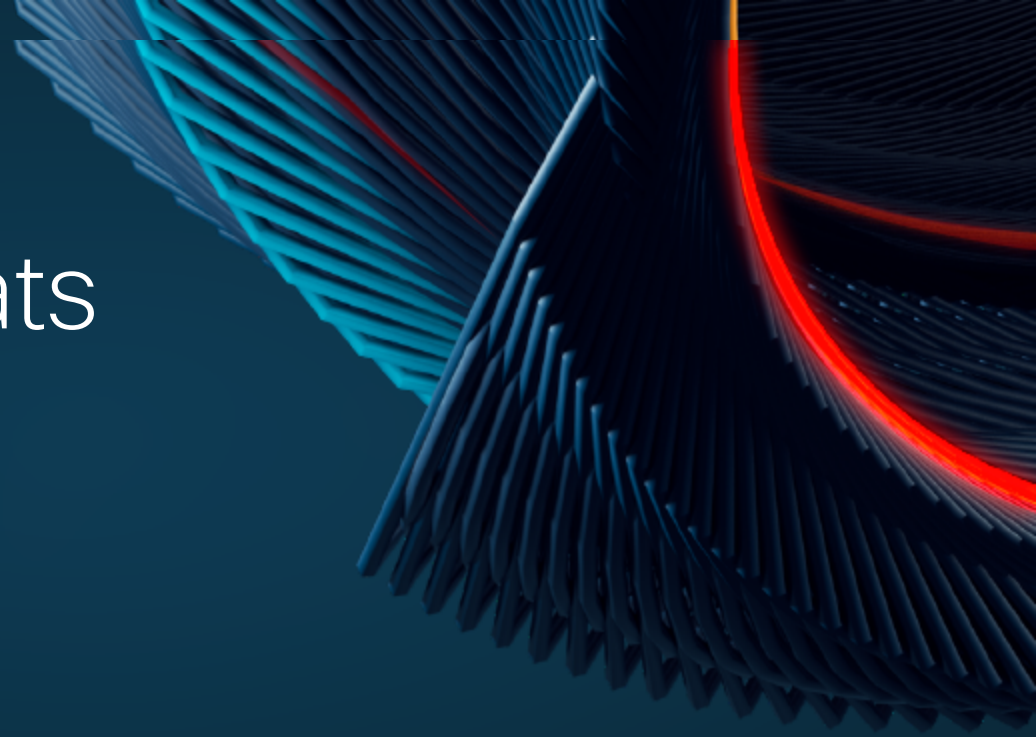
Advanced Threats Detection

Machine Learning Approach



Petr Cernohorsky
Security Business Group
November 2017

It's not If, it's When

DynDNS attack *"A massive cyberattack knocked out major websites across the internet"*

-Business Insider

"CryptoLocker bursts onto scene again, targeting Europe and U.S."

– SC Magazine

"Worse than WannaCry... Nyetya is deemed worse than WannaCry mainly because it spreads laterally, meaning it targets computers within networks and affects even systems that have been patched."

