Enterprise Security Products

Jonathan Martin
HP Enterprise Security Products

Agenda

- Today's Threat Landscape
- Application Intelligence
- Threat Intelligence
- Summary

Agenda

- Today's Threat Landscape
- Application Intelligence
- Threat Intelligence
- Summary

The Threat is Real

Target Shares Drop After CEO (Steinhafel's Resignation

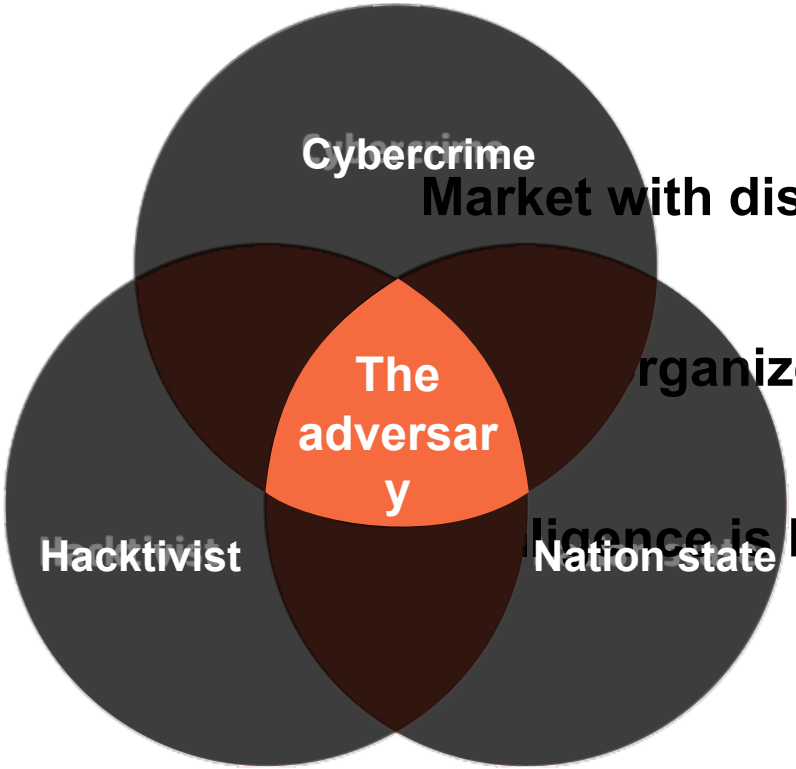
+ Comment Now + Follow Comments

What Target and Co aren't telling you: your credit card data is still out there

Hackers have an open window that no fallen CEO has bothered to close, because the retail industry is looking for security in all the wrong places

Brian Krebs
theguardian.com, Tuesday 6 May 2014 11.30 BST
Jump to comments (4)

