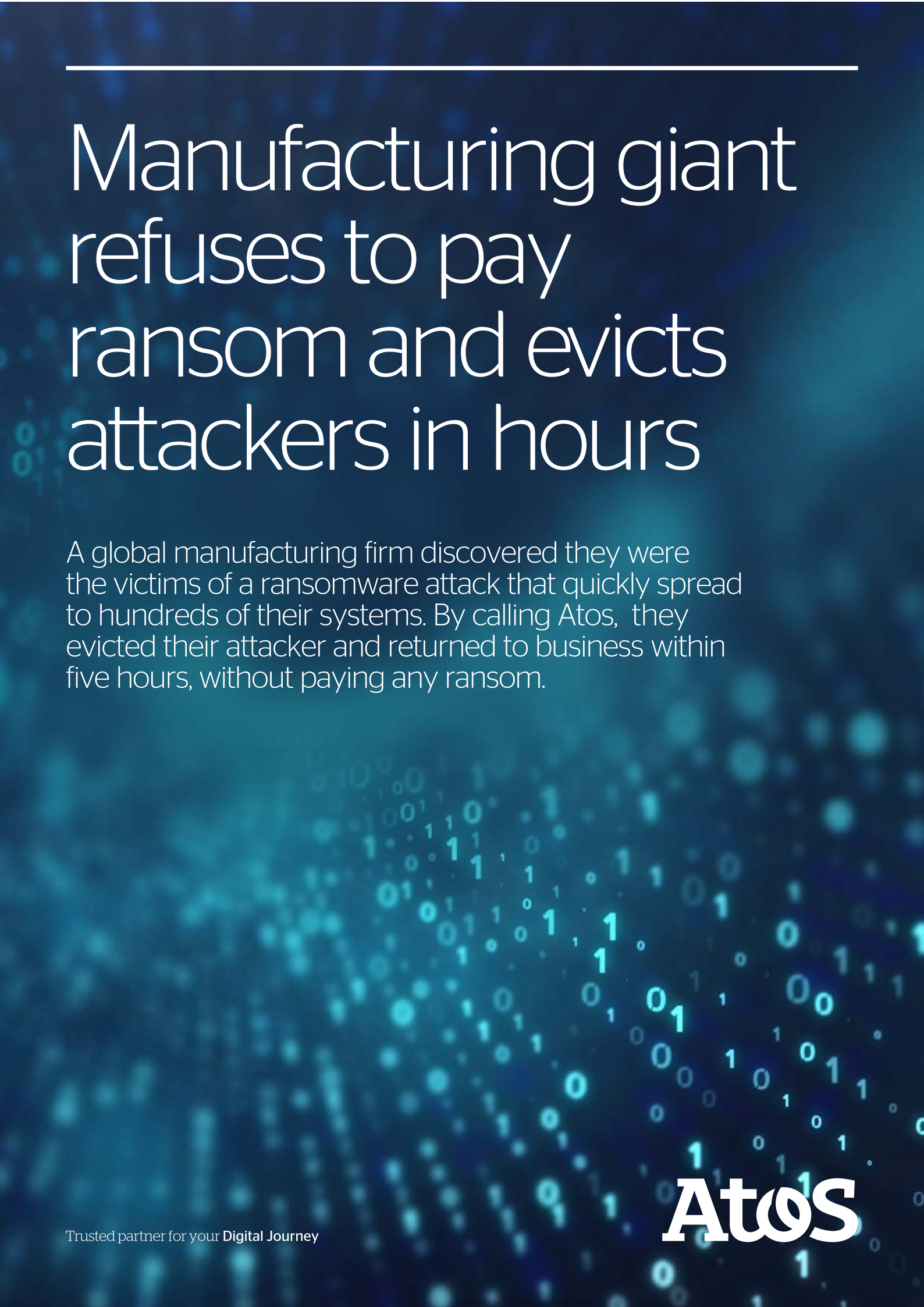
Manufacturing giant refuses to pay ransom and evicts attackers in hours

A global manufacturing firm discovered they were the victims of a ransomware attack that quickly spread to hundreds of their systems. By calling Atos, they evicted their attacker and returned to business within five hours, without paying any ransom.



Trusted partner for your **Digital Journey**

Atos

At a glance

Industry
Manufacturing

Location
Global operations

Challenge
The company suffered a ransomware attack that infected over 450 of its systems in less than an hour, with a ransom of over $5 million USD in XBT.

Solution
Atos deployed its breach management services. These included sending an incident response team to the client site, combined with remote analysis. Atos was able to extract and detonate the cryptoworm behind the attack, and returned the manufacturing company to operation later that day.

Results
By partnering with Atos, this manufacturing company:

- Actively investigated and identified the methodology behind the ransomware attack.
- Removed the threat and returned the business to operations within 12 hours of discovering the attack, and within 5 hours of calling Atos.
- Began to safeguard their systems with a full AI-driven MDR program.
- Reduced incident analysis effort by over 50%.
- Increased speed to detect, and time to remove threats, by over 80% each.

