

ZPower**Overview****Industry**

- Manufacturing & Supply

Challenge

- Insufficient insight into internal and external network traffic
- Concerned about 'unknown unknowns'
- Apprehensive about night-shift employee activity
- Needed to safeguard cutting-edge IP

Results

- Enterprise Immune System spots threats as they emerge
- Confidence in capabilities to detect insider threat
- Prioritizes the most serious anomalies to cut through the noise
- Unprecedented visibility of a growing corporate network

Business Background

Established in 1996, ZPower is a leading manufacturer of rechargeable, silver-zinc microbatteries. The company's innovative technology – born from nearly two decades of cutting-edge R&D – provides high energy microbatteries for medical devices, hearing aids, and other compact electronics. ZPower's dynamic manufacturing facilities, advanced R&D practices, and consequent business growth have contributed to its expanding and increasingly complex network.



Darktrace opened our eyes to every kind of device we had on our network. The platform provides real-time anomaly detection capabilities and unprecedented visibility that is simply unmatched by any other vendor in the industry.

Nitin Arneja
Director of Information Systems

**Challenge**

Faced with an unfamiliar and fast-evolving threat landscape, that includes subtle attacks, insider threats, and ransomware, ZPower's IT team sought to develop a robust security stack that could help mitigate these risks. The organization was expanding rapidly, and the steps taken to accommodate that growth – such as hiring third-party staff and introducing more devices onto the network – expanded ZPower's attack surface.

The IT team lacked comprehensive visibility of its entire network infrastructure, and thus wanted to deploy a technology capable of visualizing all network activity in real time. Additionally, the team recognized that today's threat landscape includes never-before-seen threats, which go undetected by signature-based tools. The ability to protect against zero-day threats was a top business priority for ZPower and its security team.

Solution

To meet these needs, ZPower deployed Darktrace into the core of its network during a four-week Proof of Value. After a swift one-hour deployment, Darktrace immediately started learning the 'pattern of life' for every user and device on ZPower's network. Using AI algorithms and machine learning technology, Darktrace develops a powerful and evolving understanding of 'normal' for the network, from which it discerns subtle deviations and potential threats as they emerge in real time.

Additionally, Darktrace maps all activity onto the 3D Threat Visualizer, a graphical and interactive interface that provides the security team with real-time visibility into its entire network infrastructure. Furthermore, it classifies each anomaly by its level of deviation from 'normal' allowing for smart prioritization of threats and increased efficiency among the security team.

During the third week of the trial period, in the middle of the night shift, Darktrace detected anomalous activity occurring on ZPower's production floor and immediately alerted the security team. An employee had accessed a seedbox site and downloaded a large amount of data. Upon investigation, it was found that the employee had downloaded unlicensed software to do his personal work, exposing ZPower's entire corporate network to malware infections in the process. Fortunately, Darktrace detected the download in real time, and the security team was able to address the issue before further damage could be done.

"When the Enterprise Immune System identified an emerging insider threat incident, it was all the proof we needed," commented Arneja. "Darktrace provided more visibility and better anomaly detection capabilities than any other tool on the market."

Benefits

Armed with Darktrace's Enterprise Immune System, ZPower is now confident that its valuable IP and growing corporate network are secure from advanced cyber-attacks and subtle insider threats. Now ZPower can continue its rapid growth without worrying about the implications its expansion might have for the company's changing cyber risk profile.

In addition to monitoring ZPower's on-premise environment and SaaS applications, the team also plans to expand Darktrace's deployment into its ICS environment. More-over, Darktrace has motivated ZPower to re-evaluate their internal security procedures, and to develop an initiative to better educate its staff on cyber security best practices.

“

Darktrace exceeded my expectations. It's a great product, and I look forward to working with the platform – and the company – for many years to come.

Nitin Arneja
Director of Information Systems

”

Contact Us

North America: +1 415 229 9100

Europe: +44 (0) 1223 394 100

Asia Pacific: +65 6804 5010

info@darktrace.com
darktrace.com