Defining the adversary

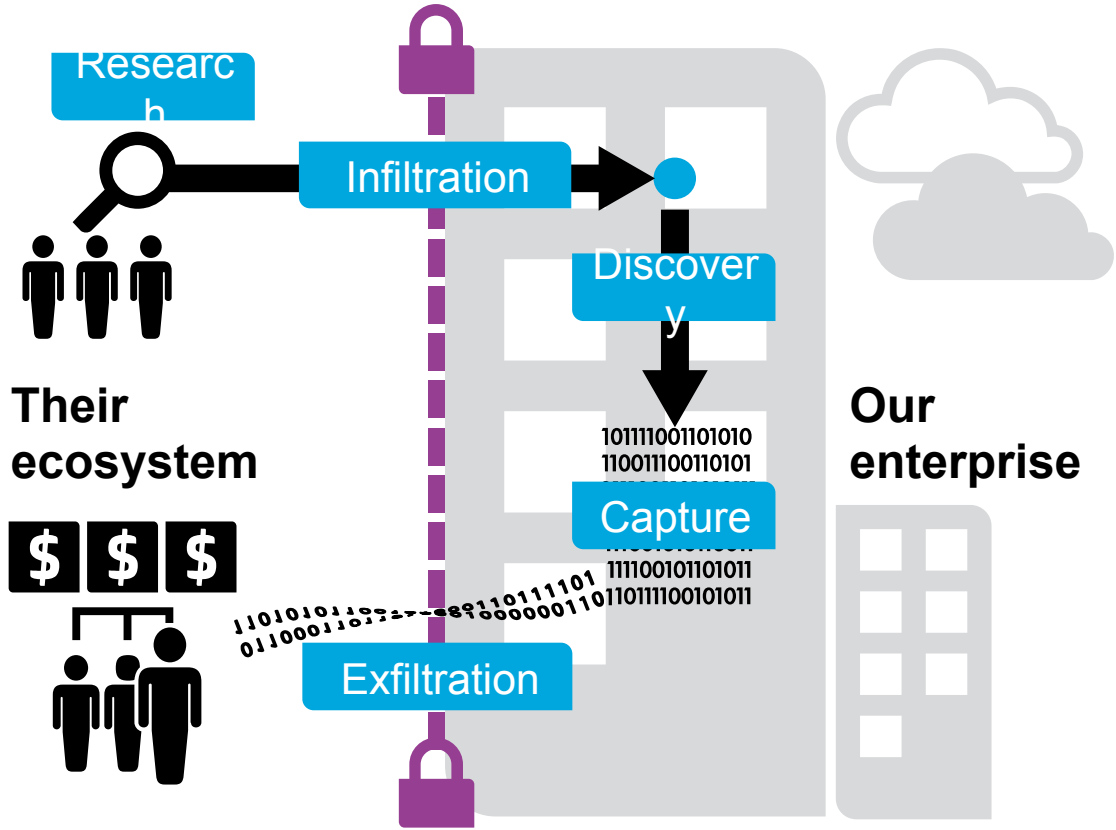


Market with distinct process

rganize and specialize

ligence is bought and sold

Organize our capability to disrupt the market



84% of breaches occur at the application layer

68% increase in mobile application vulnerability disclosures

94% of breaches are reported by a 3rd party

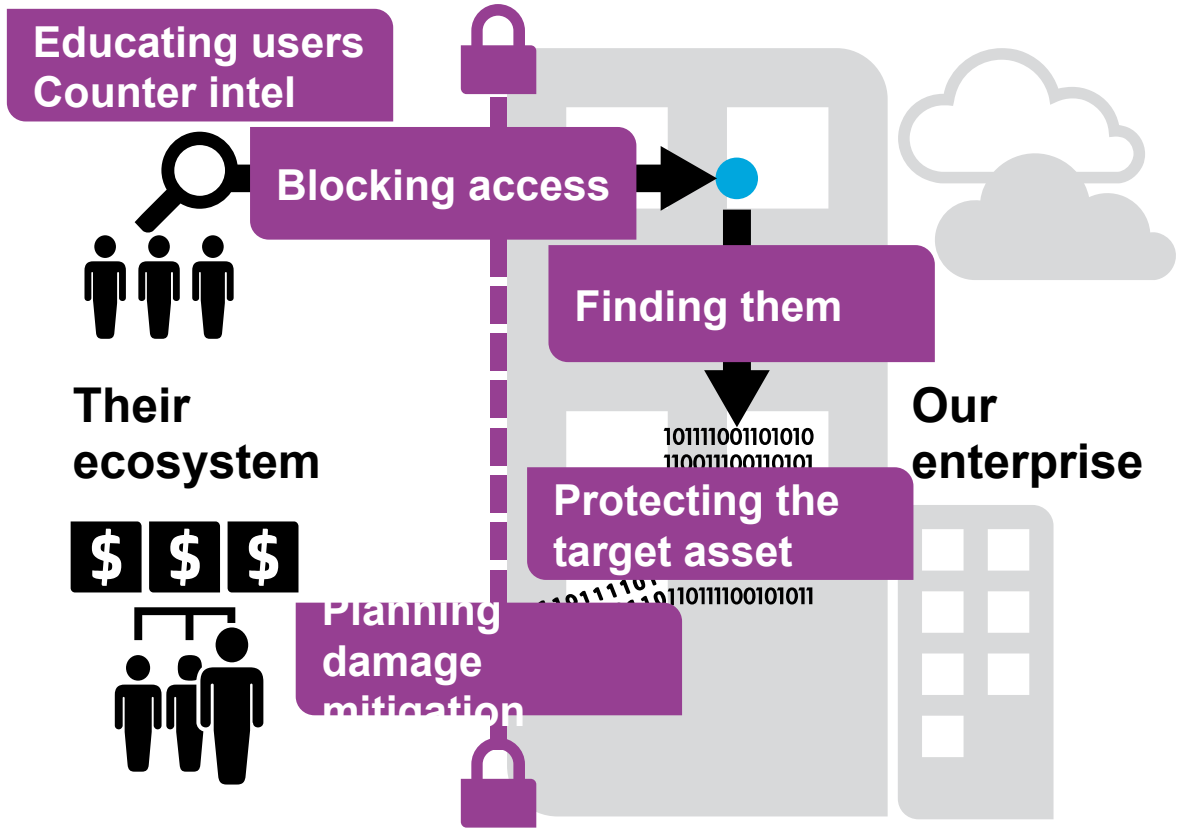
Since last year, time to resolve an attack **has grown**

