Foregenix

Case Study

Welgevonden Game Reserve

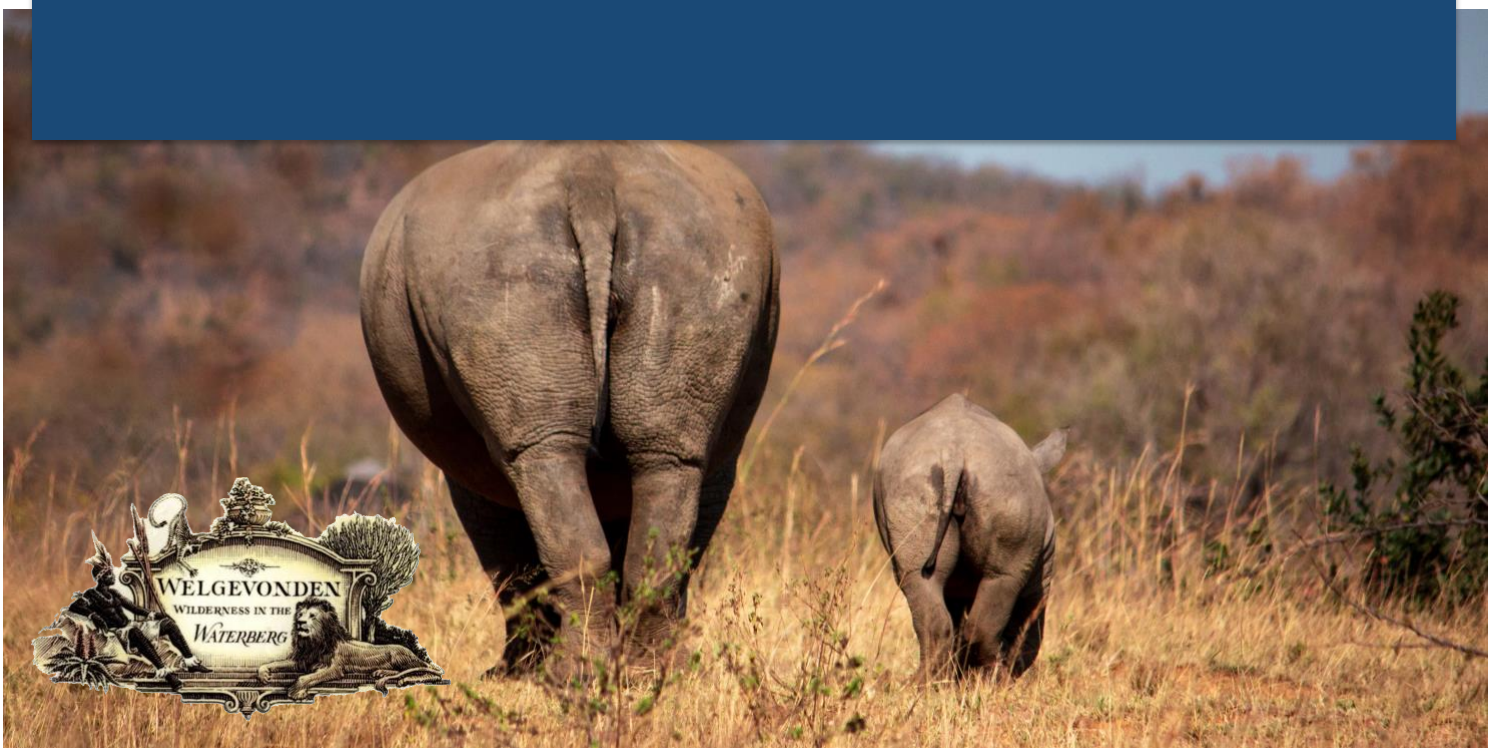

Image via: Welgevonden Game Reserve

Summary

Welgevonden Game Reserve is in the Waterberg District in the Limpopo province of South Africa. The reserve forms part of the Waterberg Biosphere Reserve and is home to a plethora of wildlife (including the Big 5), vegetation and fascinating geology structures. The area was declared a UNESCO Biosphere Reserve in 2001.

