
cl@b2015
What's hiding in your web app perimeter?
FIBA
FELABAN 50 anos

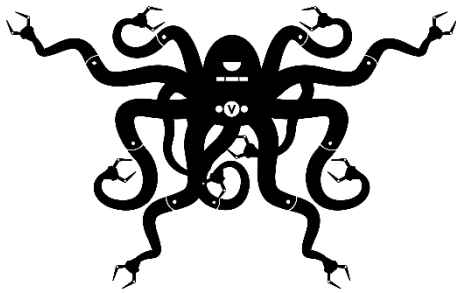
What's Hiding in Your Web App Perimeter?

- **Jason Kent** - @jkentakula
  - Wireless (802.11) Infrastructure Security
  - Web Content Security
  - Web Application Security
  - Bee Keeper
  - IOT enthusiast
  - First SQLi 1998

VERACODE

- Booth
- Building AppSec programs since 2006
- Billions of equivalent lines of code scanned
- Application Security Focused
- We are the monster

in your corner.



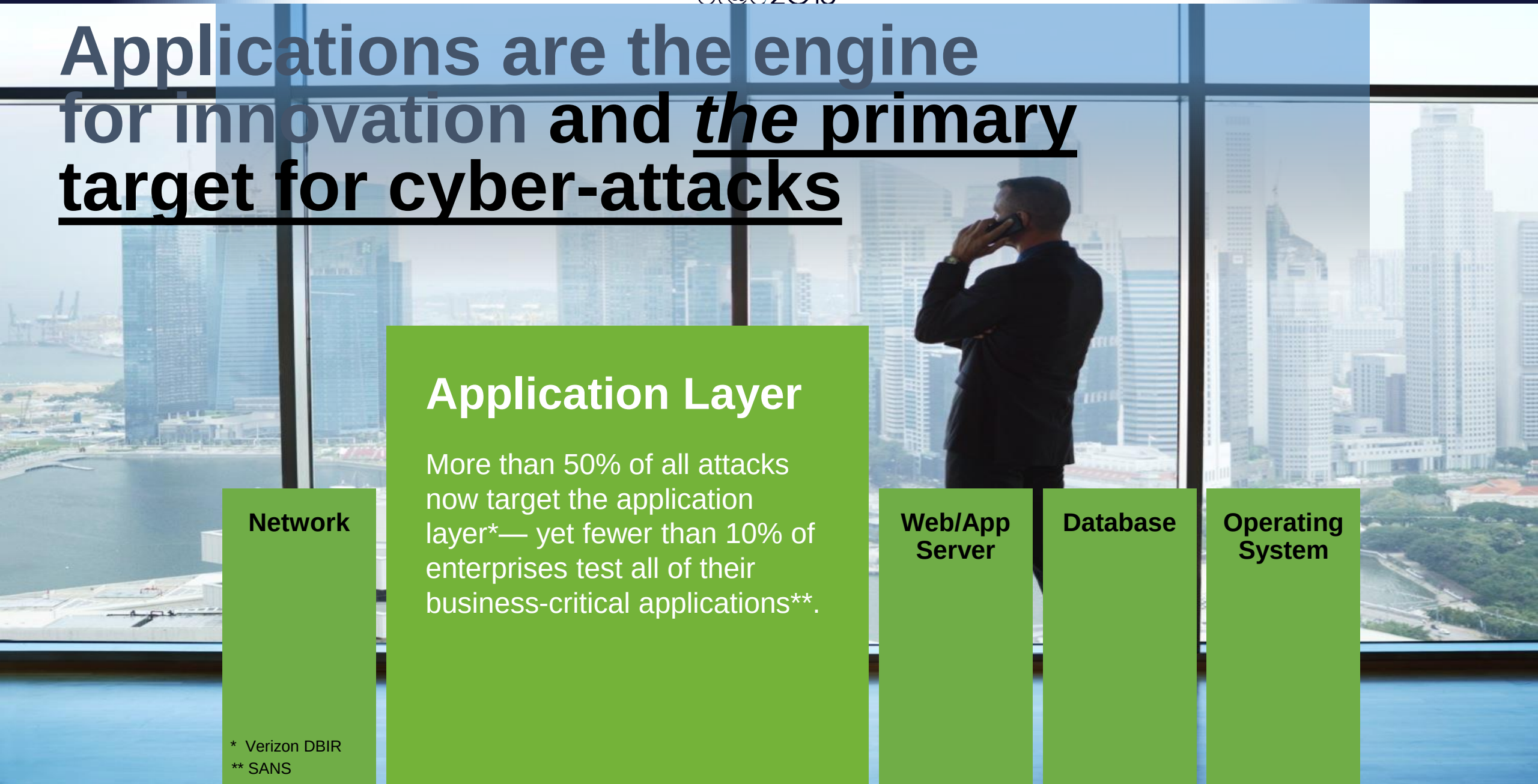
WHO FIXES THE MOST VULNERABILITIES?