A manufacturing giant chose Atos breach management services to defend themselves against an in-progress ransomware attack. After Atos quickly and successfully remediated the threat, the manufacturing company signed up for Atos's full AI-driven MDR program.

Overview

This multi-billion dollar, multinational manufacturing company, based in Asia, sold its products throughout the world. With a distributed global network and over 6,000 employees, their core infrastructure held many vulnerability points. They operated production and distribution 24x7x365, and could not afford to suspend operations for long. Cyber criminals took advantage of this fact and targeted the manufacturing giant with a crippling ransomware attack.

Challenge

Around 11am, this company's internal security team discovered they were the victims of a cyber-attack. The attack moved fast, and spread from three systems to over 450 systems (including servers) within one hour. The internal security team suspected they were suffering a ransomware attack, and by 1pm they shut down all critical systems to prevent the malware from spreading further. During this time, they were forced to suspend production in their plant.

By 2pm, the cyber criminals behind the attack submitted their ransom: they demanded XBT 1.7 per infected machine, or XBT 28 for the Enterprise Key. They demanded these funds within one week. They did not promise to attack further, even if they received their ransom.

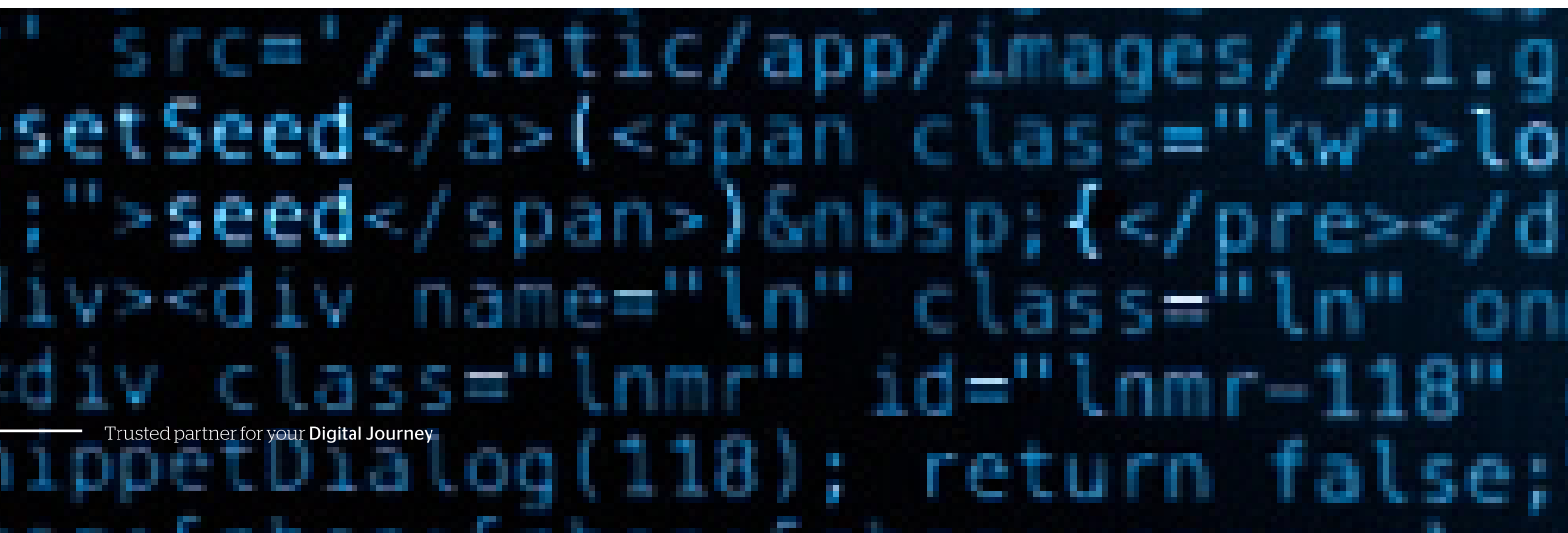
After reviewing the impact of losing data on the infected systems', the company's management made a decision. They would not negotiate with the cyber criminals behind the attack. They would not pay the ransom. Instead, they would call Atos, and enlist the security firm's breach management services to stop the attack from spreading and recover the data.

Solution

The global manufacturing company chose Atos breach management service to save them from their ransomware attack. The attack had already shut down the company's production, and they needed to resolve the threat quickly. The company called Atos at 7pm with an urgent request for help, and contracted Atos breach management services.

Atos breach management services provide comprehensive cyber forensics and rapid response to deliver rapid, coordinated, and effective security breach response.

These services provide access to Atos "always-on" 24x7x365 response team and **AIsaac** platform, a tailored breach response plan based on the unique needs and context of the enterprise under attack, and a coordinated execution of the defense plan.



Each breach management engagement ensures:

Collaborative, Orchestrated Responses

Atos's industry-leading response teams and AIsaac platform give organizations the advanced forensics and response procedures and technologies they cannot develop on their own.

Supervised Autonomous Response

Atos response AIsaac platform automates work flows, case management, forensic tools, and playbooks for common incidents (and adds new threats once they are discovered and resolved).

