Profinet DCE/RPC
- Profinet debug
- S7 comm
- TDS
- TDS RPC
- TDS SQL batch
- BACnet *



OTD BİLİŞİM
GLOBAL VAD

How would your engagement look with Guardsix?

Path to success