McAfee by Intel

GDPR

Opportunity for Security Transformation

Mo Cashman
Director, Enterprise Architects
Intel Principle Engineer
EMEA

How is *Your* Strategy Evolving?

Threats

Defenses

Environments

Threat Evolution - Changing and Familiar Face of Hacking

Cybercriminals / Organized Crime

Recreational / Vandals

Hacktivism / Reputation Attacks

State Sponsored Cyberespionage Cyberattacks

Digital Transformation and GDPR

Device and Data Proliferation

Increased Attack and Loss Surface as users go mobile and businesses become more data rich

Cloud Services

Increase risk of loss as more data and services are moved to or delivered from the cloud

DevOps

Applications are developed and put into production with vulnerabilities that can lead to data exposure

Cloud Services and GDPR

What are the key questions I need to ask of my CSP?

What are my responsibilities for security?

I don't have expertise, I need security as a service

Defining Your Journey

1 FOUNDATION

COMPLIANCE CENTRIC

2 OPERATIONAL

THREAT DRIVEN

3 TRUSTED

BUSINESS ALIGNED

3 Think like an Executive

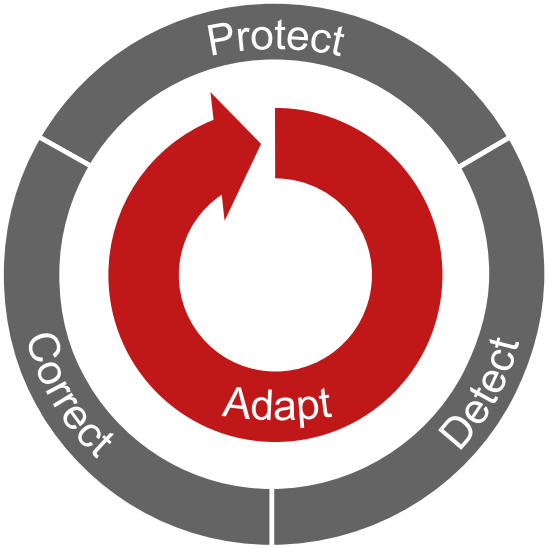
2 Think like the Attacker

1 Think like an Auditor

*internal testing

**with SIA Partners

Operational Data Security – Capability Strategy



PROTECT – Continuous discovery and attack surface reduction against accidental, intentional and unintentional incidents across enterprise and cloud operating environments.

DETECT – Continuous processes and orchestrated workflows to identify, analyze and validate key indicators of a data breach and understand the full scope of a data breach

CORRECT – Efficient processes and orchestrated workflows to contain a breach through pre-planned response actions such as privilege and data isolation

ADAPT – Orchestrate protection updates and automated intelligence-sharing to identify or prevent a reoccurrence of an attack in the enterprise, cloud or industry partnerships

Operational Data Security Considerations

Lost Devices

About 40% of all data exfiltration incidents are reportedly carried out with the use of physical media.

External Attackers

About 59% of data loss incidents are the result of malware or application exploits from external attackers

Employees and Suppliers

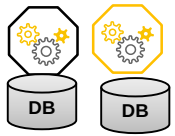
About 57% of data loss incidents are the result of accidental or malicious insider activity

Over 50% of data loss incidents discovered externally!

