Leveraging node based cloud containers to secure borderless networks
Issue: Traditional security appliances were designed to protect web browsing

Example: Secure Web Gateways

Secure Web Gateway

Only scans for exploits & malware on web pages
Challenge: Internet access consists of more than web pages

Applications & Malware co-exist outside of the web browser and are connected to the Internet

They focus on web browser activity

- Are blind to non-web browser Internet traffic on the device
- Applications and evasive protocols (i.e. TOR) exist outside of the web browser
- Legacy solutions lack effective approaches to managing SSL traffic
- This leaves a massive security blind spot which is leveraged by malware, ransomware and exploits
Increasing this challenge is the growth of remotes sites and mobile employees. Legacy approach responds by deploying more appliances or backhauling data which is inefficient & costly.
Alternatively, hybrid cloud deployments are utilized which only complicates matters.

Requires managing multiple consoles which increases demand for administrative resources and limits network visibility.

Corporate HQ = On-Premise appliances
Security is scanned via appliances at HQ with policy & reporting managed through the on-premises admin console.

Remote Sites = Cloud web security
Security is provided in the cloud with policy & reporting managed through the cloud policy admin console.

Inconsistent User Experience
Because security is applied by appliances deployed at HQ, users get a web experience provided by the appliances at HQ.

Mobile User Experience
Because security is applied in the cloud, users get a web experience provided by the cloud web security platform.
All-cloud web security’s monolithic cloud architecture becomes a concern

Data is shared across one massive cloud, increasing compliance concerns for the mobile workforce.

**Concerns with traditional cloud security**

- A monolithic cloud architecture which shares sensors and databases across many customers.
- This cloud can fracture, leading to latency as well as expose organizations to security breaches.
- Concerns meeting regulatory compliance such as Safe Harbor.
- Corporate data is forced to the cloud, which may not be desirable.

HQ is forced to the cloud.

© 2016 iboss, Inc. All rights reserved. All trademarks and registered trademarks are the property of their respective owners.
We can solve these challenges by leveraging a flexible node-based elastic container cloud architecture

Advantages:

- Benefit from the infinite **scalability** and **elasticity** of the cloud

- **Comprehensive** security to protect remote sites and mobile users with security that **follows users** in the cloud

- Cloud **nodes are elastic** and can be customer-hosted, reside in the cloud virtualized fabric, or both

- **Eliminates hybrid** deployment pain points of managing hardware and multiple policy consoles

- Provides a **seamless** node-based solution for customers who are cloud adverse or restricted from adopting the cloud
Cloud architecture is fundamentally different from conventional security cloud architectures

- Does not rely on virtual appliances instantiated in the cloud to replace traditional appliances
- Cloud utilizes a proprietary container-based virtualized architecture
- Leveraging nodes to deliver an infinitely scalable, dynamic and elastic cloud
Cloud Container
• Built from individual modules working together (e.g. URL, Reporting, ATD)
• Represents all of the iboss cloud functionality for a customer

1 Container = Multiple Modules
• Modules represent a component (e.g., URL, Reporting, ATD), and together they create a customer container.
• They independently scale on demand, resulting in a more resilient cloud architecture

1 Module = Multiple Virtualized Nodes
• Multiple cloud nodes performing the same functions cluster together.
• Module functionality is identically replicated in each node.
• Each node is a virtual instance (VM), and can be created or destroyed in seconds across the node fabric
The flexibility of a node-based elastic cloud container architecture is unmatched

1. **Corporate HQ**
   Traffic is scanned through customer hosted nodes that reside locally at corporate HQ

2. **Remote sites and branch offices**
   Traffic is scanned through virtualized cloud nodes residing in the cloud fabric

3. **Mobile Users**
   Traffic is scanned through virtualized cloud nodes residing in the cloud fabric

4. **Cloud Container**
   Encapsulates all nodes, providing consistent policy & reporting across all users and managed through one central management console in a secure isolated environment
Stream based security leveraging elastic containers eliminates blind spots

Deep stream-based packet scanning engine with full traffic visibility provides security beyond the web browser

Stream based advantages:

- Security that extends beyond web browser traffic to secure all Internet traffic
- Leverages a node based elastic container cloud architecture to secure all users and locations with ease
- Enables safe access to approved SaaS applications ensuring uninterrupted business operation
- Detects evasive, polymorphic malware including those masking communication via TOR (ex. Zeus64, Locky)
Module for anomaly does not rely on known malware samples

- Triggers based on behavior of the current data compared to normal data baseline
- Does not rely on malware signature updates
- This makes it capable of detecting malware even if it has never been seen in the wild and is unclassified
- Shortens the data loss window. For every passing minute that elapses waiting for a signature update, thousands of files are stolen resulting in massive losses

Protection against even the most advanced polymorphic malware

- Normal traffic
- Abnormal traffic

Internet

Alerts Sent

Alerting Threshold

Data Hijack In Progress

35,00 GB
25,00 GB
20,00 GB
15,00 GB
10,00 GB
5,00 GB
0 GB

Baseline Bytes: Actual Bytes
Secures borderless networks in a node-based containerized environment

- Customer hosted cloud nodes servicing HQ
- Hosted cloud node servicing mobile users
- Hosted cloud node servicing branch offices

HQ, remote sites, and mobile users secured by hosted cloud nodes
Cloud node-based containers prepare you for the future

Today

- Customer hosted nodes

- Nodes migrate seamlessly

Policy console remains consistent during migration

Tomorrow

- Hosted node migrates to cloud nodes

- Virtualized cloud nodes in cloud fabric

- Internet

- Node-based elastic container
Are you prepared for the future?

On-premises appliances and hybrid solutions require network restructuring and purchasing new products.

Today

Traditional Appliances

Limited migration path

Dispose of on-premises appliances = increased TCO

Limited migration path

Must invest resources to migrate security policies & report logs

Tomorrow

Massive network restructuring

Migration to cloud security

© 2016 iboss, Inc. All rights reserved. All trademarks and registered trademarks are the property of their respective owners.
For more information, visit www.iboss.com