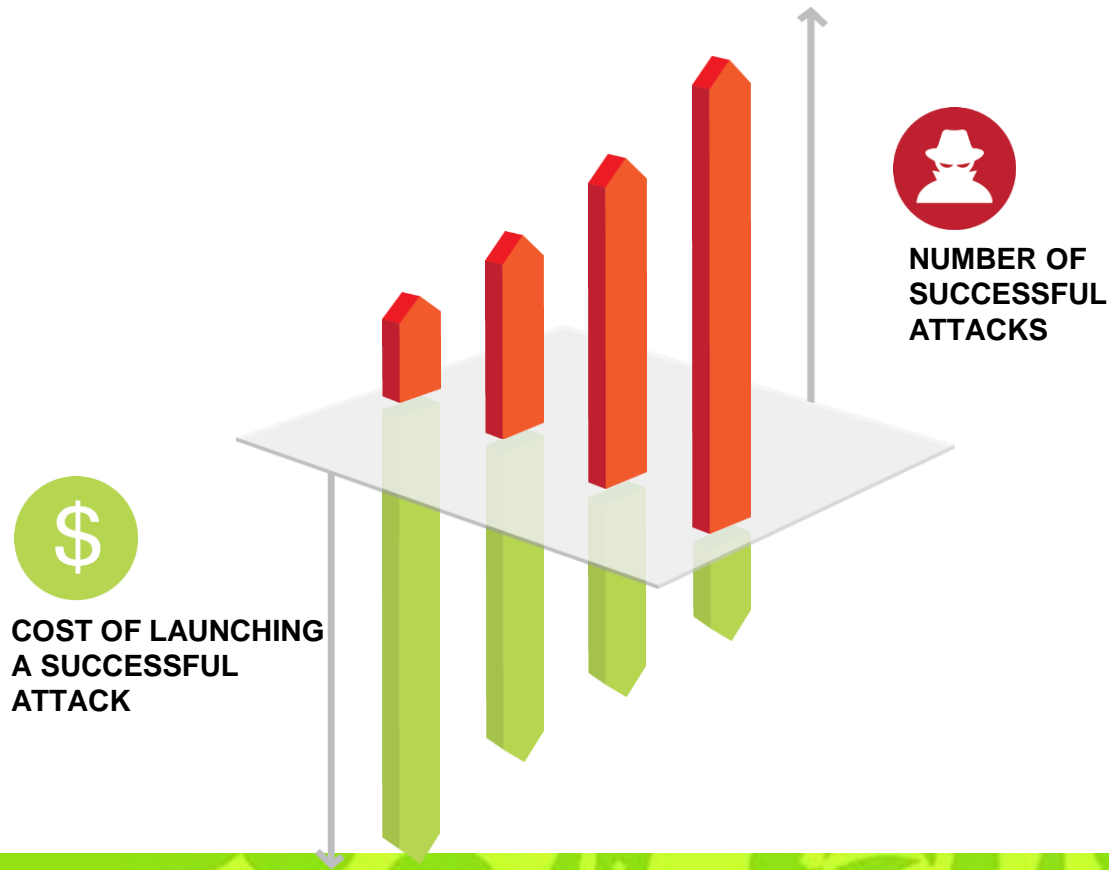


**ITAPA 2017 International Congress
Technology and Humanity
Bratislava, Slovakia
14-15 Nov '17**

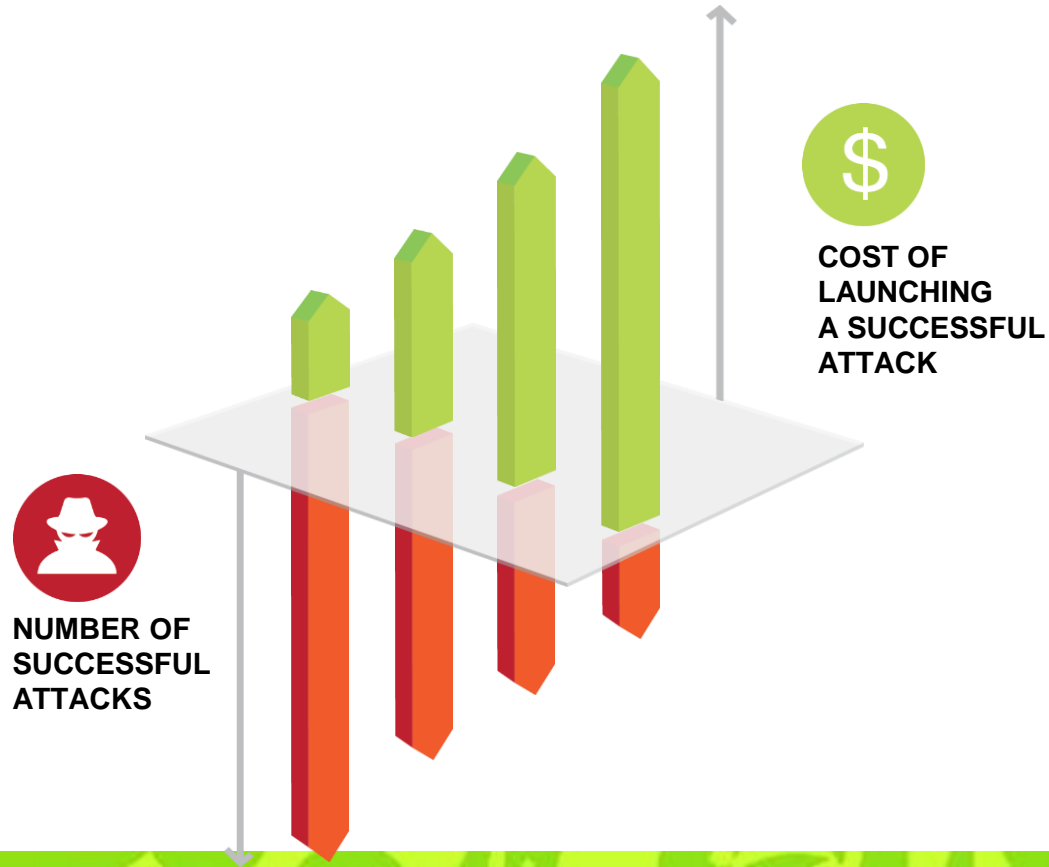
***How **technology** development has
empowered **cyber threats** and the
cybersecurity community's **needed response*****

John A. Davis
Major General, U.S. Army (Retired)
Vice President and Chief Security Officer (Federal)
Palo Alto Networks

We Must Restore Trust



Changing the Cost of Successful Attacks



Today's Problem



The world of technology and the world of the security designed to protect technology are moving in opposite directions

6 Major Trends

Simpler and Easier

More Convenient

Fewer People

Natively Integrated

More Automated

Designed to Prevent

*These trends are driving the movement to Mobile, Virtual, Cloud and IoT

World of Technology

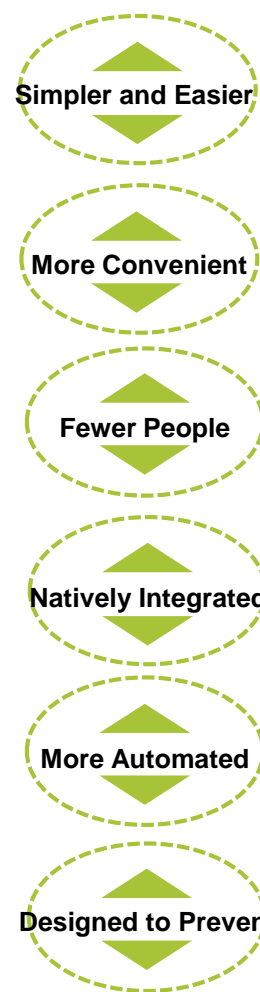
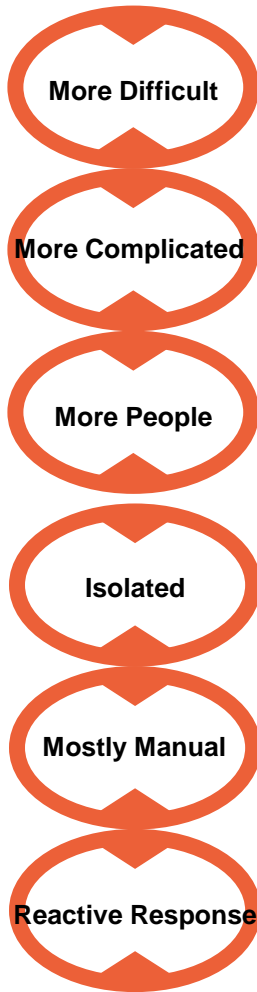
*These trends generate requirements that drive innovation

*User and operator experience:

