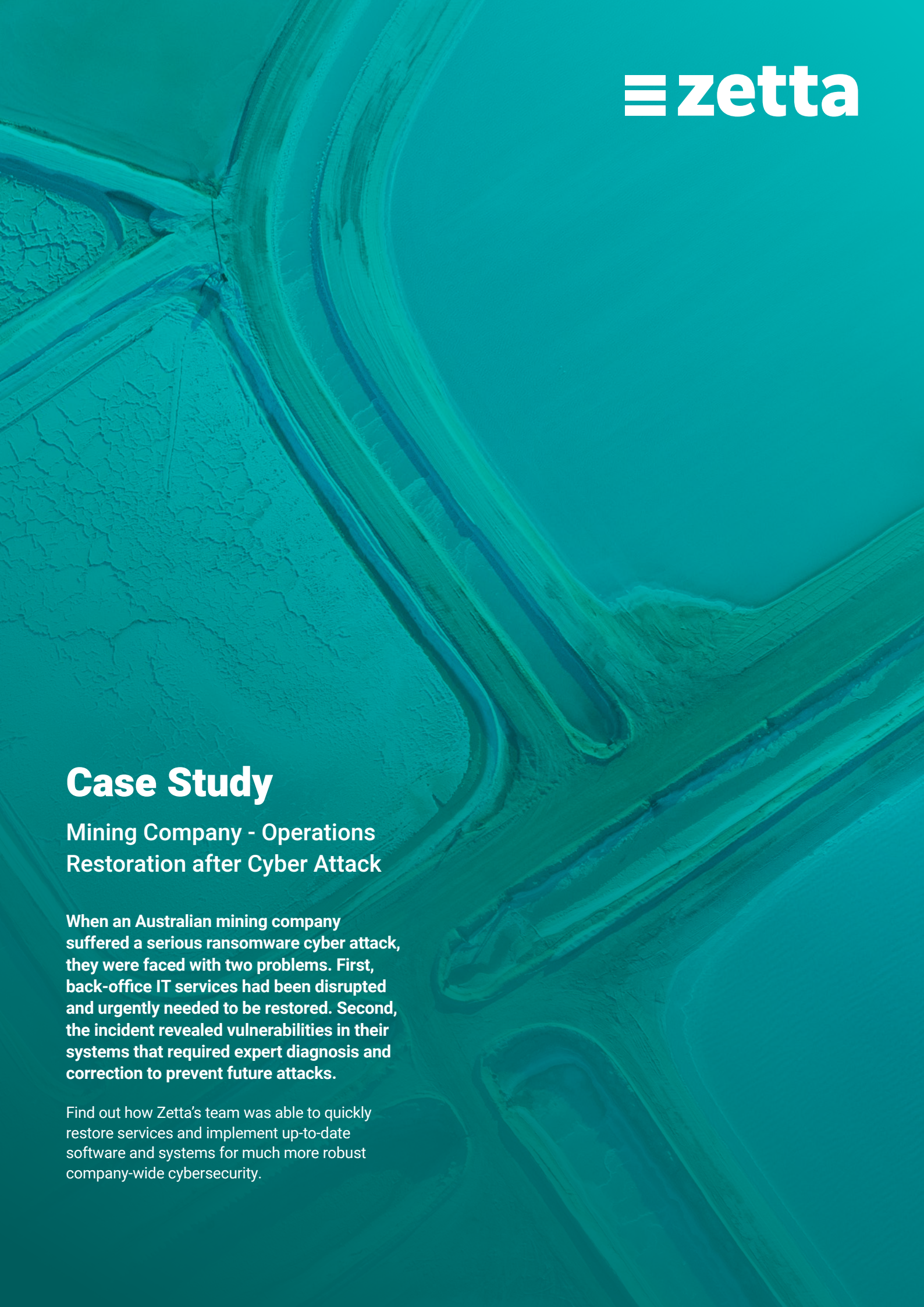


Case Study

Mining Company - Operations Restoration after Cyber Attack

When an Australian mining company suffered a serious ransomware cyber attack, they were faced with two problems. First, back-office IT services had been disrupted and urgently needed to be restored. Second, the incident revealed vulnerabilities in their systems that required expert diagnosis and correction to prevent future attacks.

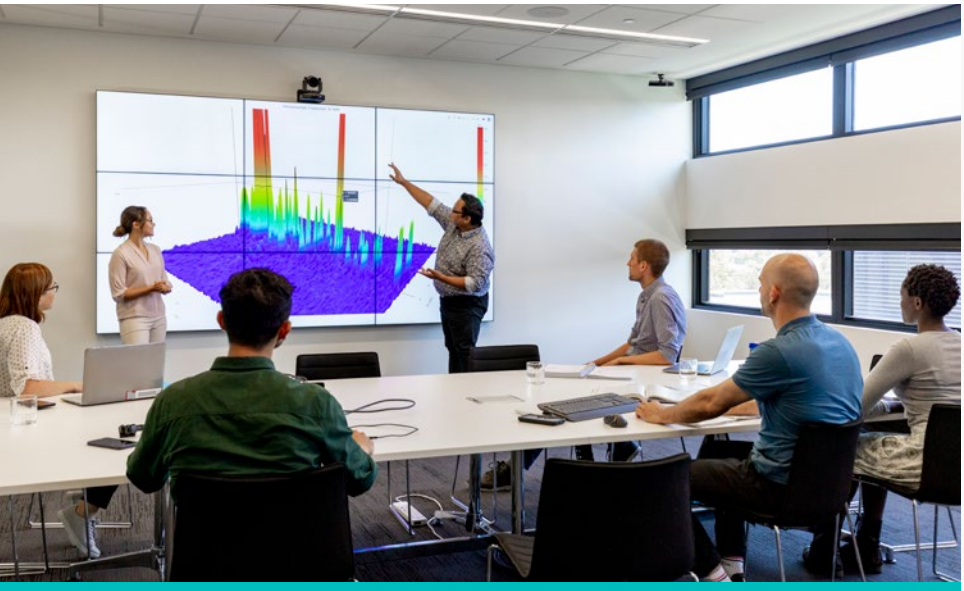
Find out how Zetta's team was able to quickly restore services and implement up-to-date software and systems for much more robust company-wide cybersecurity.