243 days

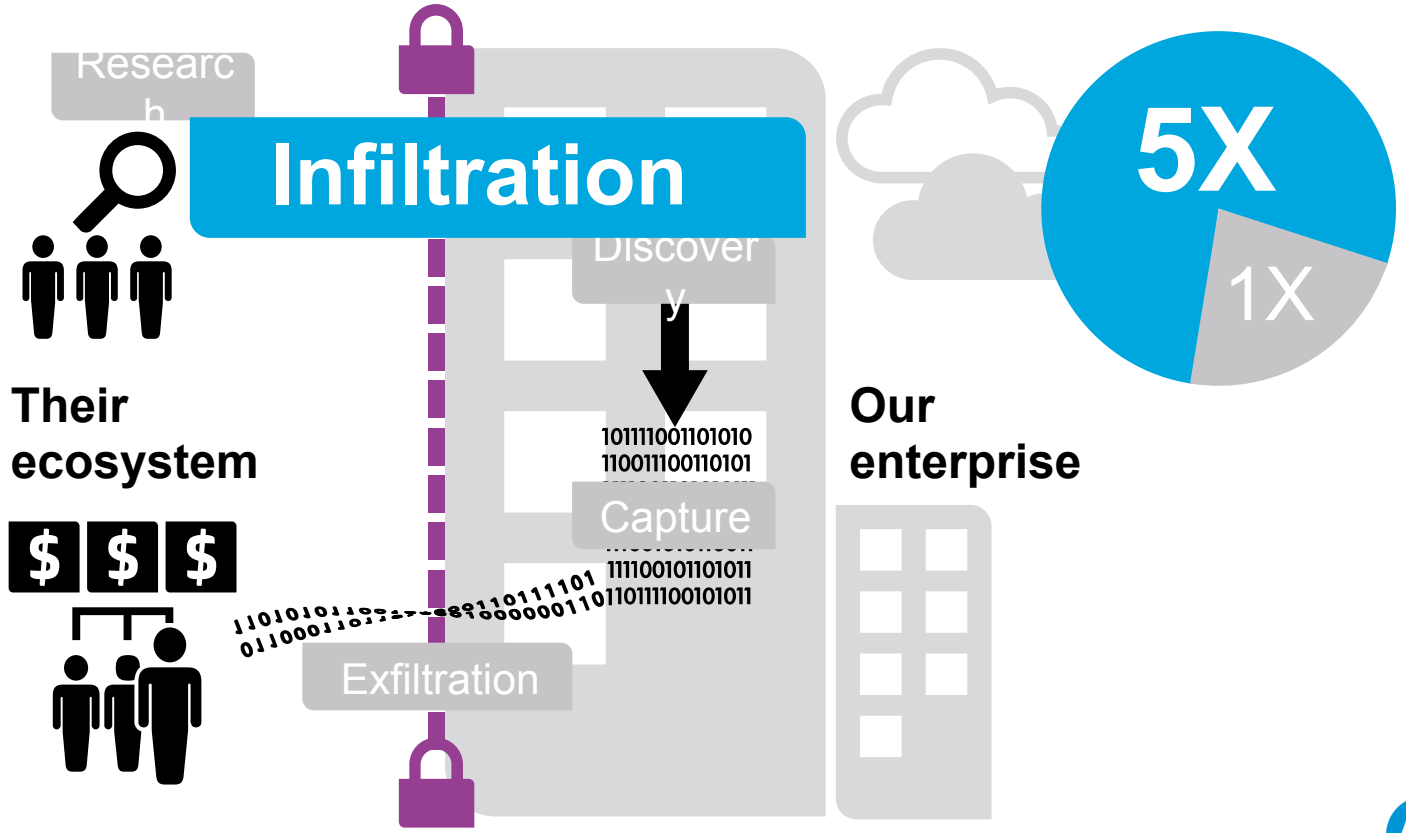
average time to detect breach

2013:**September** October November December **2014** January February March April **May**

Organize our capability to disrupt the market



Rethink our capability investments



Agenda

- Today's Threat Landscape
- Application Intelligence
- Threat Intelligence
- Summary

Agenda

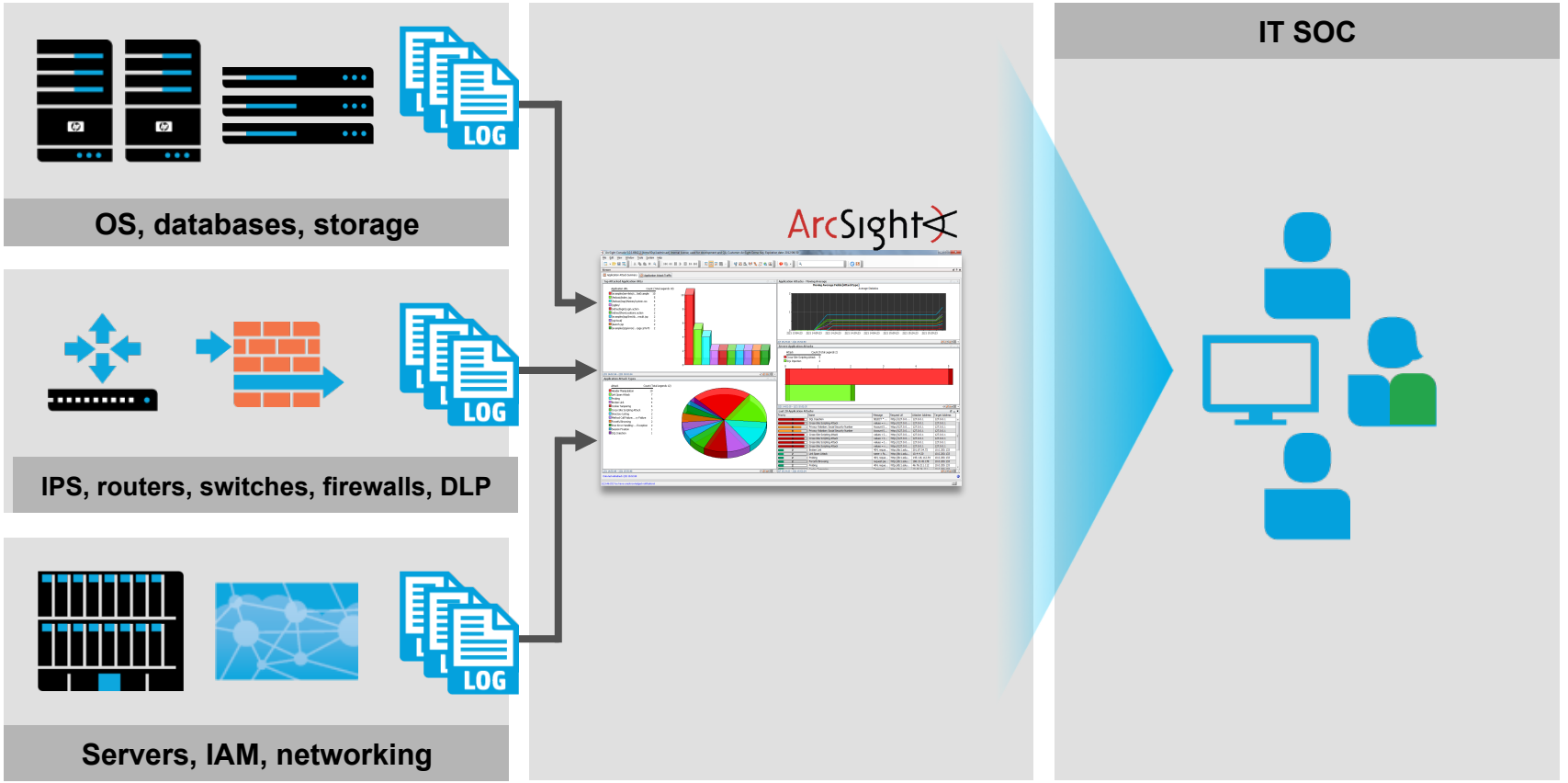
- Today's Threat Landscape
- Application Intelligence
- Threat Intelligence
- Summary

The Challenge

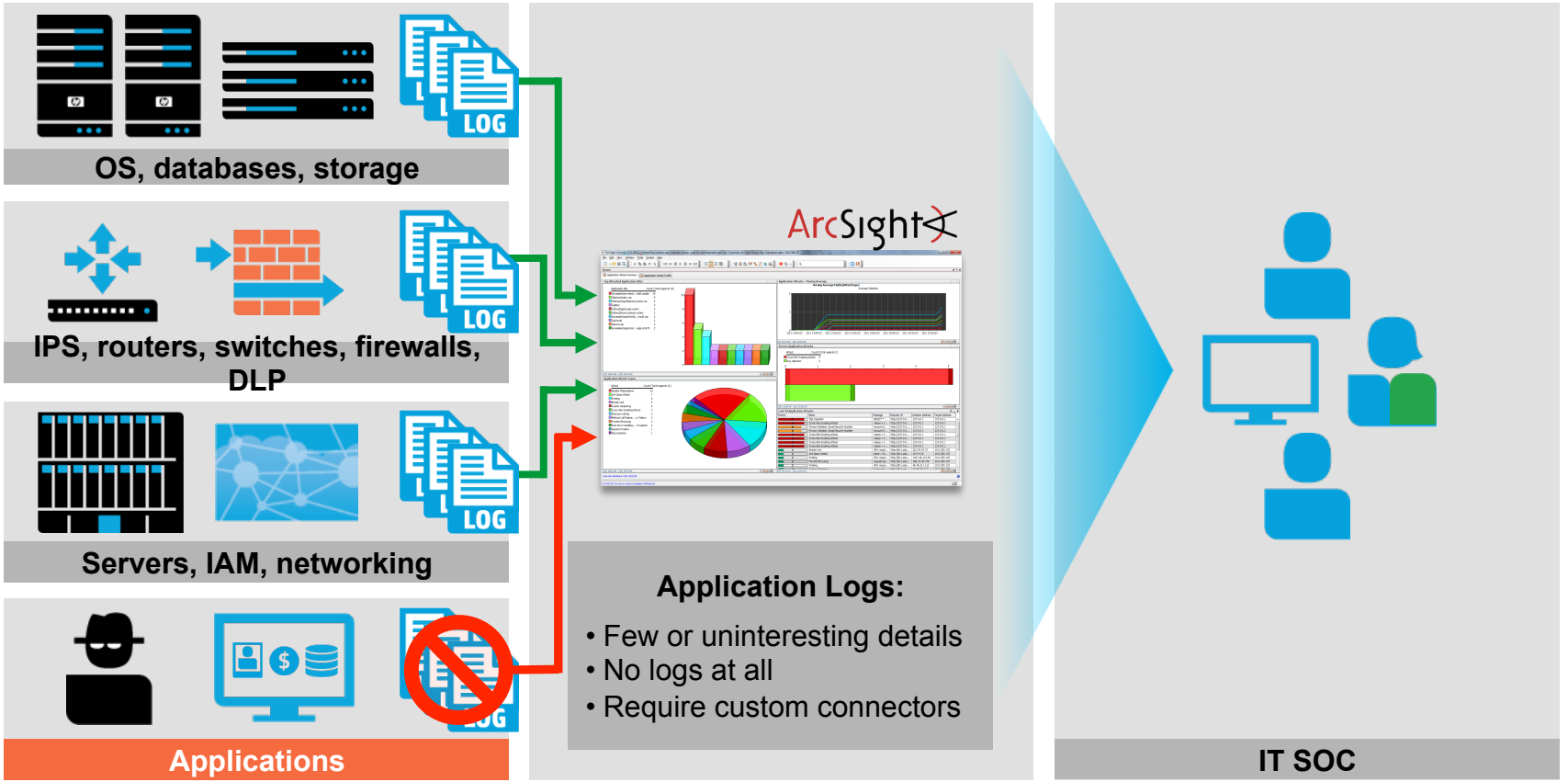
84% of breaches that occur are application related

*Gartner, 2013

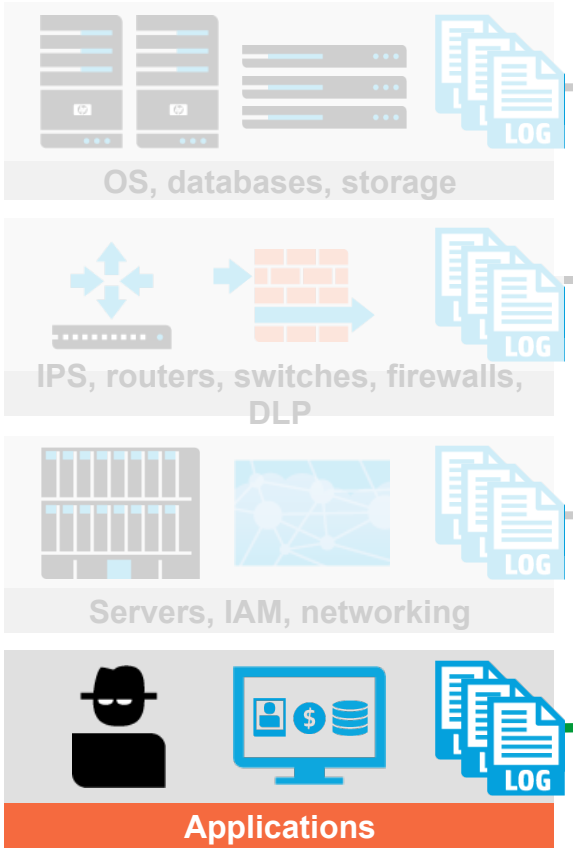
Typical Security Monitoring Today



Application Visibility is Limited



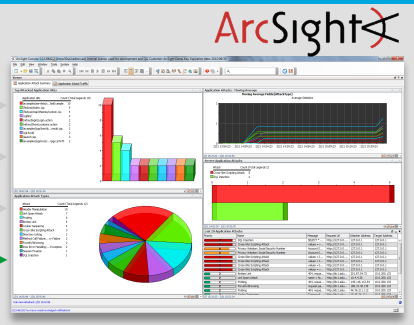
ArcSight ESM with Application View

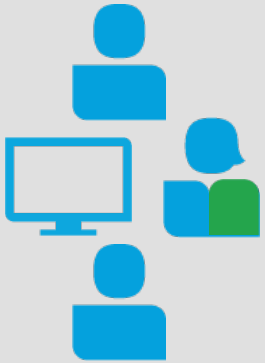


Introducing Application View

Know you apps. Know your users. Know your data!

FORTIFY An HP Company





- Retro-fits applications with security event logs
- No change to application required
- Out-of-box ready for ArcSight ESM

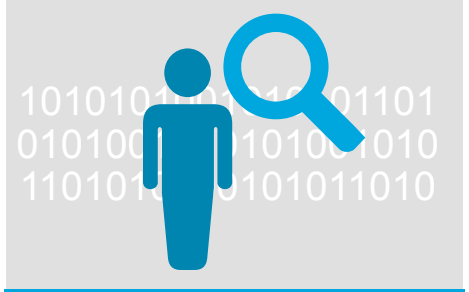
Application View: What is it?

Application View provides software application log visibility for security event analysis and correlation to help you:

Know your apps

- Remove the blind spot
- Application intelligence
- Application monitoring
- Out of the box views

Know your users



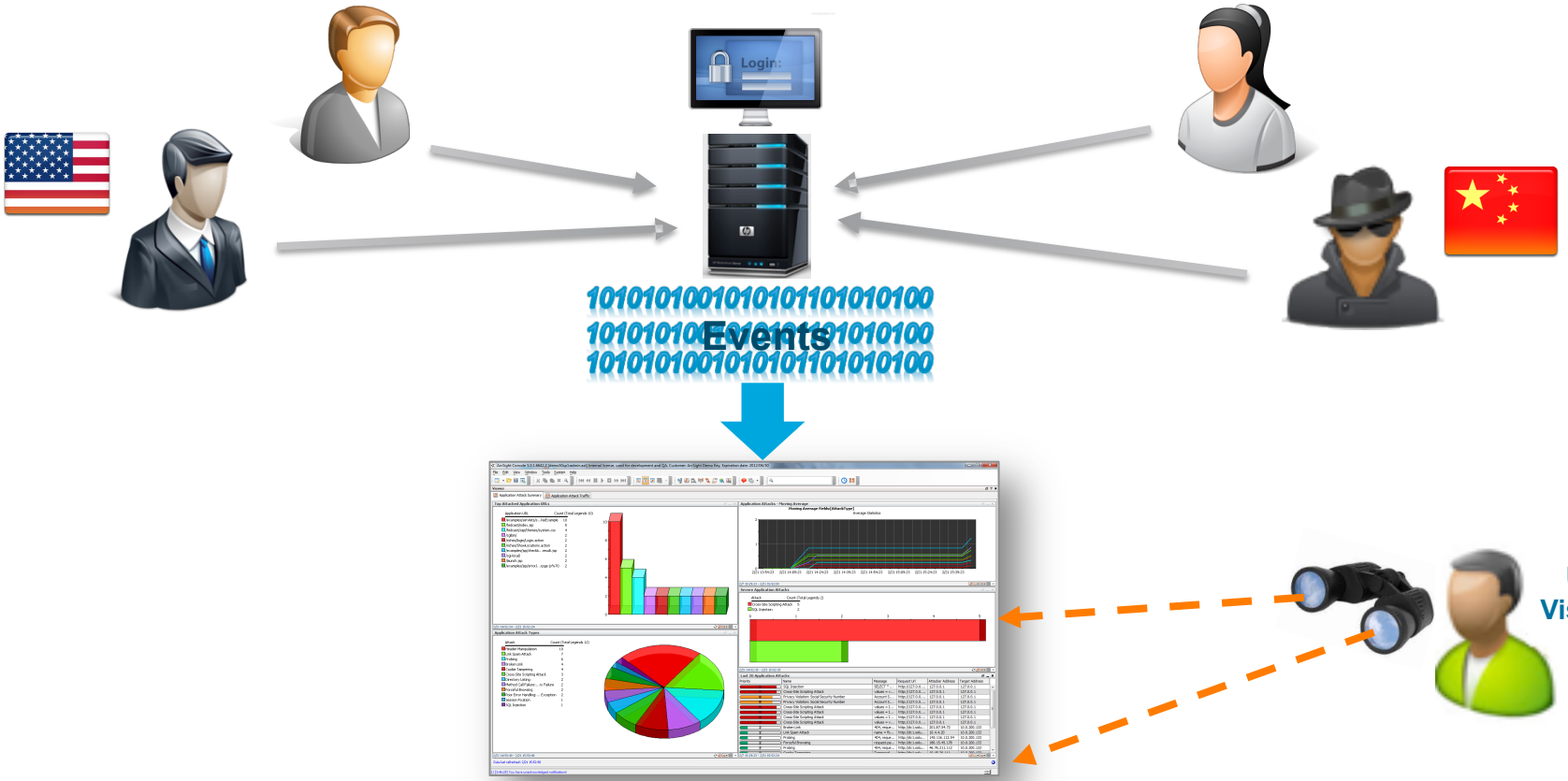
- Monitor user access
- Identity fraud
- Track user activity
- Protect against ID theft

Know your data

- Track resource access
- Identify data leakage
- Review security forensics
- Identify application errors

Scenarios

User Tracking: Track users and their behavior

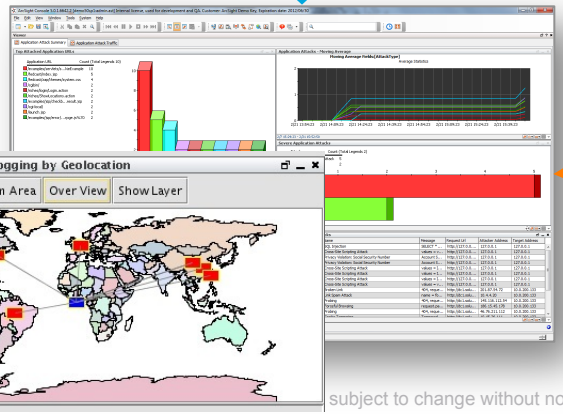


Resource Tracking: Track everything a user does

User Tracking: Geo Location Discrepancy

Action: login
User: eddie
Login time: 1/1/13, 10:00pm
Place: Sunnyvale, CA, USA

Action: login
User: eddie
Login time: 1/1/13, 10:05pm
Place: Shanghai, China



User Visibility

Multiple Authentications from the same IP

Agenda

- Today's Threat Landscape
- Application Intelligence
- Threat Intelligence
- Summary

Agenda

- Today's Threat Landscape
- Application Intelligence
- Threat Intelligence
- Summary

Threat Intelligence

Reputation-based intelligence to further reduce business risk

RepSM combines reputation intelligence with SIEM real-time correlation for early detection, analysis, prioritization, and remediation of advanced threats

Correlates security events with vetted security intelligence to

- Prevent spread of persistent threats
- Block exfiltration of sensitive information
- Improve SOC efficiency in handling incidents
- Protect the reputation of your own enterprise

Use cases

Prevent Attacks

Before a breach occurs RepSM can detect **dangerous browsing** of ill-reputed sites, potentially preventing a compromise

Identify Infection

After a breach occurs RepSM can **identify infected assets or infrastructure** trying to communicate with ill-reputed command and control centers, potentially before intellectual property is leaked out of the company

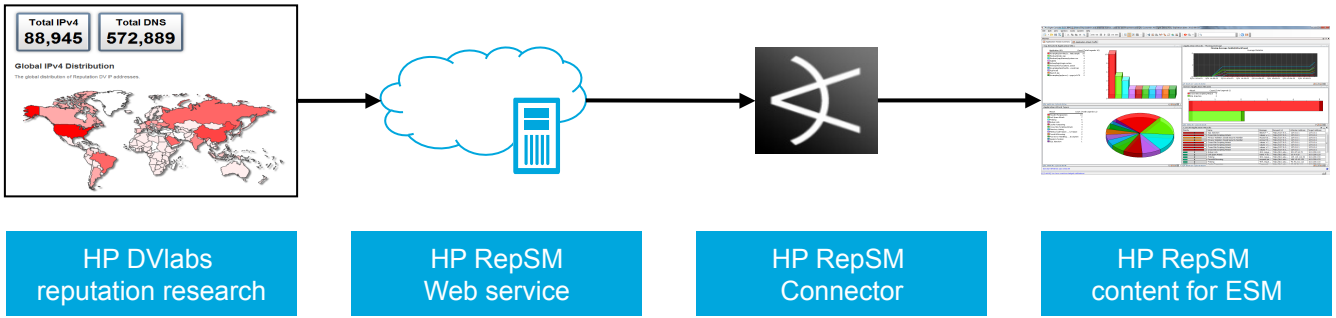
Protect reputation

Given that most breach victims are notified by a third party, RepSM can proactively check the enterprise's **own customer-facing assets and web sites** to verify none have landed on the threat list, potentially blocking access by customers and business partners.

How does it work?

RepSM actively manages “reputation-based” security policies to detect and prevent communication with “known bad” actors.

- Research and insight from global security community
- Intelligence fed to SIEM for real-time correlation
- Detects and prioritizes threats through correlation of suspicious activity
- Active response taken in response to malicious activity utilizing TP integration



DVLabs is the recognized security research leader

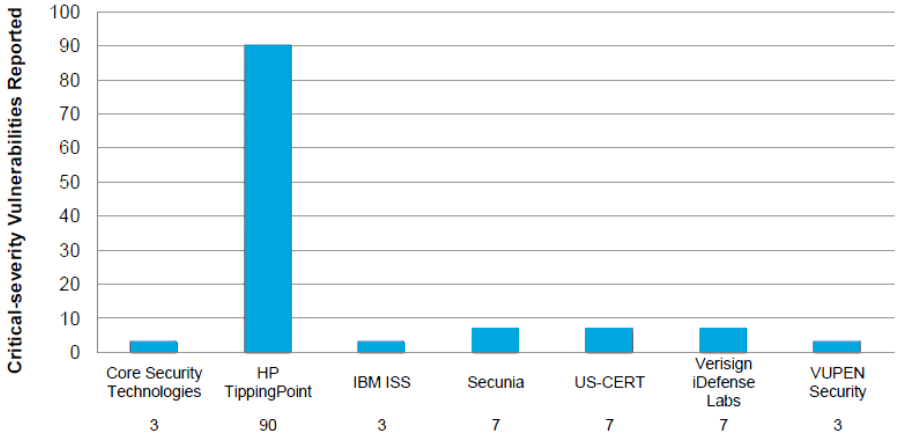
Frost & Sullivan Market Share Leadership Award for Vulnerability Research –

3 years in a row!

At any time, 200 to 300 zero day vulnerabilities only HP knows about

Analysis of vulnerabilities by severity

HP TippingPoint continues to lead in critical severity vulnerability disc

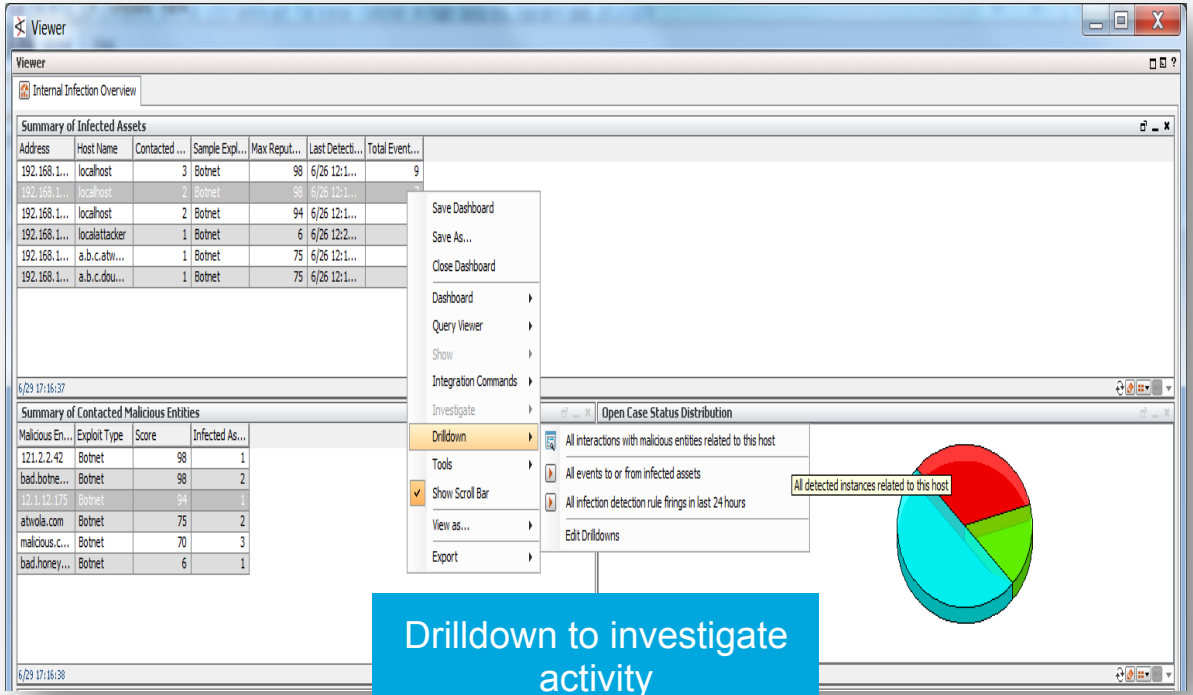


Note: All figures are rounded. The base year is CY 2011. Source: Frost & Sullivan analysis

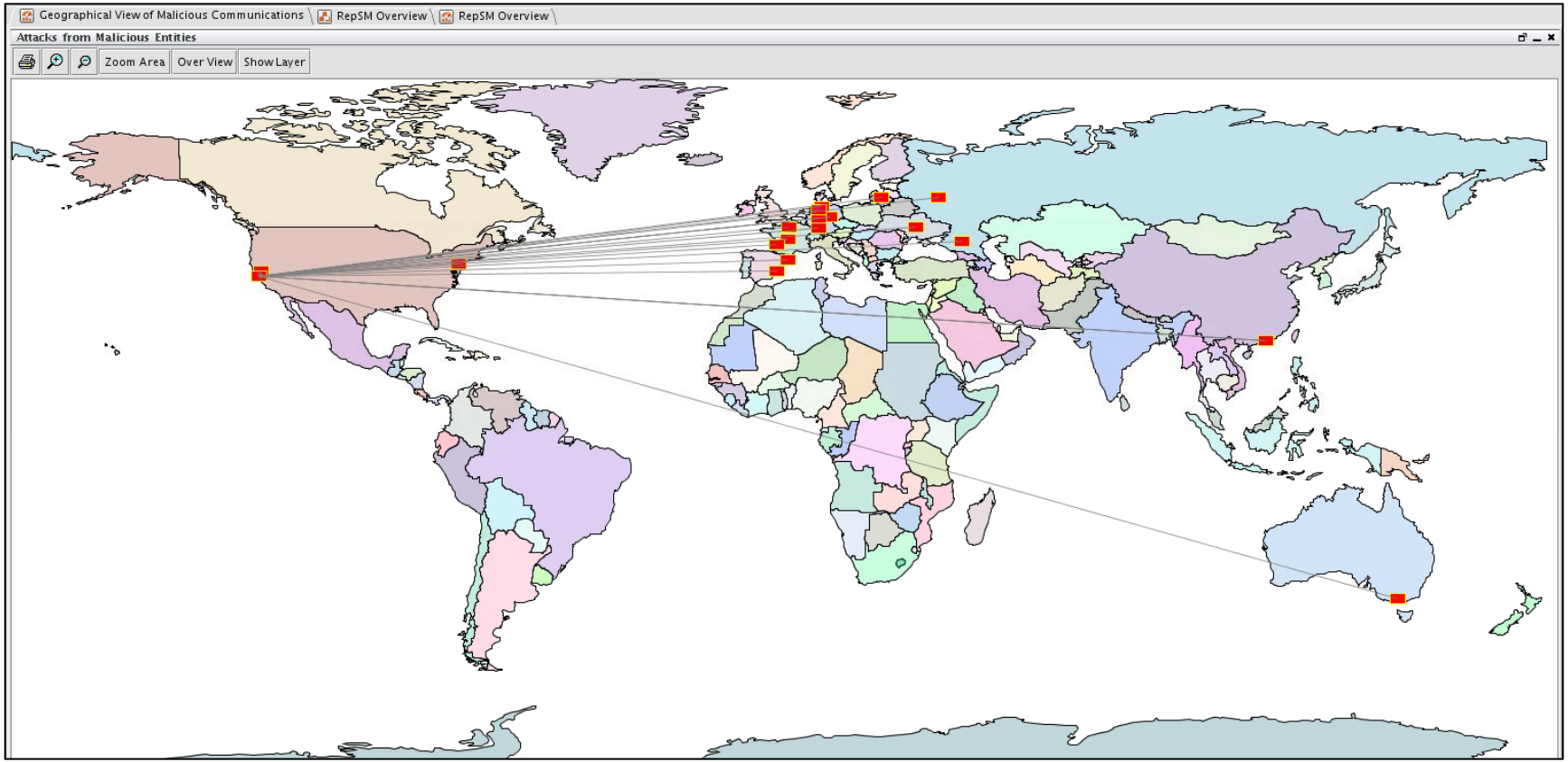
And this is how it looks in RepSM

Internal Infected Assets

Malicious hosts they accessed



Drilldown to investigate activity



Agenda

- Today's Threat Landscape
- Application Intelligence
- Threat Intelligence
- Summary

Agenda

- Today's Threat Landscape
- Application Intelligence
- Threat Intelligence
- Summary

Why HP ArcSight?

100,000

Breadth & depth of collection

350+ SmartConnectors to collect logs, events, and flows from 350 distinct log generating sources

350+

Speed of collection

The connectors enable collection up to 100,000 EPS, a speed that nobody else can match in the market. HP-IT, an internal HP's IT organization collects flows at 150,000 EPS

100,000 EPS

Ultra-fast & full-text search

Advanced filtering and parsing with rich metadata on unified machine data enables search speeds at over 2 million EPS

2,000,000 EPS

Scale linearly with big data

Modular solution helps you to grow linearly with big data, analyzing and storing at compression at 10:1

10:1

Huge savings through SIEM

Average companies $1,700,000 through SIEM implementation per Ponemon Institute research

$1,700,000

Reduction in compliance audits

Automating these compliance is one time task and saves 90% of time every quarter from each audit

90%

Make it matter.

Thank you