INETCO
BullzAI®

CYBERSECURITY
FOR ENTERPRISE

# INETCO BullzAI®<br>Cybersecurity for Enterprise

## Surgically block malicious network traffic without stopping legitimate business

Enterprises that depend heavily on their on-line presence face continual network attacks. The list of victimized industries is long, including financial services, games, gambling, merchants, internet service providers, web hosts and domain providers. DDoS, DDoS ransom, bot attacks, velocity attacks, and advanced persistent threats are on the rise as cyber criminals seek to steal millions though theft and ransom.

Early solutions included packet filters, deep packet inspection firewalls and intrusion detection, but they all had limits. This is where application layer firewalls were touted to cover the gap. The vast majority of application layer firewalls are web application firewalls (WAFs) or application programming interface (API) gateways. For at least the past decade, WAFs have been deployed extensively in web-facing environments. In some respects, they were seen almost as an upgrade of the older intrusion detection/prevention systems. However, many of the WAFs still presented the same problem of being signature based, which resulted in large amounts of false positives. As such, many of these WAFs were deployed in detect mode or partial block mode, but were never trusted enough to be deployed in full blocking mode because of the high rates of false positives.

Another tool, API gateways, began life as service-oriented architecture (SOA) gateways and quickly became an integration point into organizations' key technology assets. Current API gateways are identity-centric and provide many of the authentication and authorization brokering that is required when interconnecting different environments. They also offer a basic set of features associated with XML firewalling and threat protection.

Today's existing firewalls can detect external application layer attacks, but they can only block traffic at the network level (IP address and port). Blocking malicious transactions at this level also blocks legitimate transactions coming through the same IP address and port. As a result, legitimate customers are stopped from transacting or purchasing on-line. The impacts are lost revenue, brand damage, and angry customers. A decision not to block an attack can seriously degrade network performance or bring down the entire network for days. Either way, companies are left to deal with the impacts of lost revenue, brand damage, and angry customers. In other words, the gap is not completely covered by existing solutions.

**INETCO BullzAI® Cybersecurity for Enterprise (INETCO BullzAI)** is the only solution that automatically detects and surgically blocks application layer attacks generated by today's sophisticated DDoS, DDoS ransom, bot, velocity and APT attacks. It even catches insider fraud. INETCO BullzAI does this at the message and message field level, without blocking legitimate on-line activities or adding latency. Losses are minimized, brand reputation is preserved, and customer impacts are limited. The time and effort by network security teams to contain and mitigate attacks are dramatically reduced.

## An Intelligent Application Firewall Unlike Any Other

INETCO BullzAI® Cybersecurity for Enterprise performs the heavy lifting and pre-screening of transactions before they get to the transaction switch or web application server. It is a container-based application firewall that sits between the network firewall and the internal network. The advantage of being container-based is that it can be deployed in seconds when attacks take place, into many different segments of the network to protect the environment.

Existing firewalls operate at the packet level, so they cannot see the bigger picture at the message level. Existing firewalls only see transactions at a single point in the network. INETCO BullzAI® Cybersecurity for Enterprise is different. It sees transactions at every point across the network. It uses sensors to capture traffic directly off the network at various Policy Information Points (PIP) along the transaction journey. Transactions are decrypted and decoded in milliseconds, making every field of every message, as well as timing and duration, available to a central Policy Decision Point (PDP) where the decision on a specific transaction is made. This decision on whether to allow a specific transaction is based on a combination of rules and machine learning, both supervised and unsupervised, which is extensively leveraged to detect anomalies in expected behavior.

If the PDP finds that the transaction is anomalous and a potential threat, it sends a request to the Policy Enforcement Point (PEP) – the INETCO BullzAI application firewall - to drop the transaction based on specific fields rather than IP addresses or ports. This is particularly important as transactions may be coming from an intermediary, sharing the same source IP addresses and ports, including a mix of legitimate transactions and anomalous transactions. Transactions that are not anomalous pass through the INETCO BullzAI application firewall without any action taken on them. Importantly, no network latency is introduced.

INETCO BullzAI also defends against insider threats. As it sees transactions across every point in the network and automatically recognizes anomalous transactions, it can detect and block man-in-the-middle attacks as well as insider fraud, where beneficiaries are changed or transfers/withdrawals occur without an initiating customer transaction.

## Rapid Time to Value

INETCO BullzAI® Cybersecurity for Enterprise runs on standard hardware and can be deployed rapidly. It captures a copy of the data directly off the network without any instrumentation of endpoints, thereby avoiding a resource-heavy IT project. When additional endpoints or channels are added to the network, their traffic is automatically available to INETCO BullzAI, which can be easily configured to start monitoring the traffic.

### EXAMPLE 1

In 2020, a major US financial institution (FI) network was brought down for three days as the result of a set of bots that continuously created new accounts. Industry leading firewalls (network, web application firewalls and API gateways) were installed both within the FI and the upstream service provider. However, they were not able to identify the attack early enough, and when they eventually did, they were unable to stop the attack quickly. As all transactions had come through an intermediary, the FI could not identify the source IP address. Even if they could have identified the source IP address, blocking at the IP address and port would have blocked all legitimate transactions coming in from the intermediary.

INETCO BullzAI can automatically identify the originating IP address, as it is contained in the message payload, as well as the machine fingerprints of the systems executing the bot attack. Because the INETCO BullzAI application firewall can block at the field level, it can block only the transactions coming from the offending IP addresses/machine fingerprints.

### EXAMPLE 2

In 2016, a major African bank was the victim of an elaborate ATM cash-out attack. Social engineering was used to install malware on the bank's transaction switch. It forced the switch into standby mode and instructed the switch to approve all transactions. The anti-fraud systems on the back-end never saw the transactions so they were unable to detect the attack. Overnight, 100 people used forged cards to withdraw $19M from 1,400 ATMs worldwide in under 3 hours in a massive cash-out attack. The bank had no indication that the attack was occurring and only identified it after the fact.

INETCO BullzAI monitors the entire end-to-end transaction and knows what a legitimate transaction looks like. In a case like this, INETCO BullzAI can identify individual withdrawals being made without approvals from the authorization host. The INETCO BullzAI application firewall can automatically stop the transactions associated with the anomalous withdrawals without stopping legitimate withdrawals.

### EXAMPLE 3

In 2021, a mid-sized US bank suffered a velocity attack. Their existing firewalls could not identify which uniform resource identifiers (URI) on the website were being called, nor block the transactions with the offending bank information numbers (BIN). Their IT security and network teams worked to manually identify the attacking BINs and update the lists on their transaction switch to block the transactions. Doing so risked blocking BINs associated with legitimate transactions. For the period of the attack the bank suffered from degraded network performance and customer complaints. In addition, the IT security and network teams were pulled away from their planned activities resulting in delays to several projects.

INETCO BullzAI can automatically identify the terminal ID information and the originating IP addresses, the machine fingerprints, and the corresponding BINs used in an attack. Because INETCO BullzAI can block at the field level, it can block only the BIN transactions coming from the offending IP addresses/machine fingerprints. Legitimate card transactions continue without interruption.

## Summary

While existing WAFs offer protection at the port and firewall level, INETCO BullzAI® Cybersecurity for Enterprise is the only solution that automatically detects and surgically blocks DDoS, DDoS ransom, bot, velocity, APT and insider fraud attacks at the message and message field level, without blocking legitimate on-line activities or adding latency. It plugs the chinks in an organization's cybersecurity armour, adding an essential layer of protection.