What is the percentage of known vulnerabilities remediated by each industry vertical, in order to reduce application-layer risk?

The data represents 208,670 application assessments submitted for analysis during the 18-month period from October 1, 2013 through March 31, 2015 by large and small companies, commercial software suppliers, open source projects and software outsourcers.

VERACODE

Applications are the engine for innovation and *the* primary target for cyber-attacks



Application Layer

More than 50% of all attacks now target the application layer*— yet fewer than 10% of enterprises test all of their business-critical applications**.

Network

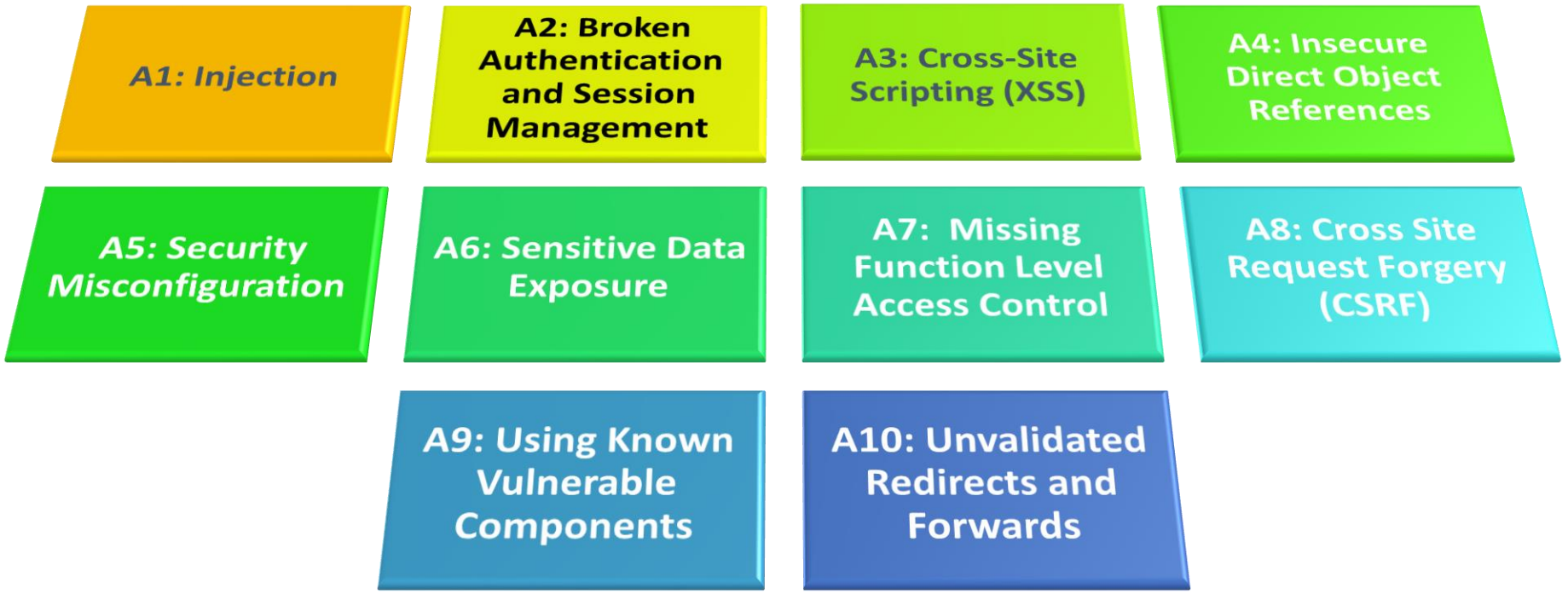
Web/App Server

Database

