The BOHH Security Appliance

For the Cloud (Public and Private)

BOHH Eliminates:
• Data Transaction Hijack Attacks
• Piggy-Back Attacks
• Man-in-the-Middle Attacks
• Website Threats/Attacks
• SQL Injection Attacks
• Public Wi-Fi Threats
• Endpoint Attacks

The Problem: Unsecured Cloud Services
Enterprise Cloud adoption continues to grow as a faster and more efficient method to replace legacy on-premise services that no longer scale and meet the needs of new customer mobile and digital demands. However, with this comes an increase in security threats that can quickly eliminate any of the gains made by adopting cloud technology into your business model.

The Solution: BOHH Cloud Security Appliance
Our multifaceted security solution secures Cloud (public and private) networks from external and internal security flaws and threats. BOHH is a software and infrastructure agnostic appliance that is easily deployed on top of existing infrastructure systems to securely transport data across all cloud services. This means quick implementation without compromise to transaction performance, speed, or customer accessibility. Enterprises can make further Cloud investments while being confident their assets (confidential and customer information) are secure from unauthorized users. BOHH autonomously reacts to all threats in real-time while storing no data, ensuring no latency, adjustments to your systems, or how your customers interact with their data.

How We Do This: Patented, Unique Encryption & AI
BOHH is built to secure your applications and infrastructure (cloud-based services) by leveraging a patented encryption method and AI technology to manage ports, maintain a secure connection, and interact with the users’ request. Our AI technology learns as it works to manage, maintain and protect against external and internal threats. With each data request, we use a patented block encryption system combined with our AI engine to pull up the right blocks and decrypt them. It then puts the data request together and passes it in memory. This is without any direct access to the server from the requester, preventing attacks and changes to confidential data.

Advanced Security
• Dynamically generates AES 256 encrypted message packets using a transient key (no key store management), for a fractional second in memory
• Digitally signs all requests & responses. Network sessions and keys are destroyed after each transaction, eliminating endpoint attacks
• Encrypts entire websites with no transaction delay or latency
• Additional Secure RESTful API add extra layers of security to the external connections (we don’t deal with/rely on standard http protocols)

AI Technology
• Built to work with industry cloud partners: SAP, Google, Oracle, AWS, etc.
• BOHH Labs Modules:
  • Cryptography
  • AI
  • Port Manipulation; Bot Compatibility
  • Dynamic Key Creation; Manipulation & Allocation, Block Transport of Messages
• Parallel Processing
• Service Manager
Technical Specifications

- Runs on SAP Cloud Platform and Google Cloud Platform
- Infrastructure agnostic appliance: deployed on the existing system between the infrastructure, firewall and transactions with Cloud and on-premise implementations for backend platforms and data protection
- Secure Voice / Text Bot compatible with API.ai, enabling voice-activated and messaging access through all of your customers’ digital applications
- Patented block files system enables full encryption of the website inside the firewall
- Built in security to protect backend web applications from multiple attack routes
- BOHHiMT Secure in memory database for transient, temporal in-situ data that is never stored or duplicated on the server
- Acts as a Secure Gateway for network traffic: one request manages and handles all connections to legacy data and external world

Key Benefits

- Lower Cloud security investments with one appliance
- Leverages existing infrastructure investments
- No migration of data required or legacy issues
- No overhead in terms of equipment or staff
- No downtime to implement or lag time on the system
- Customer-Facing: Secure 24x7 interaction across any device, from any location
- Proprietary secure bot engine validates access and customer experience
- No 3rd party interaction. Data is automatically invalidated when accessed by unauthorized users
- Real-time, secure transport of data, without compromising speed or customer accessibility

We are redefining Cloud security to become more dynamic within the existing system. Our solution is the foundation for delivering secure and trustworthy cloud-based services, so you give your customers the control, convenience and access to their information using the digital interfaces they increasingly demand.

- CEO and Founder, Simon Bain

Cloud investments are complex, expensive and often insecure, but they don’t have to be with BOHH Labs. Contact us to learn more.

About BOHH Labs

BOHH Labs is ushering in a new era of security for the Fintech market with a multifaceted solution that immunizes networks from brute force attacks, man-in-the-middle hacks, and quantum decryption. Built on a validated portfolio of patented IP, our security solution automatically invalidates data when accessed by intercepting parties and unauthorized users. BOHH autonomously reacts to internal and external threats in real-time, ensuring all incoming and outgoing messages are transacted securely. With this approach, Fintech organization can protect their banking infrastructure, brand and bottom line from the imminent threat of attacks without compromising speed or customer accessibility. BOHH Labs is headquartered in Oakland, CA, and has offices in Atlanta, GA, and New York.

https://twitter.com/BohhLabs
https://www.linkedin.com/company/bohh-labs
https://www.bohh.io/blog.html