Welgevonden is known for developing advanced techniques and technology for the conservation and wildlife industry and is one of the few private reserves with a formal partnership with the SA National Parks. In another partnership, with IBM, MTN and Wageningen University (from the Netherlands), the reserve is at the forefront of developing a new anti-poaching system, which not only focuses on the widely publicised poaching of rhinos, but on all wildlife poaching. Named the Welgevonden's Wildlife Protection Programme, the system has the potential to increase the poacher capture rate from less than 5% to more than 85% — which is widely considered a potential game changer in the fight against poaching.

Relative to conservation and wildlife organisations, the reserve has a significant investment in IT with more than 30 active users. Apart from a fully computerised administrative system, the reserve deals with an abundance of sensitive anti-poaching data and other security information on a day-to-day basis. While the bulk of this information is used to evaluate and regulate human activity within the reserve, a portion of the data collected is also used for research purposes.

Key Points

- Welgevonden Game Reserve suffer Ransomware attack
- The attack encrypted key data files and affected network & email accessibility
- Foregenix' two step approach, eliminating the threat and protecting them for the future

Image via: Welgevonden Game Reserve

Challenge – Data blocked, Bad guys want money

Small and medium organisations are a significant target for hackers for three simple reasons: there are more potential 'victims', their IT environments are usually not prepared for sophisticated cyberattacks and they assume that they are unlikely to be a target.

A challenge arose when the reserve was confronted with a **ransomware attack**. The virus affected both network and email accessibility and encrypted key data files. While the team was desperate to get their system back up and running, there was a caveat. It had to be restored without further compromising the organisation's security (i.e. they needed to make sure that the intruder could not perform another attack).

Ransomware is a malicious software that blocks access or threatens to publish the victim's data unless a ransom is paid.

Unable to access their data and still at risk of suffering another attack, Welgevonden was at a standstill.

Solution – Foregenix' two step approach

Welgevonden's got in touch with Foregenix, a globally recognised cybersecurity leader, to find out if they could assist them, and if so, how quickly. After assessing the situation, Foregenix provided a two-step solution.

Step one – Securing the environment and getting it running again

A cyber security specialist was sent on-site. He provided the reserve with a full assessment of its IT security profile and assisted and guided the Welgevonden team in securing their environment, so that they could operate again with confidence.

Step two – End Point Sweeping and Protection

Part two of the solution was to provide Welgevonden with access to Foregenix Managed Detection and Response (MDR) powered by Serengeti. The deployment of this technology allowed for the Foregenix Threat Intelligence Group to monitor key security telemetry across the IT environment, and rapidly detect and mitigate any existing and early stage threats.

Results – Eliminate the threat and be better prepared for the future

Foregenix

The telemetry captured and analysed was valuable in helping Welgevonden identify latent threats in their environment and assist them in not only remediation the ransomware attack, but in minimising the threat of future cybersecurity attacks as well.

Welgevonden, together with its IT service provider, has now put suitable security measures in place and adopted Foregenix MDR services.

These measures have proven successful as Foregenix MDR is regularly detecting and preventing new attacks. Now Welgevonden can have peace of mind that the security of their valuable research data and customer information is being monitored and protected.

Takeaway

Companies and organisations need to be aware that they're a potential target and implement the right security solutions to keep their data safe. Small and medium-sized businesses are particularly at high risk, with hackers viewing their lack of security knowledge and investment as a weakness.

We've developed MDR with these organisations in mind, so that they can protect their valuable data quickly and cost-effectively, thus avoiding the risk of becoming the next victim.

Be sure to get in touch and learn more about Foregenix Managed Detection and Response (MDR).

United Kingdom (HQ)

8-9 High Street
Marlborough
SN8 1AA

UK Tel : + 4 4 (0) 8 45 309 6232
Fax : + 4 4 (0) 8 45 309 6231

MEA

Foregenix (Pty) Ltd.
58 Peter Place
Sandton
2060 Gauteng,
South Africa

Tel: +27 860 44 4461

North America

Foregenix Inc.
60 State Street
Boston, MA
02109

Tel : +1 (508) 644 1504

LATAM

Foregenix S.R.L
11500 Montevideo
Montevideo
Uruguay

Tel: +54 9342 421 6688

Europe

Foregenix Germany GmbH.
Betzelsstraße 27
55116 Mainz
Germany

Tel : +49 6131 2188747

APAC

Foregenix (Pty) Ltd.
1 Market Street
Sydney
NSW 2000

T: +61 420 904 914

Foregenix