- TechAdvisory.org

New Cyber Threat Reality

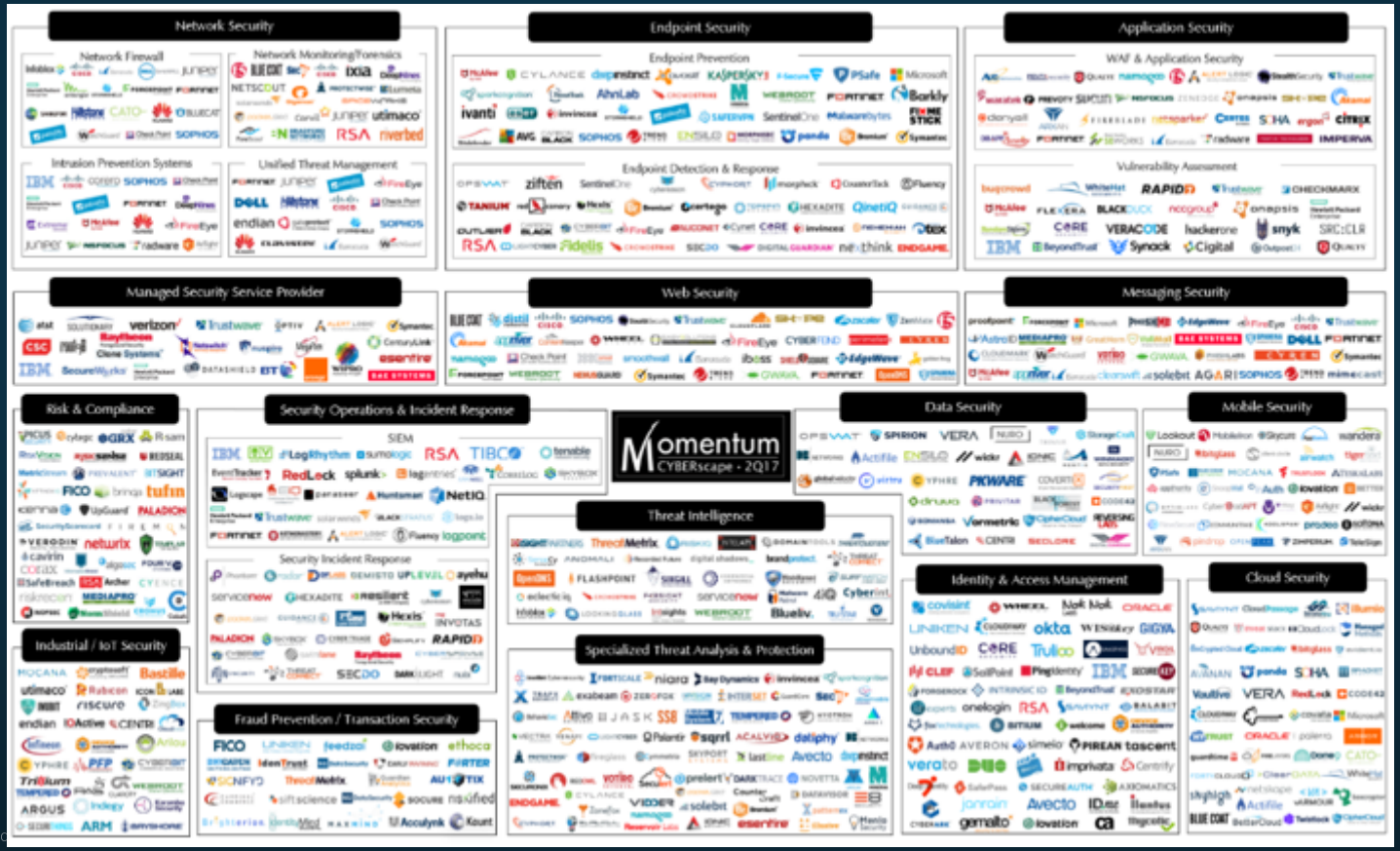
Your environment will get breached

You'll most likely be infected via email

Hackers will likely command and control your environment via web

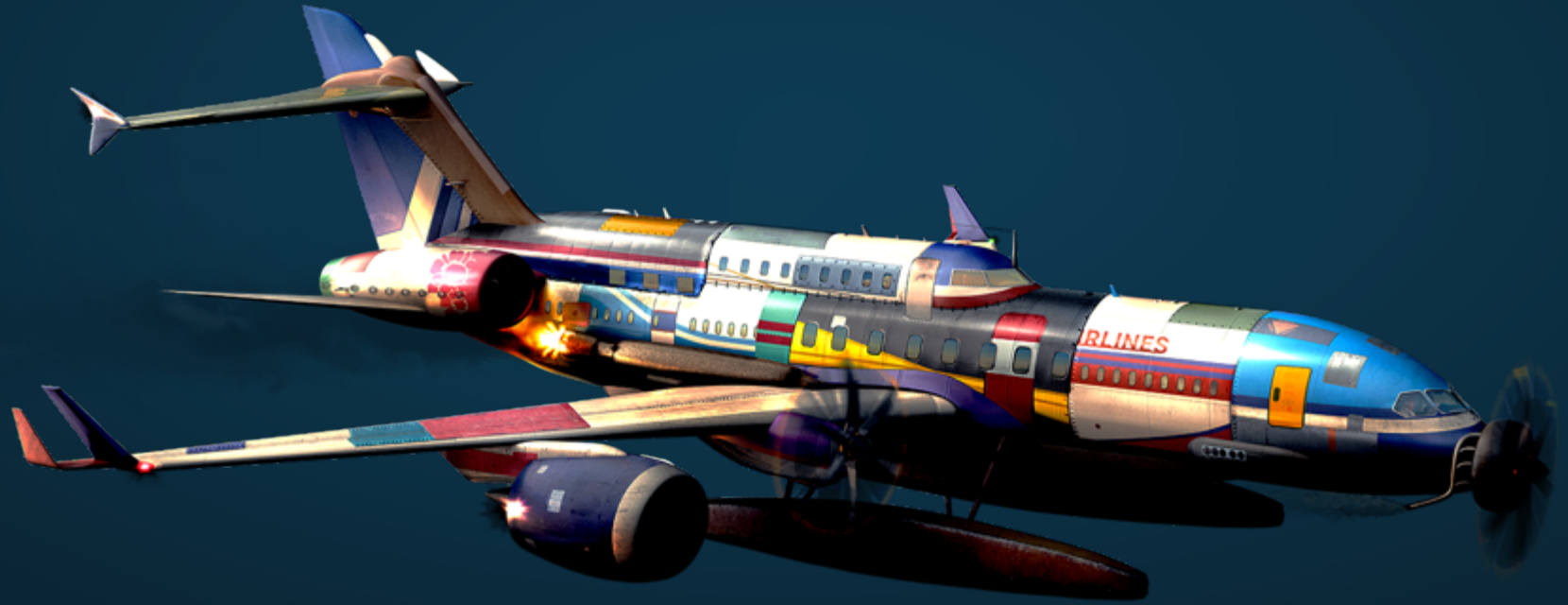
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