Operational Data Security - Key Processes

Discovery and Classification

Identity and Access Management



Application Security

Breach Reporting

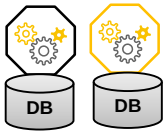
Compliance Reporting

Operational Data Security – Prevention Strategy

Covering the Attack Surface

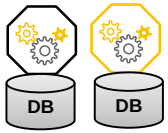
Mobile Devices and Office Services

Cloud Storage



Databases

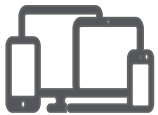
SaaS Services



Apps and API

Privileges

Covering Loss Vectors



Accidental Device Loss

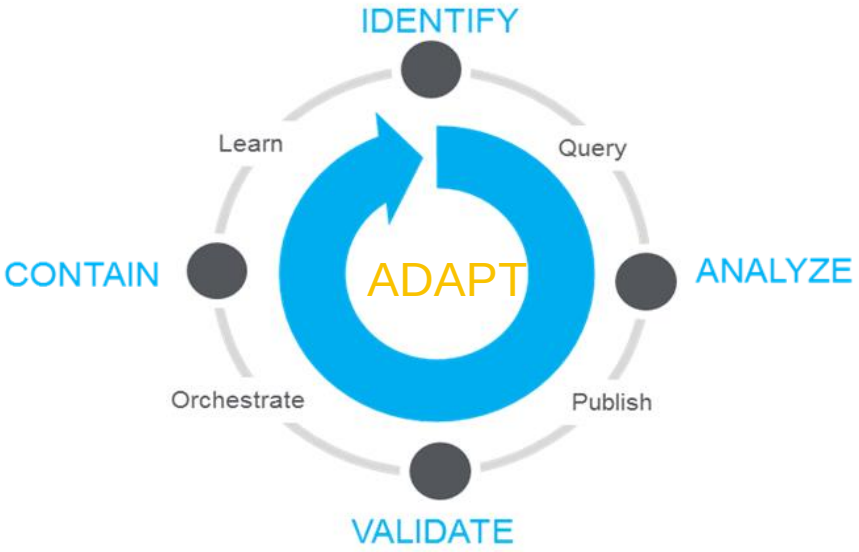
Policy Violations

Cloud Services

Malicious Exfiltration

Insider Threat

Operational Data Security – SOC Strategy



Visibility

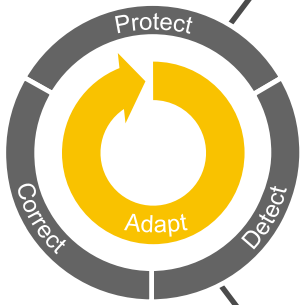
Analytics

Triage Workflow

Response Actions

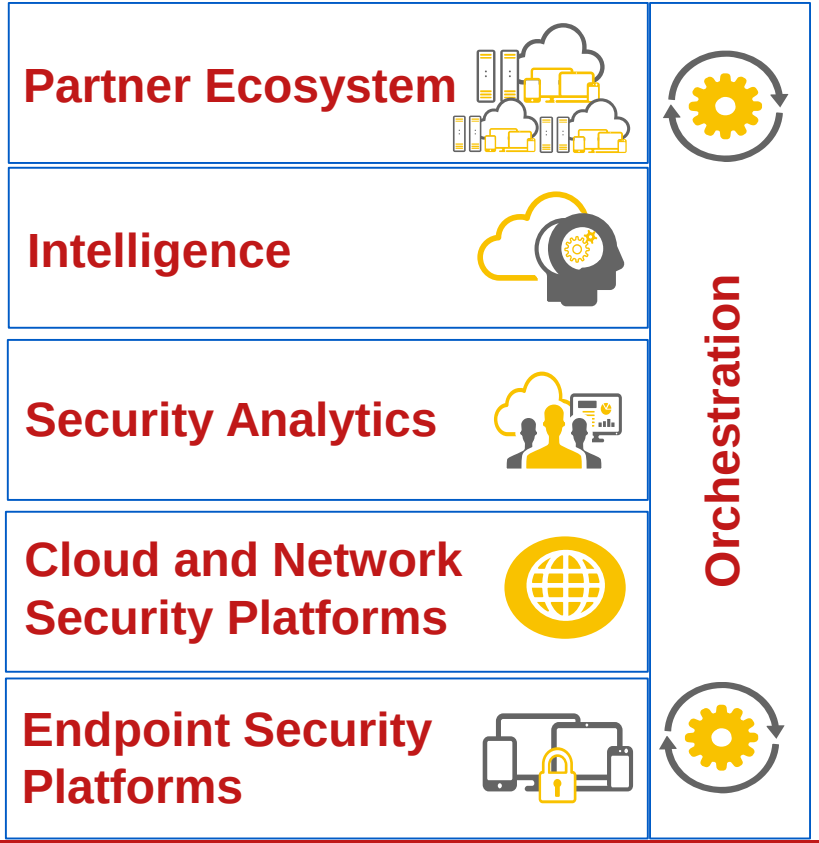
Remediation

Think Security Outcomes



Neutralize Advanced Persistent Threats	Advanced Threat Protection, Detection and Response
Protect Customer and Business Data	Data Loss Protection for Data in Use, At Rest, in Motion anywhere
Protect Critical Environments	Threat Protection and Visibility for Datacenter, Cloud servers and apps
Optimize Security Operations	Fast Threat Detection and Response

Think Security Systems



Think Collaboration

Call to Action

Opportunity for Real Change

Think Security Systems

Positive Culture