Operating System

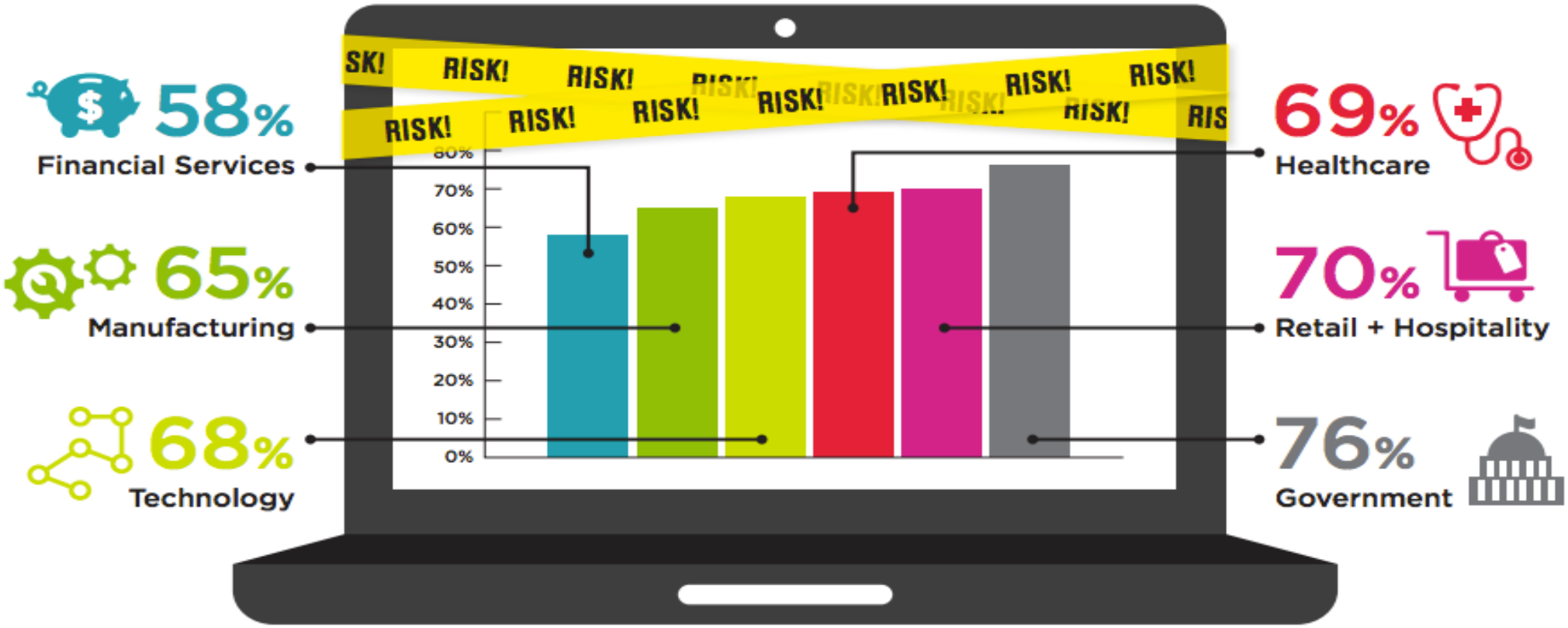
* Verizon DBIR
** SANS

OWASP Top 10


A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Control
A8: Cross Site Request Forgery (CSRF)
A9: Using Known Vulnerable Components
A10: Unvalidated Redirects and Forwards

FAILED OWASP TOP 10

How many apps fail the OWASP Top 10
upon initial risk assessment?



The data represents 208,670 application assessments submitted for analysis during the 18-month period from October 1, 2013 through March 31, 2015 by large and small companies, commercial software suppliers, open source projects and software outsourcers.

VERACODE

A general question.

- How many of you in the room work at an organization that writes any amount of software?

Over an 8 year range

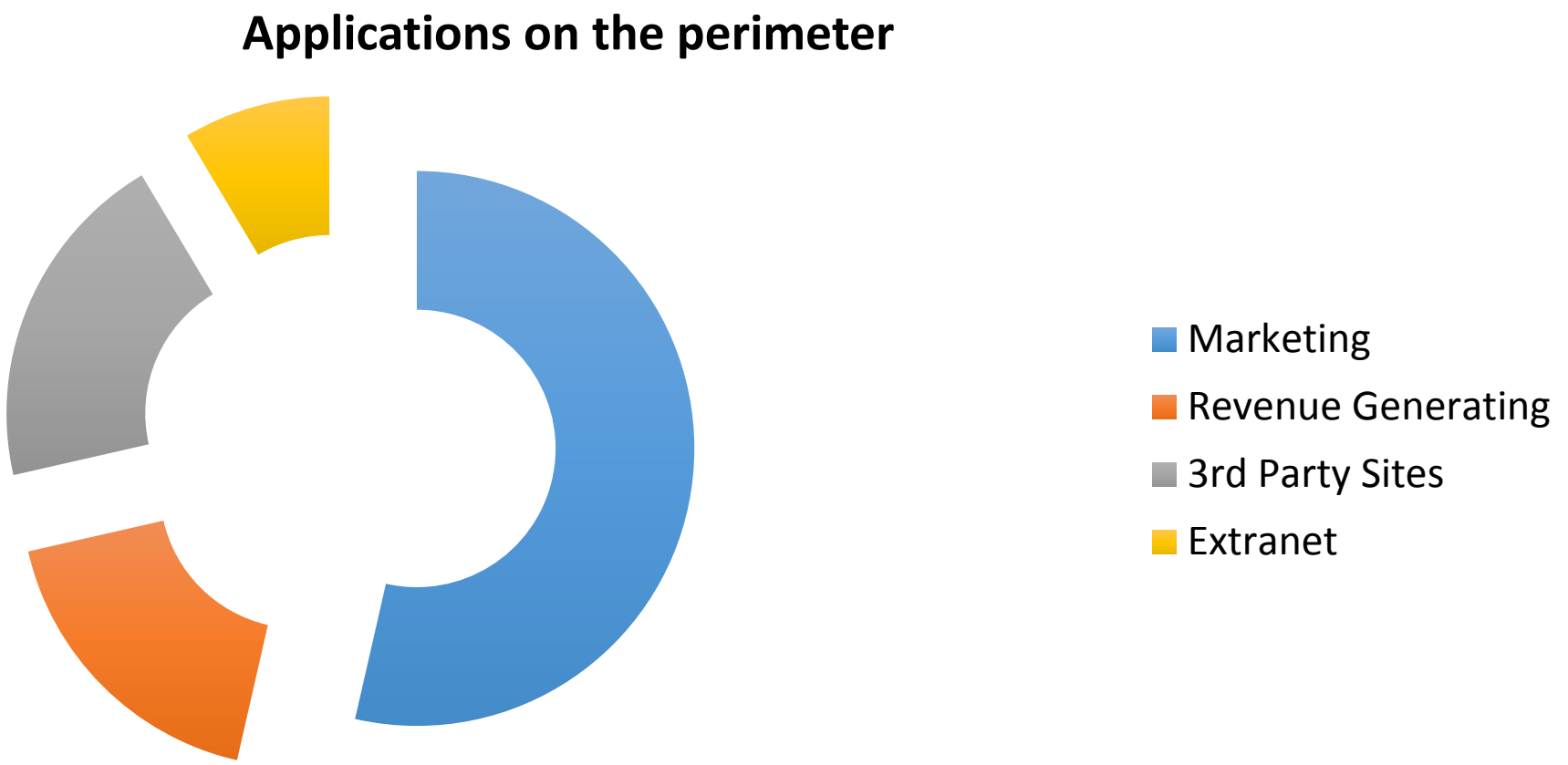
- How many flaws per MB have we seen?

70 Flaws per MB

1MB is 1000 – 20000 lines of code

Average Mobile Phone game is roughly 20MB

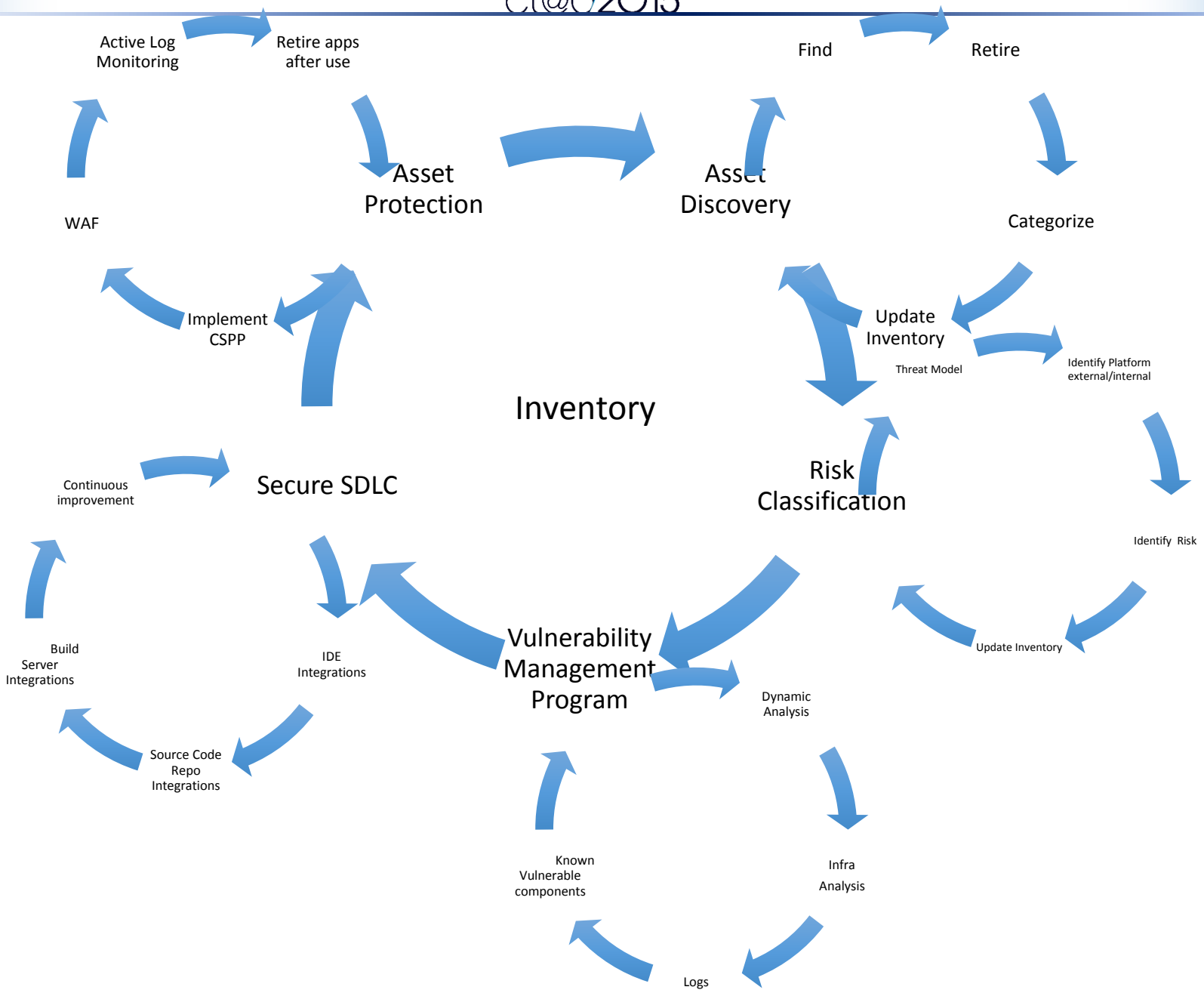
What is your web footprint like today?



Do you know how many web applications you have?

- The answer is probably no.
- If you know the answer, you are probably off by 30%
- If you don’t know you have it, it’s a vulnerability.

What does a good Application Security program look like?


Active Log Monitoring
Retire apps after use
Find
Retire
Asset Protection
Asset Discovery
WAF
Categorize
Implement CSPP
Update Inventory
Threat Model
Identify Platform external/internal
Inventory
Continuous improvement
Secure SDLC
Risk Classification
Identify Risk
Update Inventory
Build Server Integrations
IDE Integrations
Vulnerability Management Program
Dynamic Analysis
Source Code Repo Integrations
Known Vulnerable components
Infra Analysis
Logs

Lets get the basics right.

- Rule number 1, if you haven’t done the first thing you must do that.
- Rule number 2, see rule number one.

Asset Discovery – Inventory your footprint

- Every application can lead to some type of data on your footprint.
- Even something as simple as password reuse can lead to a huge problem. - Chase
- Knowing what is out there can lead to finding logo reuse and branding problems. - Rolex
- Systemic problems can be identified. - Patching

But what about….

- RASP?
- IAST?
- WAFs?

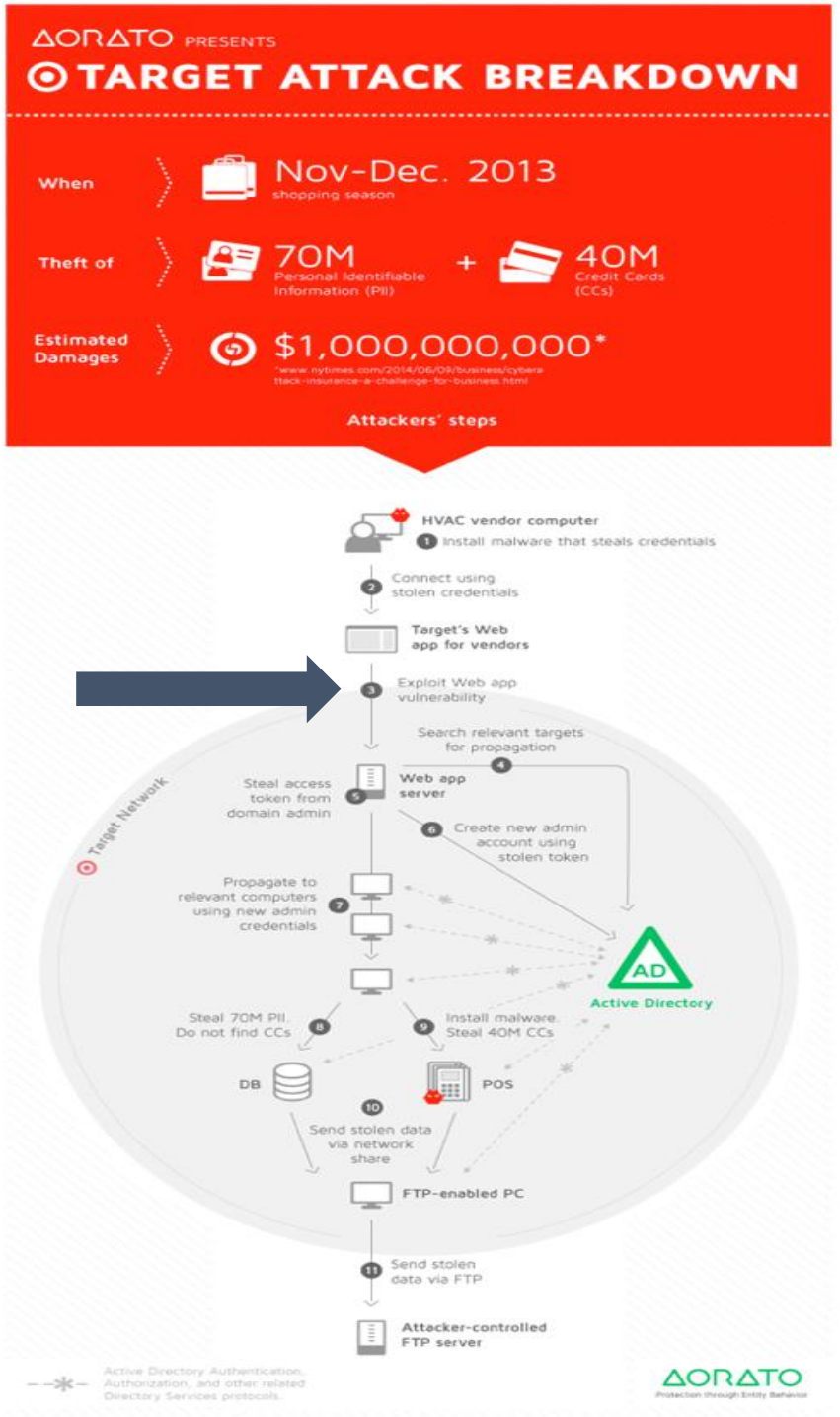
See rule number 1!

Target - an example of not knowing enough

- Entry point to Target was through a vendor's computer
- Credentials were found that allowed access to be gained to a Target Web App
- **An exploit was found in the Target Web App**

The attackers used this as their bridgehead and Propagated throughout the organization

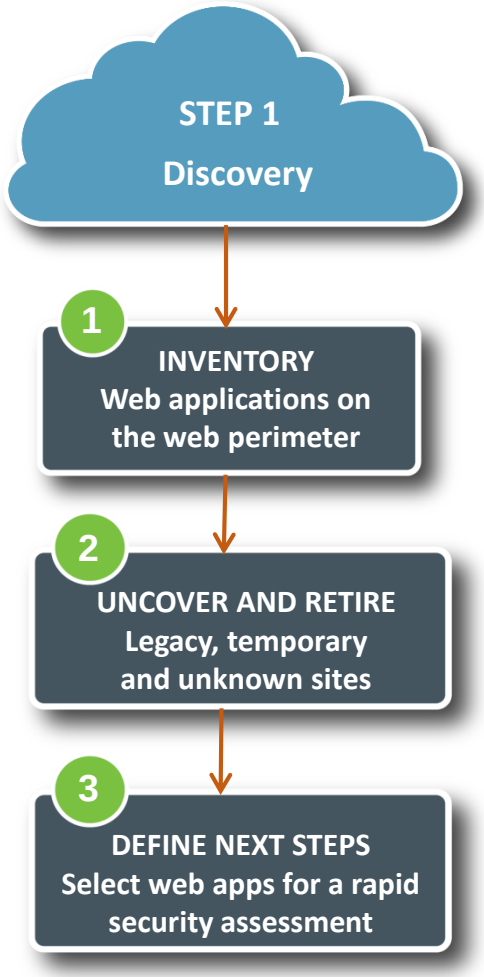
Veracode Application Perimeter Monitoring is designed to reduce the count of flaws and exploitable attack surface



Chase Bank

- Chase sets up a charity fun run with an organization.
- Chase Employees sign up/register.
- Site breached, username/passwords acquired.
- Password reuse leads to Chase systems breach.

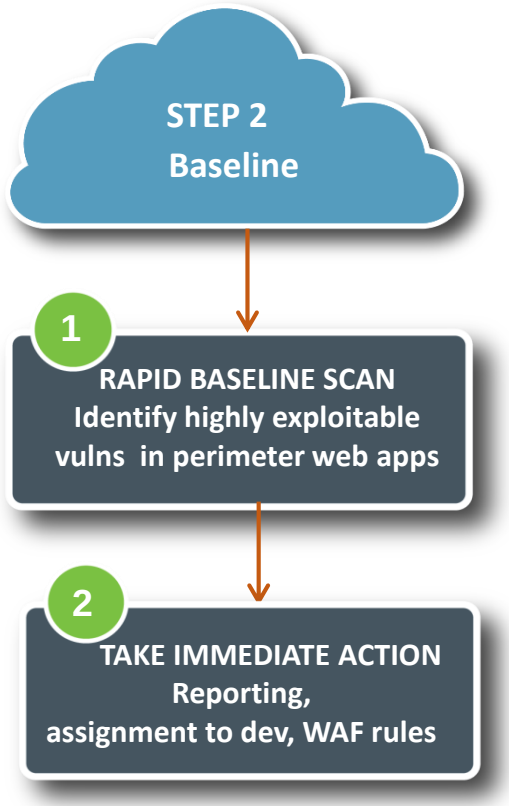
Get an INVENTORY!!!



Start with a list of domains, IPs, project names, etc.

Easily identify legacy sites

Start testing NOW!

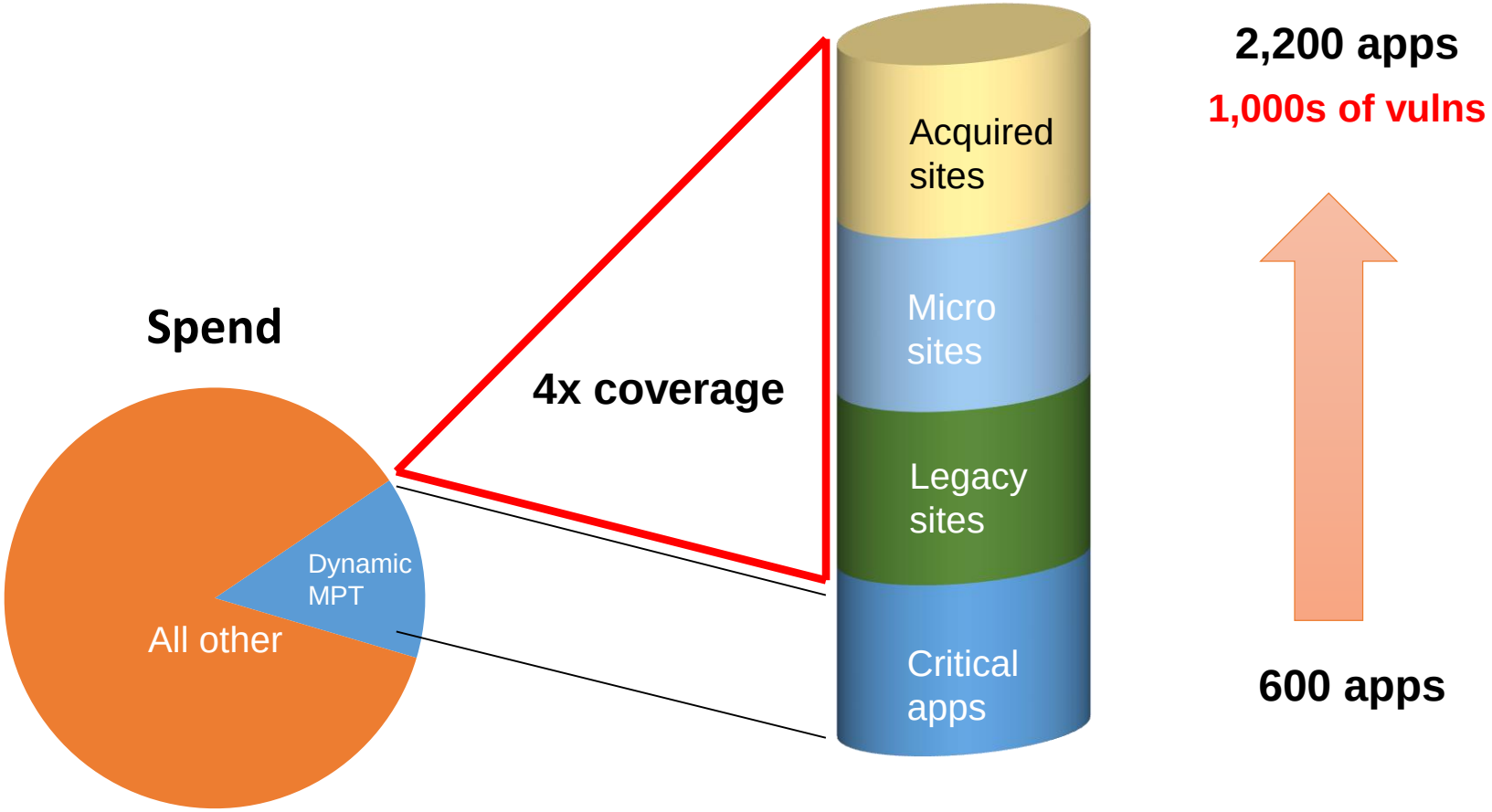


Take action on newly discovered apps

Add to your vulnerability management program

Increased coverage for same spend

Global Financial Services Organization



Helping Enterprises Succeed:

How a global manufacturer massively leveraged the web to engage consumers

- ✓ Need: Extend security coverage across all critical applications worldwide
- ✓ Results: Massive scalability
  - Examined 30,000 domain names & IP addresses
  - Assessed 3,000 applications in 8 days
  - Now continuously monitoring and remediating every month
  - Reduced critical and high vulnerabilities by 79% in 8 months

The New York Times

Bits Blog, July 31, 2014

"…one of the principles I apply to information security isn't security-related at all. It's about ***simplification and consolidation****. My geeky term for it is 'attack surface* ***reduction.'"***

- Brad Maiorino, Target CISO

What's hiding in your web application perimeter?

- E-Commerce Applications
- Legacy Applications
- Shadow IT Applications
- Brand Associated Applications
- Vulnerabilities

Questions?

- Q&A

Thank You

- Andrew Foxcroft – VP of Channels
- Jake Alosco – Channel Account Manager
- Jason Kent – Technical Director, Channels