A vendor buffet is not a strategy



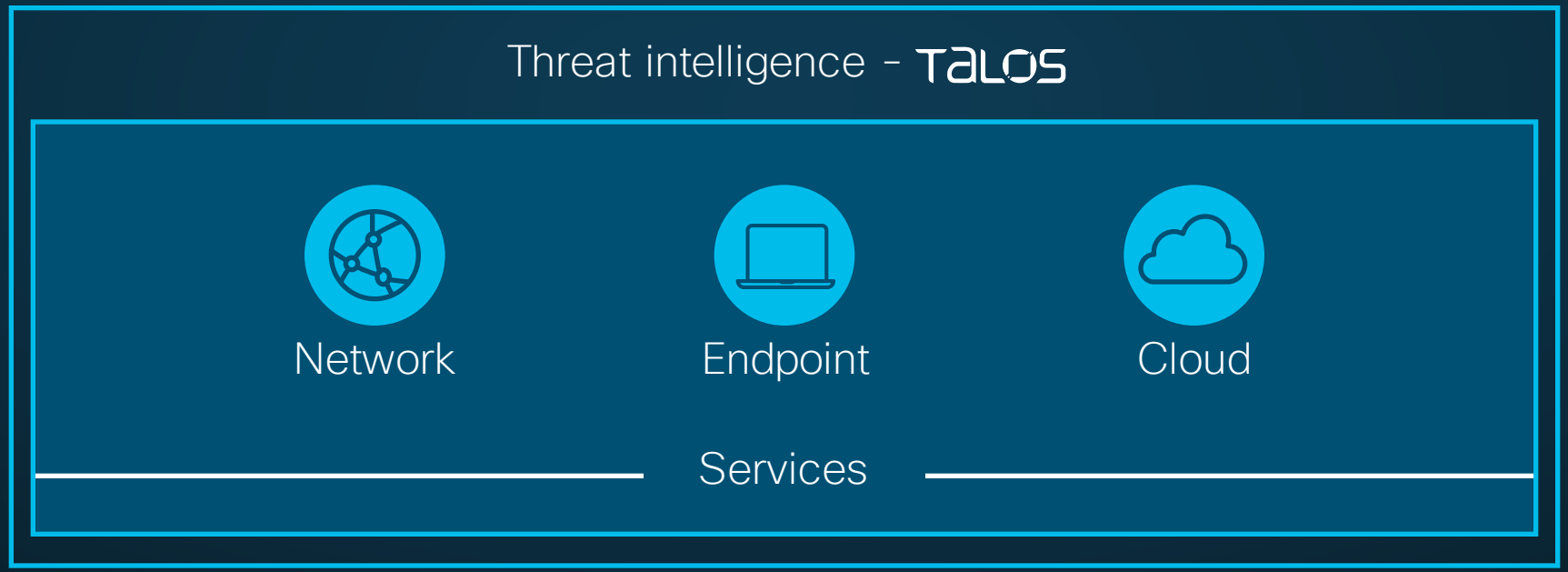
© 2017 Cisco and

No algorithm needed to figure out how ineffective this is!



