Selling Deterrence by Denial

Security Products, Hard Targets, and Protecting Your Customers' Crown Jewels
Agenda

Memorize this, there will be a test later

Economic and technical background

Deterrence by denial

Selling deterrence by denial

Recap
My multiple identities

Chief Engineering Officer
Professor
Editor
Author
# Learning objectives

<table>
<thead>
<tr>
<th>Discovering</th>
<th>Discovering what cyber deterrence by denial is, how it works and where denial solutions and products fit within a portfolio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing</td>
<td>Implementing deterrence by denial</td>
</tr>
<tr>
<td>Making</td>
<td>Making the sales case for deterrence by denial solutions</td>
</tr>
</tbody>
</table>
What’s this discussion really about?
Free money!
And, really, who doesn’t like free money?
What are your customers facing?

(Before we get to the free money)
The workforce is changing

Growing numbers of knowledge workers

“Knowledge work occupations adding more jobs than any other ...since the 1980s—about 1.9 million per year.”
- Wall Street Journal

Workforces are distributed, virtualized, and/or outsourced

“70 percent of professionals work remotely — at least one day a week, while 53 percent work remotely for at least half of the week.”
- CNBC

Value is becoming virtual

- Customer information
- Business strategy
- Intellectual property
- Employee PII
- Financial records
- Medical data
Most value is created at the edge

Computers  Mobile Phones  Tablets  IoT
Consequences of value protection failures are severe

GDPR
$22.5M or 4% Global Revenue

CCPA
$7,500 per Violation

NYDFS Cybersecurity Regulation
$75,000 per Day per Violation
Edge device security hasn’t kept pace with value virtualization or the threat

- Computers: Full disk encryption + Antivirus
- Mobile Phones: Full disk encryption + Antivirus (unless it’s an iPhone)
- Tablets: Full disk encryption + Antivirus (unless it’s an iPad)
- IoT: ?
Important, but not enough

- Full Disk Encryption
- Antivirus
Antivirus

Relies on known bad

Can be overcome by malware
Full disk encryption

Safety!

Danger!
All perimeters are porous
That sounds terrifying!
However...
With every risk comes opportunity.
Deterrence by denial
A special kind of scorched earth policy
Situational awareness

All networks are compromised

Breaches cannot be prevented

Attacks are investments
How attackers earn their pay

- Stealing Data
- Making Unauthorized Changes
- Denying Access (Ransomware)
Attackers make CAPEX and OPEX investments, just like any other business.
Target selection is a business decision

\[
\text{IS} \left( \frac{\text{POTENTIAL RETURN} \times \text{PROBABILITY OF SUCCESS}}{-\text{REQUIRED INVESTMENT}} \right) \geq 0
\]

If yes: Arrr!

If no: Next!
Attacks are all about ROI
This perspective disrupts current security culture...

- Security isn’t a duel between cyber-samurai
- Security isn’t matter of perimeter defense
- No need for defenders to be right 100% of the time
...and changes the definition of security to:

Making the attack a risky investment
Disrupting attackers’ economics
Recap: Attacks are all about data

- Stealing it
- Identity theft
- Fraud
- Ransom/Destruction
There's no attack ROI when

Stolen data is unreadable and unchangeable by unauthorized users

Ransomed or destroyed data is easily recovered without significant operational impact
Solution technology already exists!

**Security Requirement** | **InfoSec Concept** | **Technology**
--- | --- | ---
Make data unreadable to unauthorized users | Confidentiality | Cryptography - Encryption
Make data unchangeable by unauthorized users | Integrity | Cryptography – Hashing
Make data indestructible and/or durable | Availability | Backup, Cloud, Decentralization
Technology outcomes:

- Attackers can take encrypted data but can’t read it.
- Data can’t be undetectably changed.
- Redundantly stored data is resistant to destructive attacks.
Operational outcomes create deterrence by denial

- Attackers don’t achieve their ROI goals
- Attackers find a new target (that isn’t you)
There are a number of software products that provide these capabilities.
In the end...
Selling Deterrence by Denial
Turning deterrence by denial into value

- Customer considerations
- Considerations about your organization
- Security product considerations
- Vendor partnership considerations
Customer considerations

- Is there a significant IT investment?
- Is there valuable information on the edge?
- Is the workforce distributed or virtual?
- Is the customer sophisticated enough to understand the risk?
Considerations about your organization

Can your organization make the culture shift needed to include cybersecurity?

Can you teach your customers about the value of their data?

Can your sales team drive cybersecurity sales?

Do you have the bandwidth and resources to support cybersecurity sales?
Security product considerations

What kind of problems does it solve? (E.g., general security or compliance)

What is the product model? (E.g., SaaS)

How is the product deployed?

What training is required?
Vendor partnership considerations

- Is there a free trial or demo period?
- What marketing resources are available?
- Who is responsible for technical support?
- How is the distributor/reseller relationship managed?
The perfect storm

Customer realizes cyberspace is dangerous

Customer calls security superhero (you)
The perfect storm

You sign the customer up for a SaaS product that offers deterrence by denial
The perfect storm

Channel sales automation takes care of...

- Reporting, billing and invoicing
- Payment
The perfect storm

The SaaS vendor takes care of...

- Deployment
- Operations
- Patching/Upgrading
- Compliance
- Support
Outcomes

Happy (and secure) customers

Happy (and profitable) you
Recap

- Changing workforces; increasingly distributed
- Most value is created at the edge
- Edge device security is often lacking
Recap

Attacks are economically motivated

Malicious activity is all about the data, theft or destruction

If stolen data can’t be used, or if destruction has no operational impact, attack ROI is denied
Recap
Recap

Large and growing market for deterrence by denial

There’s room, and profit for you, but...

Make sure your customer and your organization are ready

Choose appropriate products and partners
Questions?
Contact

@ACFirestone

https://www.linkedin.com/in/adamfirestone/
Thank you!