Unified AI and Human Intelligences

Our threat hunting experts sifted out suspicious activities in the client's network and applications, to stop creative attackers who were not deterred by intrusion prevention. Our multi-source analytics continuously uncovered new threats in our client's networks, which our machine learning systems triaged, investigated, and quickly responded to.

Network Threat Analytics

Atos combines its cutting-edge custom-built AI-driven response platform with a pool of nearly 1,000 cyber security experts to combine machine intelligence with human insight.

For this client, Atos immediately dispatched an incident response team to the company's location. At the same time, Atos initiated remote analysis. In a little over an hour, Atos forensics experts reach ground zero, receive the remote analysis team's report, as well as an update from the company's IT security team. They begin their active investigation.

In less than a half-hour, Atos's team identifies the attack as a cryptoworm attack—SAMAS or SamSam. They are able to extract and detonate the worm at Atos labs to study its behavior.

Results

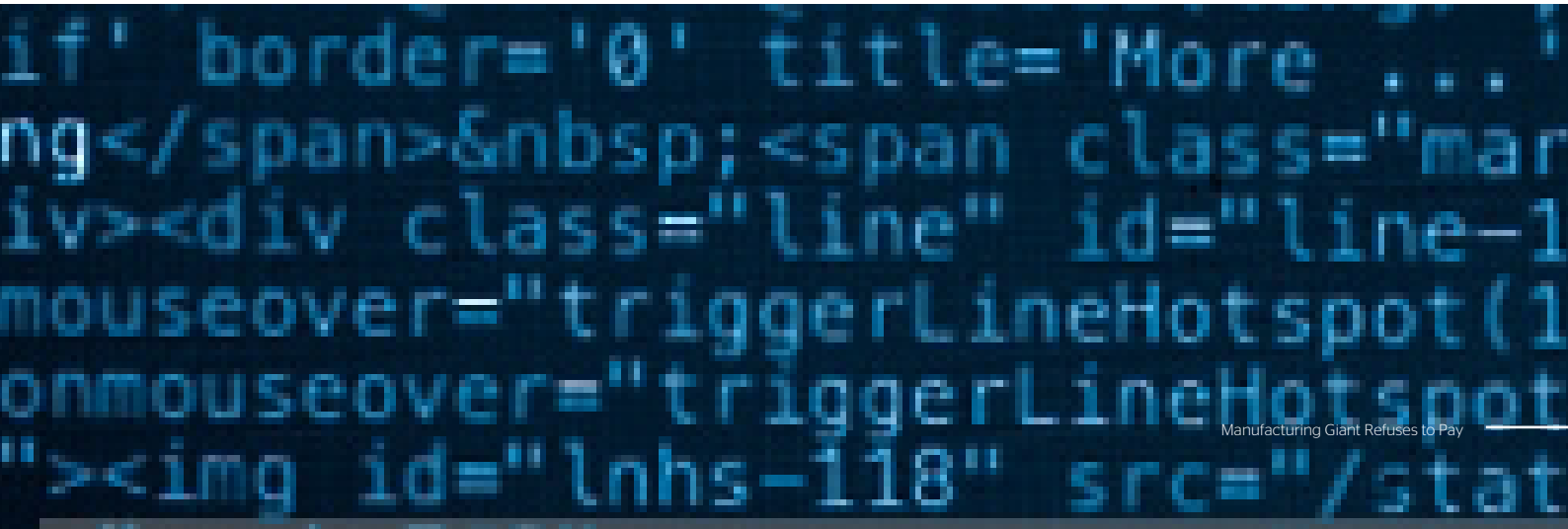
After extracting and detonating this malware, Atos quickly identified its unique behavior. They discovered the multiple conditions the malware needed to fulfill before it would begin to encrypt files on endpoints, and—by evolving the manufacturing company's defenses—ruled out the possibility of re-infection.

In their evaluation, Atos determined that a few of the company's systems were heavily infected and required reformatting. However, Atos was able to disinfect the majority of the company's systems by removing the malware associated with the files. At 12:02 am—a mere five hours after the company called Atos and contracted their breach management services —the manufacturing company began to start to bring their systems back online, and return to operations... without paying the ransom.

Once the incident was fully resolved, the company realized they experienced significant gaps in their ability to proactively defend against, identify, and remove significant threats— which lead to their infection in the first place. In response, and in recognition of the success Atos offered with its breach management service, the company immediately began to contract Atos to bring their full AI-Driven Managed Detection and Response (MDR) services to prevent similar future incidents.

"Atos Incident Response Team was able to contain the ransomware threat very swiftly. Within 30 minutes of arriving on our premises, they were able to identify the ransomware variant and brief us on the next steps that will be taken. We are thoroughly impressed with their professionalism and expertise. We have now engaged them full time as an MDR service provider."

CIO,
Manufacturing Company



About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/careers

Atos Global Head Office
River Ouest, 80 quai Voltaire
95877 Bezons cedex – France
+33 1 73 26 00 00

Let's start a discussion together

For more information: **cybersecurity@atos.net**

CT-201126-AR-MDR-CS-MFG-GIANT-REFUSES-RANSOM-EN-V1