



Case Study

**Bidvest International  
Logistics gets serious  
about Cyber Security**



# Business Challenge

Bidvest International Logistics is a leading global transport and logistics company, whose partnership with EMO Trans, provides access to an international network of 250 offices in over 120 countries.

Established in 1910, we understand what it takes to optimize supply chains, because we've been doing it for more than a century. Our experience can take you from where you are, to where you're going. Simply put, a partnership with us is your gateway to the world.

We have offices at every major port and airport in the country and our end-to-end logistics offering includes air, sea and road transport; warehousing; and customs brokerage services in all major industries.

In addition to this, our qualified Supply Chain Engineers are available to you, to help analyze, re-design and optimize your logistics processes.

Bidvest International Logistics is defined by innovation, our adaptability to a constantly changing logistics landscape and our progressive nature, which means we are equipped to take your business to new heights by delivering the world to you.

**Innovative, adaptable and progressive.**



#### SECURE COLLABORATION

Office 365 Advanced Threat Protection (ATP) replaced the existing Mimecast solution and provides BidvestIL with an email filtering service, providing robust zero-day protection. Office 365 ATP now protects BidvestIL against unknown malware and viruses, harmful links, impersonation threats as well as providing extended SPAM filtering.



#### ACCESS CONTROL

Enabling Azure Multi-Factor Authentication (MFA) for all privileged roles within BidvestIL's Microsoft Office 365 and Azure tenants, provided additional security by requiring a second form of authentication.

MFA assisted in safeguarding access to data and applications while maintaining simplicity for all BidvestIL users. MFA was also enabled for employees accessing BidvestIL resources from outside of the Trusted IP ranges.

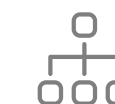
## **BUI deployed Microsoft Cloud App Security (MCAS) as multimode Cloud Access Security Broker (CASB).**



#### USER BEHAVIOUR ANALYTICS

BUI deployed the Azure Advanced Threat Protection (ATP) agents to all BidvestIL on-premise active directory domain controllers.

As a cloud-based security solution, Azure ATP leverages off BidvestIL's on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at the BidvestIL organisation.



#### SECURITY INSIGHTS

Implementing Microsoft Cloud App Security provided rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all BidvestIL cloud services.

To further advance BidvestIL's security insights, BUI ingested the Palo Alto Firewall logs into the MCAS solution, providing deeper insights into user network usage and the platform to configure activity type alerts.

## **BUI deployed Microsoft Cloud App Security (MCAS) as multimode Cloud Access Security Broker (CASB).**



**Additionally, the logs from the Palo Alto firewalls were also ingested into the MCAS solution. This allowed BPL a deeper insight into the network usage of users and allowed them to set alerts on certain types of activities.**

Azure ATP was deployed across all of the organizations Domain Controllers which provided a before unachievable visibility into the alerts and behavior of users. Microsoft Technologies enabled:

Office 365 Advanced Threat Protection | Azure Advanced Threat Protection | Azure Multi-Factor Authentication | Microsoft Conditional Access  
Microsoft Cloud App Security



## Solution and Benefits

# Using Microsoft technologies BPL was able to

- \* Improved Security Posture through advanced risk identification, visibility and reporting.
- \* BidvestIL's phishing attacks decreased with 5% in the first month post enablement of Office 365 ATP.
- \* Controlled access to sensitive and business resources.
- \* Improved Spam control.
- \* Analytical insights into user behavior and treat analysis.

BPL required **stronger security** measures to improve their security posture and reduce the number of **cyber attacks** they were experiencing.

# LET'S TALK

---

[WWW.BUI.CO.ZA](http://WWW.BUI.CO.ZA)

+27 (0)87 740 2400  
[info@bui.co.za](mailto:info@bui.co.za)



 **JOHANNESBURG**

Head Office  
Second Floor, Microsoft  
Corporate Hill,  
3012 William Nicol Drive,  
Bryanston

 **CAPE TOWN**

Harbour Bridge, Roggebaai  
Canal, Lower Long St,  
Cape Town City Centre

 **DURBAN**

Unit 13, Braehead Office Park,  
1 Old Main Road,  
Kloof  
Kwazulu-Natal