ARMOR | SECURECON 2019 | DALLAS, TEXAS

FIREWALL:

WHY IT MATTERS & ARMOR'S UPDATED EXPERIENCE

MATTHEW MCGARITY & RAHUL NOWLAKHA

Armor Complete Product Managers

AGENDA

1. What's at Stake?
2. Armor Recommendations
3. Revisiting Our Firewall Experience
4. Demo
5. Q & A / Suggestions

MATTHEW MCGARITY

PRODUCT MANAGER

Contact me at:
matthew.mcgarity@armor.com

RAHUL NOWLAKHA

PRODUCT MANAGER

Contact me at:
rahul.nowlakha@armor.com

WHAT'S AT STAKE?

INCREASED COMPLEXITIES LEAD TO SIMPLE MISCONFIGURATIONS

95%

Of cloud security failures, through 2022, will be the customer's fault.

50%

Of enterprises, by 2021, "will unknowingly and mistakenly have some infrastructure-as-a-service (IaaS), storage services, network segments, applications, or APIs directly exposed to the public internet, up from 25% at YE18."

Source: https://www.gartner.com/en/documents/3899373

A TIMELINE OF UNFORTUNATE EVENTS

100%
Involved an unsecured S3 bucket in AWS.

920 MILLION +
Records were exposed publicly.

WHAT'S ~~WHO'S~~ IN YOUR WALLET?

CAPITAL ONE – MARCH 2019

- 100M+ customer records were breached
- Records were hosted on a cloud-based infrastructure
- Hacker gained access through a misconfigured firewall permissions
  - The WAF was assigned too many permissions
  - Allowed to list all of the files in any buckets of data, and to read the contents of each of those files

WHAT DOES A DATA BREACH COST?

COSTS ASSOCIATED WITH A DATA BREACH $148 PER RECORD IS MADE UP OF 4 MAIN FACTORS:

DETECTION & ESCALATION

NOTIFICATION COSTS

POST DATA BREACH RESPONSE

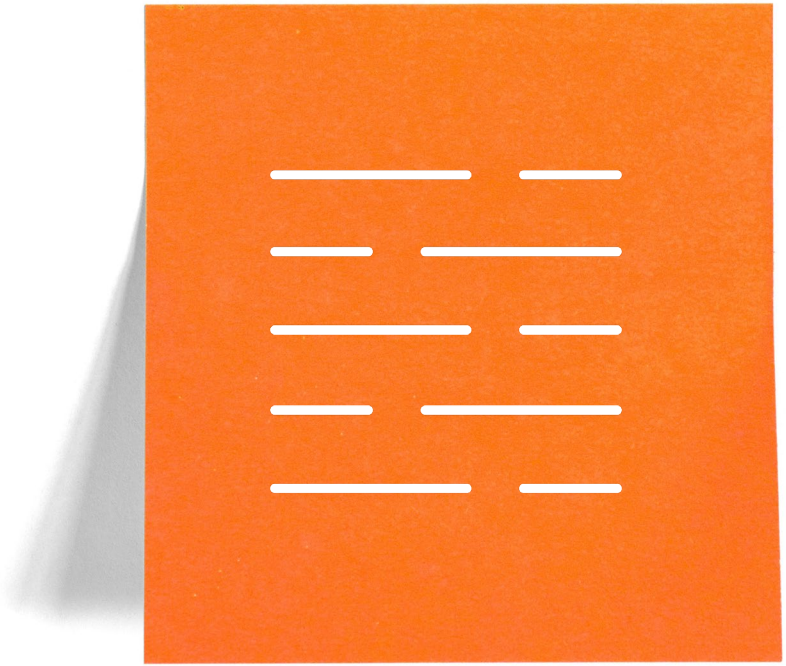
LOSS OF BUSSINESS COST

- Example: the 11 incidents of cloud misconfiguration we analyzed cost organizations upward of a combined $57 billion.
- This excludes regulatory fines

ARMOR RECOMMENDATIONS

FIREWALL: THE FIRST LINE OF DEFENSE

- Firewalls are meant for prevention
  - Hackers breaking into your system
    - Traffic coming from a bad source on the internet
  - Viruses and Worms that spread through the internet
    - Amount of traffic
    - Source of traffic and block it
- A well configured firewall is vital to protecting your data



HOW & WHAT GETS PAST FIREWALLS?

HOW DO HACKERS GET THROUGH THE FIREWALL?

- Illegitimate traffic that appears to come from a legitimate source
- Spyware placed directly on your system
- Spreading viruses and worms through email

HOW DOES A FIREWALL DETERMINE LEGITIMATE INCOMING SOURCES?

- By default, a firewall will deny any traffic incoming traffic
- Users create firewall rules that specify what traffic is allowed through the firewall
- Rules that allow traffic from an unverified IP address or open more ports than are required can be exploited by hackers

PROTECTION: A SHARED RESPONSIBILITY

CLOUD SERVICE PROVIDERS ENSURE:

- Appliances are up to date
  - Latest major versions with security patches
- Firewall is up and running
- Infrastructure is immune to subversion

TENANTS MUST:

- Secure their portion of the cloud
  - Configure firewall rules
- Ensure servers are updated to the latest Operating Systems
  - Mainly for the Armor Anywhere users
- Secure Applications and Workloads
- Keep end points up to date and secure

ARMOR FIREWALL RECOMMENDATIONS

- Frequent audit and clean up of firewall rules
- Ensure firewall rules are not overly vague
- Default block, only allow traffic that you have specified
- End Point Firewalls should also be deployed
- Ensure consistency across multiple VPCs

REVISITING OUR FIREWALL EXPERIENCE

TOP COMPLAINTS WE ADDRESSED

1. Rule creation/editing time intensive.
2. Lack of visibility into the status of a rule.
3. Rule edits get stuck.

TOP COMPLAINTS WE ADDRESSED

4	Customer can't resolve error state.
5	Searching for specific firewall rules was a challenge.
6	Hard to audit changes.

DEMO

Q & A

MATTHEW MCGARITY & RAHUL NOWLAKHA

Armor Complete Product Managers

ARMOR | SECURECON 2019 | DALLAS, TEXAS

THANK YOU.

WWW.ARMOR.COM