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Security Architecture



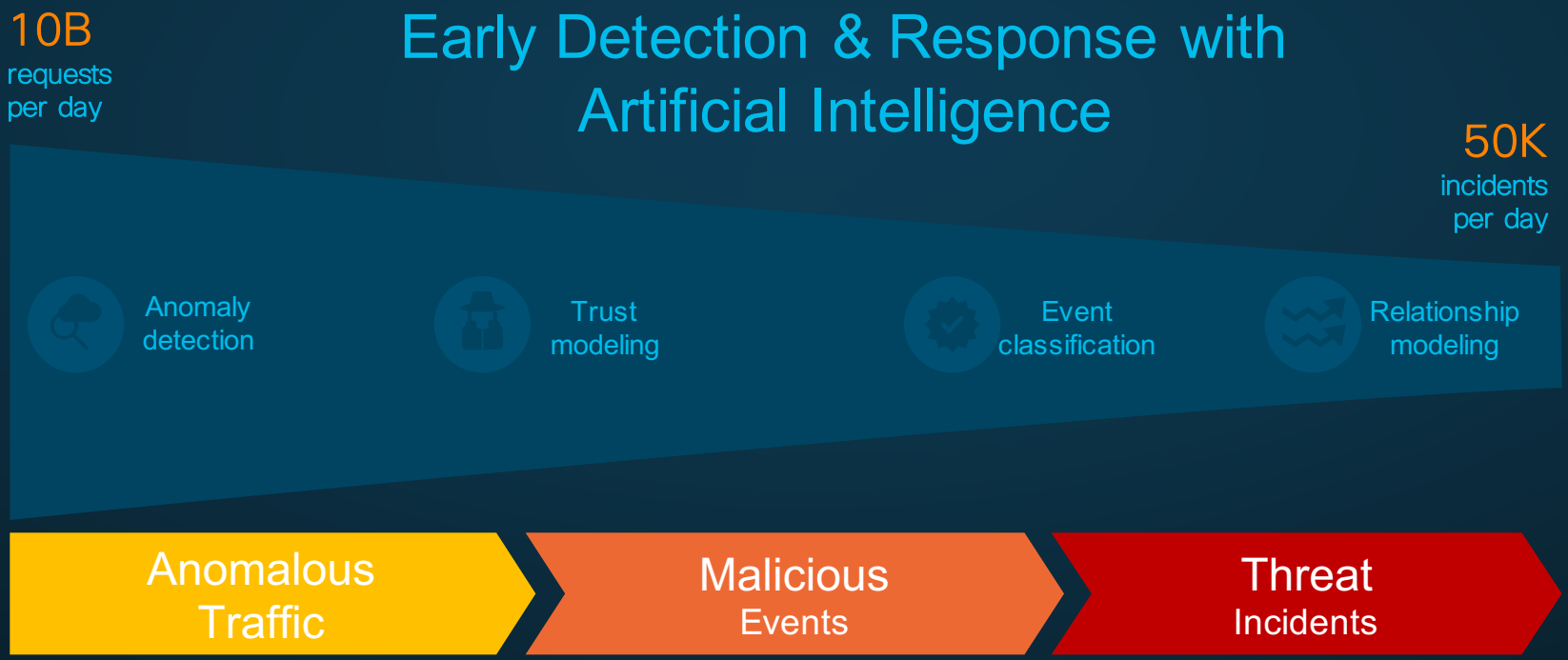
© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1% of Customer Devices Are Infected

Sample report demonstrating an advanced threat visibility gap: http://cognitive.cisco.com/preview

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cognitive Threat Analytics (CTA)



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Attacks Use Encrypted Traffic

80%

of organizations are victims of malicious activity

41%

of attacks used encrypted traffic to evade detection

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

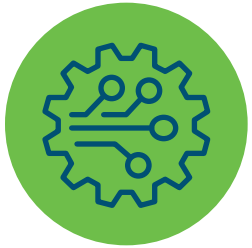
Malware Detection

Cisco Research

Known
Malware Traffic

Known
Benign Traffic

Extract Observable
Features in the Data



Employ Machine
Learning techniques
to build detectors

Known Malware
sessions detected
in encrypted traffic

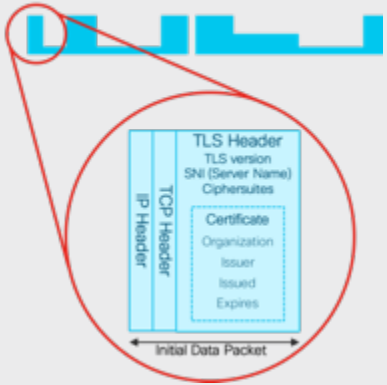
"Identifying Encrypted Malware Traffic with Contextual Flow Data"

AISec '16 | Blake Anderson, David McGrew (Cisco Fellow)

How can we inspect encrypted traffic?