- Fused
- Smooth
- Pleasant

6 Major Trends

*These trends are challenged with the movement to Mobile, Virtual, Cloud and IoT



*These trends are driving the movement to Mobile, Virtual, Cloud and IoT

*Innovation within these trends is actually making the problem worse



*User and operator experience:

- Piecemeal
- Friction filled
- Overwhelming
- Downright painful



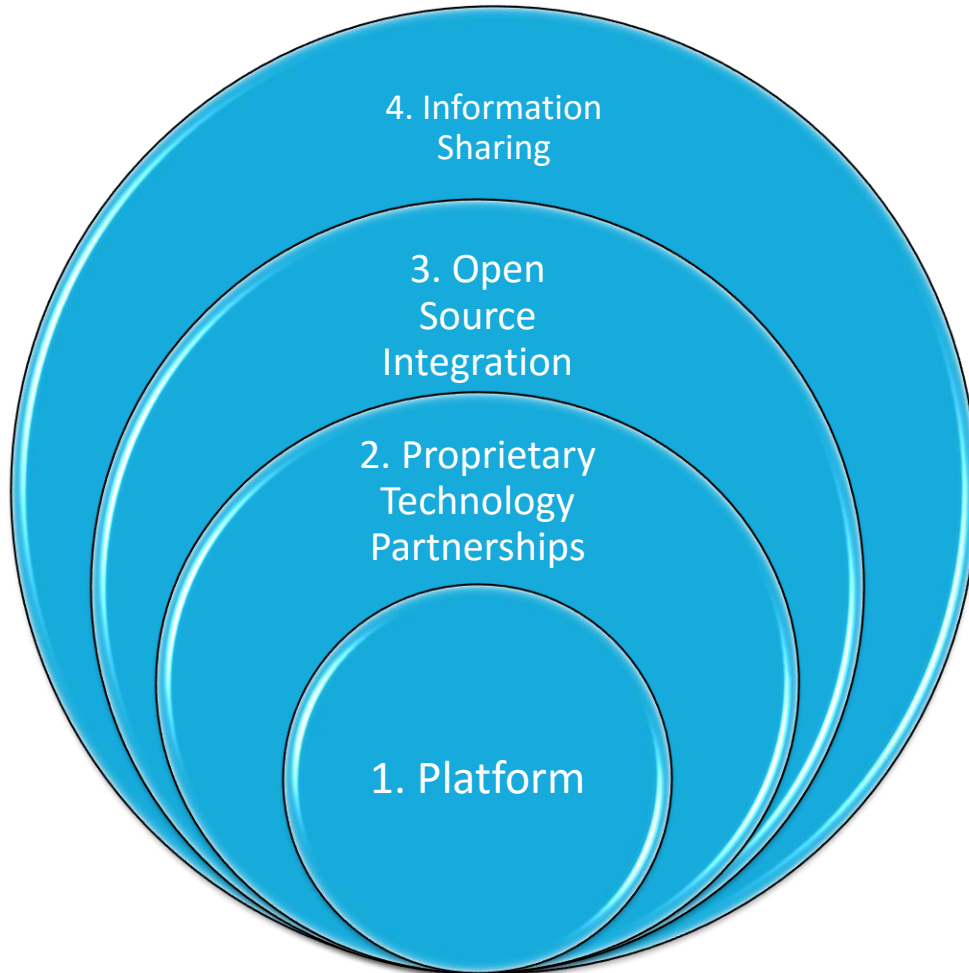
*These trends generate requirements that drive innovation

*User and operator experience:

- Fused
- Smooth
- Pleasant



Integration is leverage



4. Information Sharing: Sharing threat information through formal and informal relationships and *integration* with public and private sector network defenders.

3. Open Source Integration: Leveraging the practice of API enables *integration* of various technologies and defensive capabilities deployed by an enterprise through plug and play.

2. Partnerships: Customized deep technical *integration* of complementary technology with market leading companies.

1. Platform: Prevention at the Network, Cloud and Endpoint levels through natively *integrated* capabilities that are designed from the beginning to work together, are automated, and are context driven to provide visibility and deliver prevention controls across the threat lifecycle in all network environments.

