



Case Study: Upgrading Cybersecurity for a Metal Distributor Amidst Global Threats

Client Background

A **metal distributor** with 14 employees had been a long-time client of Underdog Cyber Defense. In 2021, during the wave of zero-day exploits targeting On-Premise Exchange servers and supply chain attacks affecting vendors in their industry, this client needed a comprehensive security upgrade to stay protected and maintain compliance.

Challenges

- 1. Evolving Threat Landscape:** The client's industry was facing ongoing supply chain attacks and zero-day exploits. While they had not yet experienced a breach, the threat was imminent, and existing systems were not sufficient to defend against more sophisticated attacks.
 - 2. Legacy On-Premise Systems:** The reliance on an On-Premise Exchange server created vulnerabilities, and the leadership team needed to be convinced to move to a more secure, cloud-based solution.
 - 3. Outdated Backup Strategy:** The existing backup solution was lagging behind, with on-site systems backing up to the cloud days after the fact, putting critical data at risk of loss.
-



Solutions Provided by Underdog Cyber Defense

1. **Cyber Insurance Review:** Before implementing security controls, Underdog Cyber Defense helped the client review and update their **cyber insurance**, ensuring they had proper coverage for the evolving threat landscape.
 2. **Endpoint Detection and Response (EDR) and SOC:** Underdog upgraded the client's defenses with a 24/7 **Security Operations Center** and advanced **Endpoint Detection and Response** tools to quickly detect and respond to threats.
 3. **Password Management:** A company-wide **Password Manager** was implemented to eliminate the use of browser-stored passwords, further securing user accounts.
 4. **Application Whitelisting and Privileged Access Management:** These solutions were installed to control application access and ensure only authorized users could access sensitive systems.
 5. **Advanced Email Protection:** Underdog deployed an **advanced email protection system** that quarantines suspicious emails before they reach users' inboxes, drastically reducing phishing risks and preventing email-borne attacks.
 6. **Image-Based Backup System:** The new backup system performs **hourly backups** to the cloud, replacing the old system that only backed up once daily and lagged in saving data to the cloud. The new system allows for **rapid recovery** in the event of an incident, ensuring business continuity.
-



Outcome

The deployment was initially met with some resistance, as the team had to shift their mindset around security best practices. However, with persistent support from Underdog Cyber Defense, the client successfully transitioned to a more secure and resilient infrastructure.

1. **Increased Confidence in Security:** Staff reported feeling safer and more aware of the dangers of mixing personal data with business systems. Leadership praised the comprehensive improvements, acknowledging that although risks remain, they are now significantly reduced.
2. **Supply Chain Attack Prevention:** The implemented layers of protection shielded the client from various threats affecting their industry, giving them confidence to continue operations without fear of a breach.
3. **Future-Proof Compliance:** As a company adhering to **ISO 9001** standards, the client benefitted from proactive controls that not only met current compliance needs but also anticipated future regulatory updates.
4. **Faster Recovery Time:** The new image-based backup system provided **near-instant recovery**, ensuring that in the event of a failure, the client could restore operations within minutes using up-to-date backups from the cloud.

Call to Action (CTA)

Is your business protected against evolving threats and supply chain attacks? **Schedule a Discovery Call Today** and let Underdog Cyber Defense help you build a resilient and secure infrastructure.