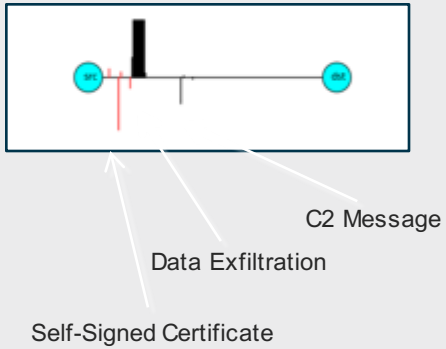
Initial Data Packet

Make the most of the unencrypted fields



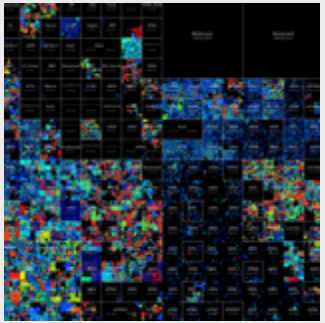
Sequence of Packet Lengths and Times

Identify the content type through the size and timing of packets



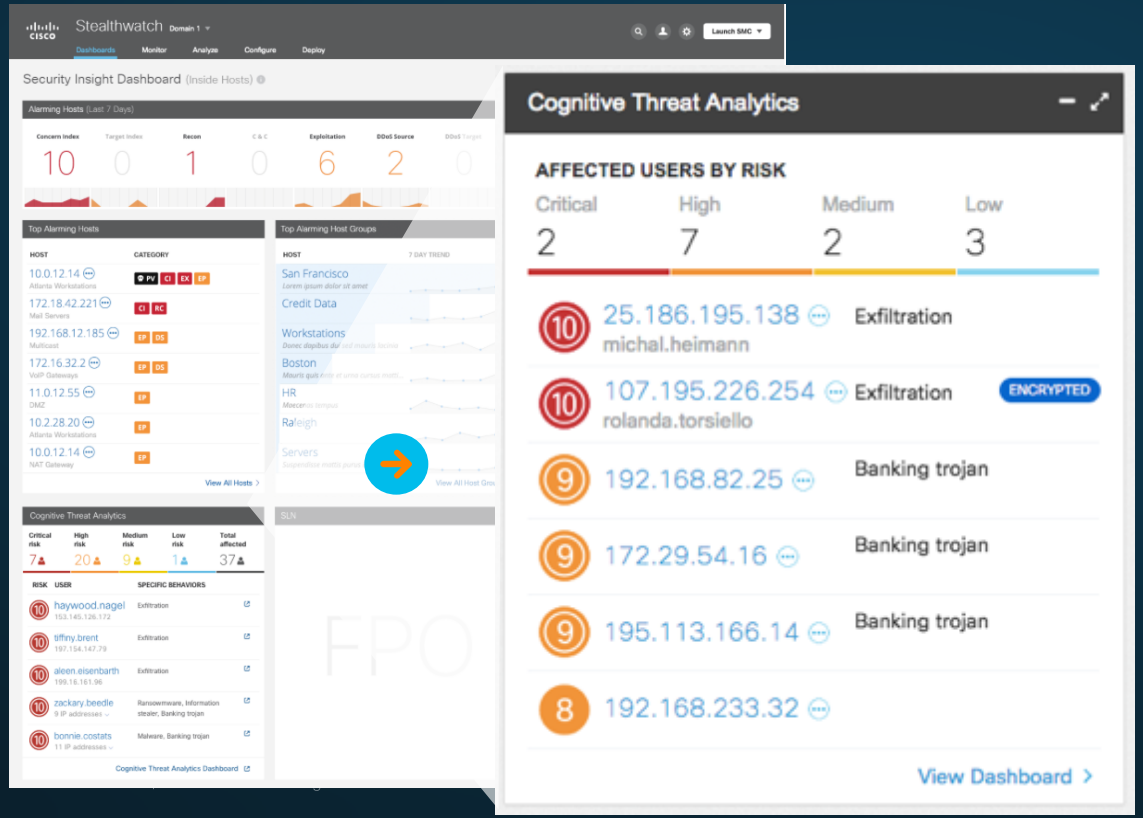
Global Risk Map

Who's who of the Internet's dark side



Broad behavioral information about the servers on the Internet.