The Problem

The deployment of ransomware on the client's computing systems was made possible by a successful phishing attack against an end user in the company. In addition to the immediate problems caused by the unavailability of crucial IT services like email and site access management, it was clear there were deep inadequacies in the systems currently in place to prevent and deal with cyberthreats. These included:

- Endpoint Vulnerability: There was no software in place to monitor employees' devices in real time to detect and respond to threats. Email and network access also had security weaknesses.
- Inadequate Updating: The software on company servers was out of date, in some cases by as much as a year. Up-to-date patches would have fixed the vulnerability the attackers exploited.
- Inadequate Backup and Restoration: The company's process for restoration in the event of data loss was neither documented nor tested. The credentials for the backup software were unavailable. Moreover, the type of backup in place was slower and less reliable than other available methods. Finally, not all servers were even being backed up.
- Poor Readiness: The client had no dedicated team to deal with a cybersecurity crisis nor did it have a plan for what to do in such a situation.

The client had an immediate need to restore vital IT services. They also wanted to make sure systems were updated to overcome these inadequacies to guard against future attacks. In addition, they wanted to ensure a smoother restoration in the event of data loss in the future.



Facts at a Glance

Client:
Mining Company

Size of Company:
200 - 500 employees

Challenge:

The client was the victim of a serious ransomware attack that disabled back-office IT services. It required rapid restoration of operations and the creation of a secure environment to prevent future attacks.

Solution:

- Implementation of cloud-computing infrastructure to restore services, provide for robust data backup, and ensure secure user authentication
- Improved endpoint security, including multifactor authentication and real-time monitoring and response to threats
- Rebuilt and reconfigured onsite servers and other infrastructure for a secure network that stays up to date, restoring applications and data where possible.

Results:

- Further damage prevented by isolation of affected systems
- Rapid transition to a cloud platform allowed efficient restoration of crucial IT services like email
- Greatly enhanced security from user devices to company servers and networks along with robust backup and restore capabilities
- Client's IT team was freed to focus on its primary task of user support.

Products:

- Azure Virtual Machines
- Azure Firewall (inc Virtual Networking and ExpressRoute)
- Azure Active Directory
- Azure Backup
- Azure Migrate
- Azure Log Analytics
- Endpoint Configuration Manager
- Defender for Endpoint

Solution areas:

- Cybersecurity Incident Recovery
- Unified Endpoint Management
- Cloud-Based and Onsite Infrastructure Design & Deployment
- Network Security

The Solution

Zetta's cybersecurity specialists worked quickly with third-party application vendors and client teams to formulate a plan to restore services as efficiently as possible while implementing systems to prevent future incidents.

Their efforts focused on three areas:

- **Cloud Computing:** Zetta was able to build Azure cloud infrastructure, including virtual machines, to quickly get core services like email up and running. Efficient, secure cloud solutions were put in place for the backup and restoration of company data as well as authentication control for end users.
- **Endpoint Security:** User devices were identified and cleaned to make sure they would not re-introduce problems on the restored company network. Further, security measures like Microsoft Defender, multifactor authentication for email, more secure RADIUS networking connections, and robust access control were implemented.
- **Onsite Infrastructure:** Zetta's team rebuilt and reconfigured the client's servers and networking using best practices for security. They set up Microsoft's Endpoint Configuration Manager to enable consistent management of user computers and ensure software remains up to date with the latest patches. They re-installed applications and restored data where possible for systems in both the central and regional locations for the client.

The Benefits

The solutions Zetta was able to plan and implement provided immediate assistance to the client and set the company up for long-term data safety.

Prevention of Further Damage

Zetta first isolated compromised systems and hardware to make sure no further damage would be done from the ransomware attack.

Quickly Back to Work

The rapid transition to a cloud platform allowed crucial IT services, like email, to be restored right away. This enabled the company to keep employees up to date about the steps being taken to restore operations after the attack.

Improved Security

The robust backup and restoration capabilities that are part of the cloud solution ensure against future data loss. A range of up-to-date threat protection and monitoring tools have greatly enhanced security on user devices, company servers, networks, and email. Future unauthorised access to company systems is much less likely and, should it occur, also less likely to cause significant damage.

IT Team Supported

During a highly stressful time, the client's IT team was freed to focus its attention on supporting end users while Zetta took on the complex task of restoring operations and updating systems.

Zetta empowers modern work by providing solutions for a mobile workforce, data security, and cloud computing. A privately owned, Western Australian-based company, it is capable of both technology implementation and ongoing management, to help clients improve their workforce productivity and information security.

zetta