Attack Life Cycle

Playbooks



CYBER ESPIONAGE	
CYBER CRIME	
CYBER HACKTIVISM	
CYBER WARFARE	
CYBER MISCHIEF	
CYBER TERRORISM	

Exfiltrate Intellectual Property for Profit

Steal Credit Card Information / Demand Ransom

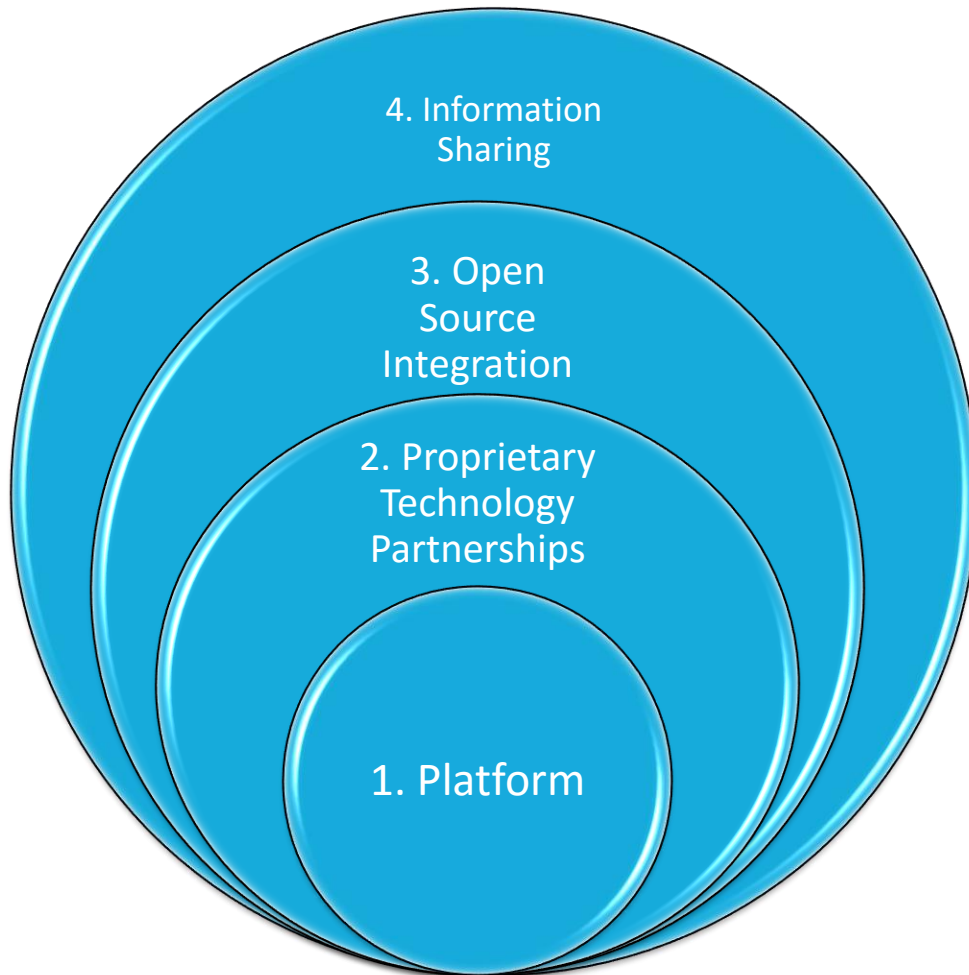
Dox embarrassing email messages

Destroy military capabilities / critical infrastructure

Deface websites / cause disruption

Create fear by threatening employees

Integration is leverage



4. Information Sharing: Sharing threat information through formal and informal relationships and *integration* with public and private sector network defenders.

3. Open Source Integration: Leveraging the practice of API enables *integration* of various technologies and defensive capabilities deployed by an enterprise through plug and play.

2. Partnerships: Customized deep technical *integration* of complementary technology with market leading companies.

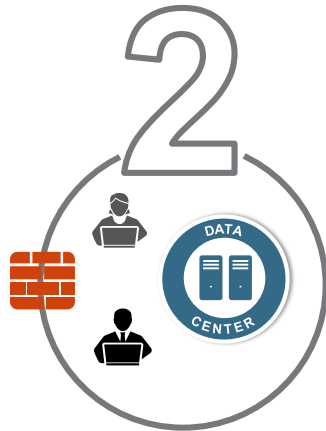
1. Platform: Prevention at the Network, Cloud and Endpoint levels through natively *integrated* capabilities that are designed from the beginning to work together, are automated, and are context driven to provide visibility and deliver prevention controls across the threat lifecycle in all network environments.