Encrypted Traffic Analytics



Detect malware without decryption

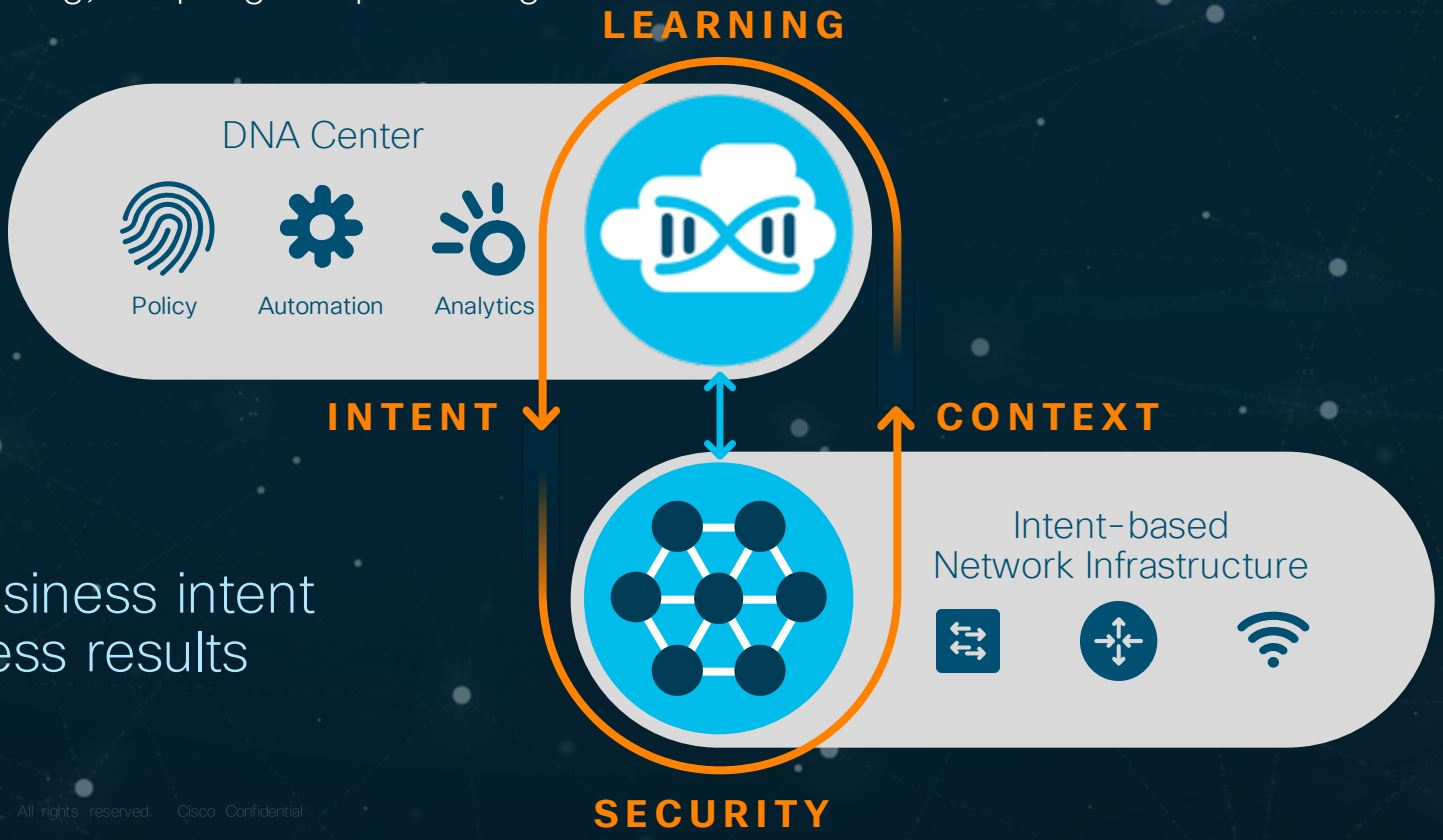
... through

MACHINE LEARNING &

correlation of global threat behaviors

The Network. Intuitive.

Constantly learning, adapting and protecting.



Turns business intent
to business results

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO