

# Breach response case study

Insurance company

## Large backups destroyed, 15,000+ devices encrypted



As Gartner notes, ransomware activities “are at an all-time high during the global health emergency. Cybercriminals are becoming more sophisticated, organizing as groups and sharing techniques, data and results of prior exploitations.”

With the right security capabilities, any organization can prevent, detect, and respond to any ransomware attack that comes their way — without suffering significant harm.

In the incident illustrated in this case study, this organization was compromised by a ransomware attack because they lacked security controls like Secure Email Gateway (SEG), Secure Web Gateway (SWG), segmentation, analytics-based threat detection, and immutable backups. This lack of basic security controls created a perfect storm that led to a significant attack — one that we were able to stop.

To show you how we stopped this attack and how you could too, we will outline:

- A detailed timeline of the incident and our response
- How to successfully prevent, detect, and respond against attacks like this
- How you can develop the ability to stop attacks like this

### What happened: Timeline of the attack and our response

This ransomware attack demonstrates how elusive an attack pattern can be and how attackers have learned to evade detection by leveraging legitimate connections and disabling conventional monitoring tools. Thankfully, we could still stop this incident before the attackers caused significant harm. Here’s what happened during the attack and how we evicted the attacker.



## Lessons learned: How to stop this attack

In this incident, the attacker moved quickly through the client's systems, built a significant foothold, and exfiltrated a large volume of data in just a few weeks. It was fortunate that the client called us in before that data had been viewed and shared and that we could stop the attack quickly.

You can prevent attacks like this— or at least detect them much earlier in their progression — by developing a few fundamental security capabilities.

### Prevention

- Use MFA for external accesses
- Disable or delete accounts of former employees
- Manage unused service accounts
- Avoid discoverable, hardcoded passwords in scripts and applications
- Eliminate discoverable, hardcoded passwords in scripts and applications
- Isolate legacy systems that can't be adequately patched
- Implement tamper-resistant backups
- Deploy agents with application controls (blacklist/whitelist servers and workstations)

### Detection

- Establish broad detection across across vectors to detect multi-channel attacks
- Perform analytics-based threat detection that goes beyond known signatures
- Monitor user behavior, even from legitimate tools, credentials, and websites
- Periodically check security monitoring to ensure it hasn't been disabled
- Maintain up-to-date threat intelligence for all ransomware variants
- Regularly verify your SIEM/MDR receives signals from your environment

### Response

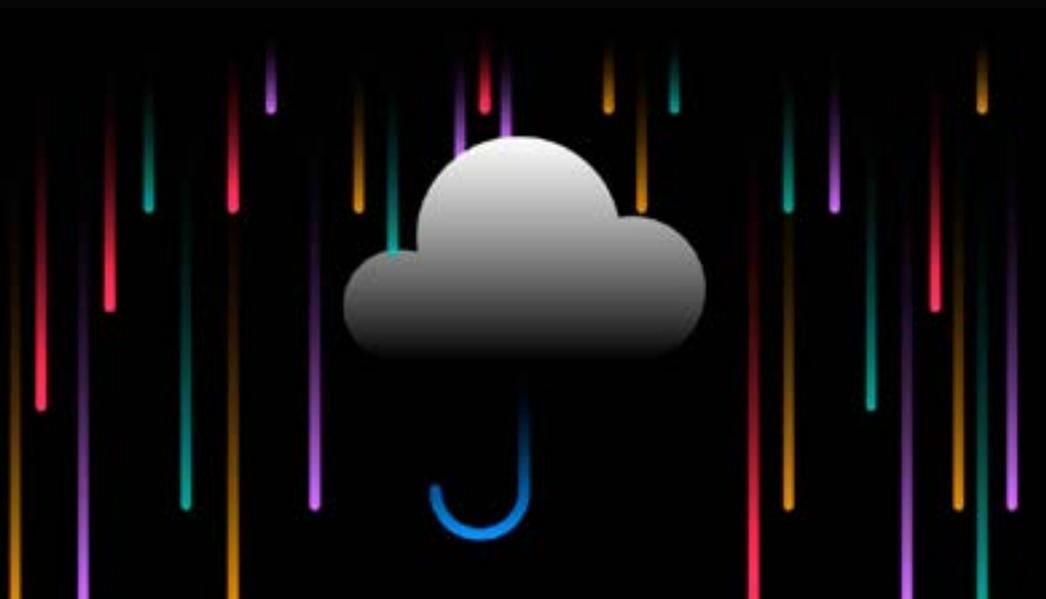
- Automate access reconciliation and policy validation
- User insider threat detection
- Ensure monitoring systems can ingest data from IAM systems
- Implement network-based detection tools for your perimeter
- Use MDR/XDR and correlate threat intel and signals from your environment

## An ounce of prevention: Prepare to stop this attack ransomware

These security lessons are simple, but they can be challenging to bring to life. This is why Atos has put together a comprehensive framework for Ransomware defense aligned to the NIST framework. You can download this complimentary e-book here:

<https://atos.net/en/lp/ransomware-defense-2022>

To learn more about Atos security solutions, schedule a no-obligation consultation with an Atos Digital Security expert and begin to build or augment your ransomware defense.



# About Atos

Atos is a global leader in digital transformation with 112,000 employees and annual revenue of c. € 11 billion.

European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries.

A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients.

Atos is a SE (Societas Europaea), listed on Euronext Paris and included in the CAC 40 ESG and Next 20 Paris Stock indexes.

The [purpose of Atos](#) is to help design the future of the information 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](https://atos.net)

[atos.net/career](https://atos.net/career)

Let's start a discussion together



For more information: [breachresponse@atos.net](mailto:breachresponse@atos.net)

Atos is a registered trademark of Atos SE, August 2022.  
© Copyright 2022, Atos SE. Confidential Information owned by Atos group, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval of Atos.