Threat Life Cycle Occurs Across All Environments

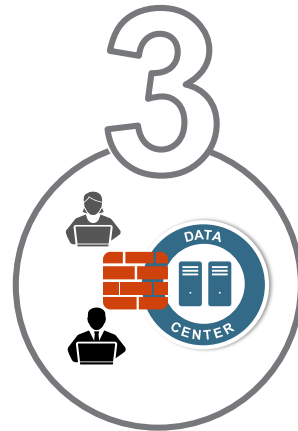
**SECURITY NEEDS TO BE CONSISTENT
AND AUTOMATED**



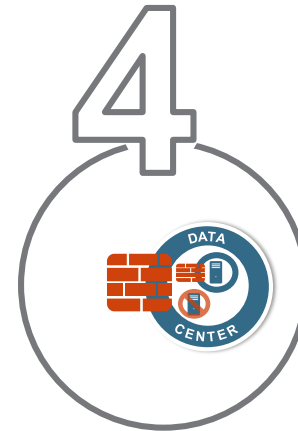
**ALL
ENDPOINTS
AND IOT**



**INTERNET
EDGE**



**BETWEEN
EMPLOYEES
AND DEVICES**

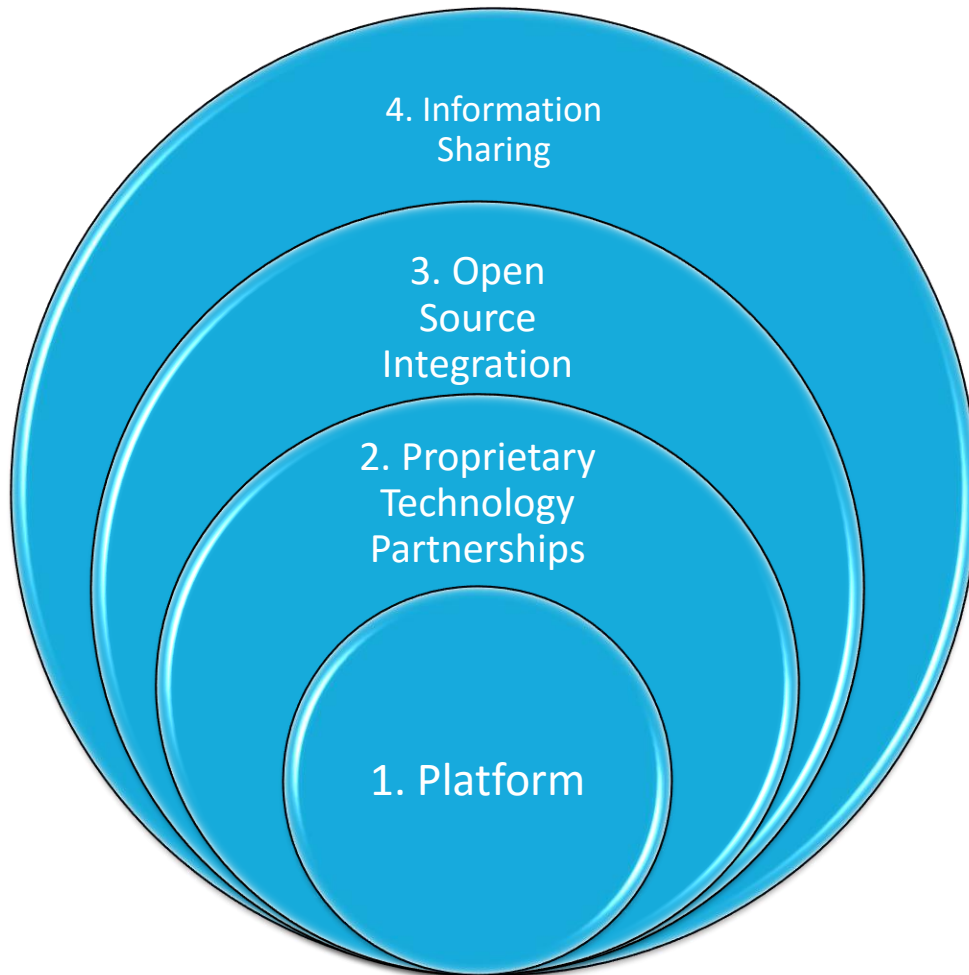


**AT THE DATA
CENTER EDGE
AND BETWEEN
VM'S**



**WITHIN ALL
CLOUDS AND
SAAS**

Integration is leverage



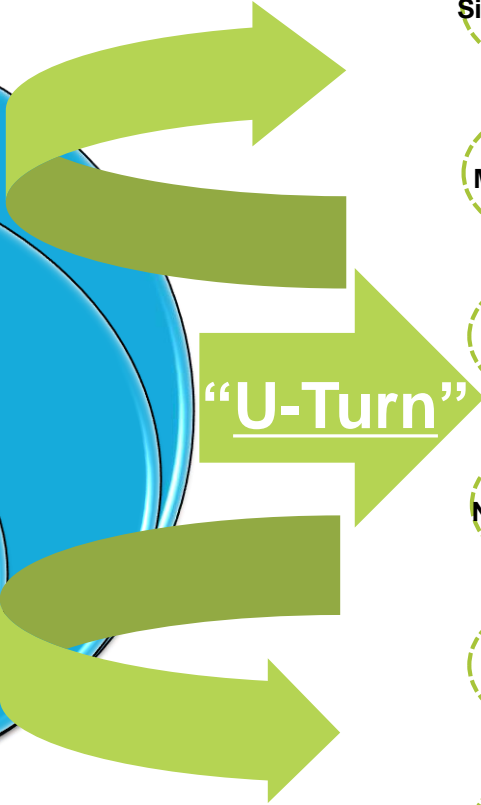
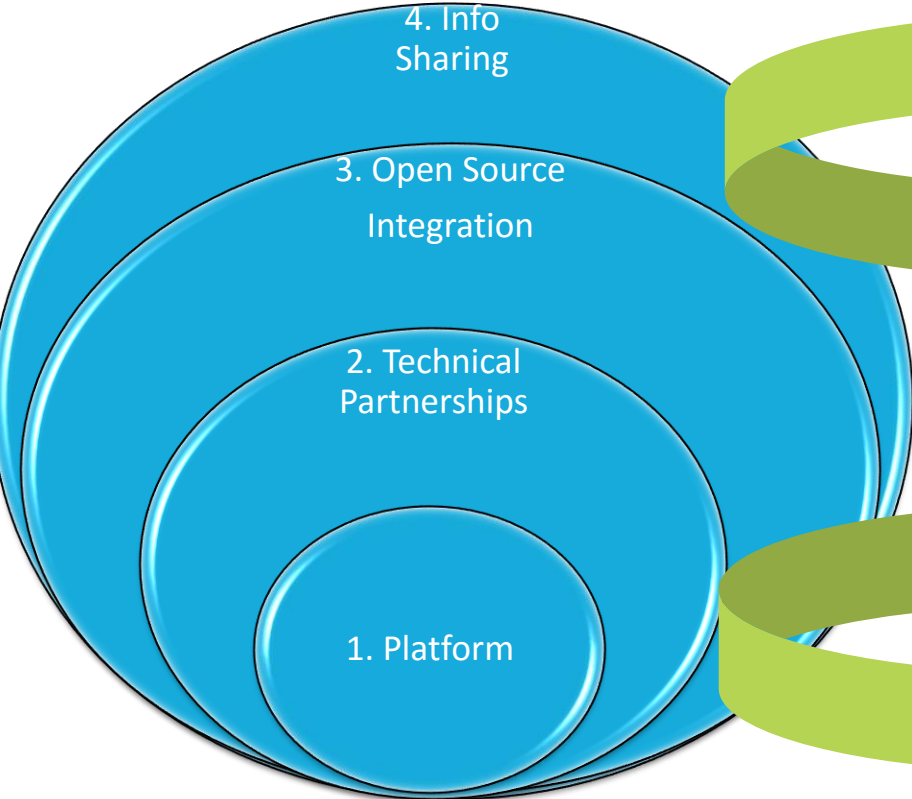
4. Information Sharing: Sharing threat information through formal and informal relationships and *integration* with public and private sector network defenders.

3. Open Source Integration: Leveraging the practice of API enables *integration* of various technologies and defensive capabilities deployed by an enterprise through plug and play.

2. Partnerships: Customized deep technical *integration* of complementary technology with market leading companies.

1. Platform: Prevention at the Network, Cloud and Endpoint levels through natively *integrated* capabilities that are designed from the beginning to work together, are automated, and are context driven to provide visibility and deliver prevention controls across the threat lifecycle in all network environments.

6 Major Trends



- Simpler and Easier
- More Convenient
- Fewer People
- Natively Integrated
- More Automated
- Designed to Prevent



Innovation Must Harness 4 Levels of Integration



THANK YOU