



# I forkant av svindleren *-med teknologien på din side*

Christian Nordve  
Systems Engineer

[chnordve@cisco.com](mailto:chnordve@cisco.com)

# The Security Problem



Changing  
Business Models

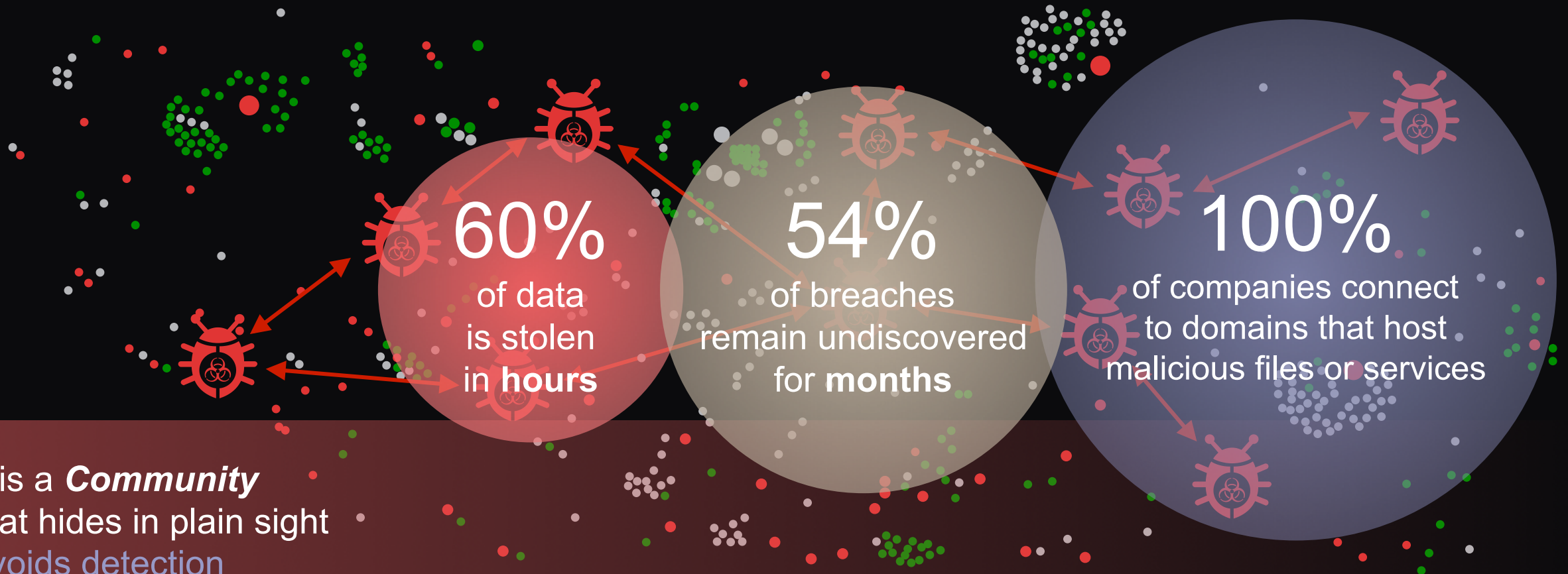


Dynamic  
Threat Landscape



Complexity  
and Fragmentation

# Breach Statistics



It is a **Community** that hides in plain sight avoids detection and attacks swiftly

*“There are two types of companies:  
Those who **have been hacked**, and  
those who **don’t yet know** they have  
been hacked.”*

John Chambers  
Chief Executive Officers of Cisco



# Hvorfor?

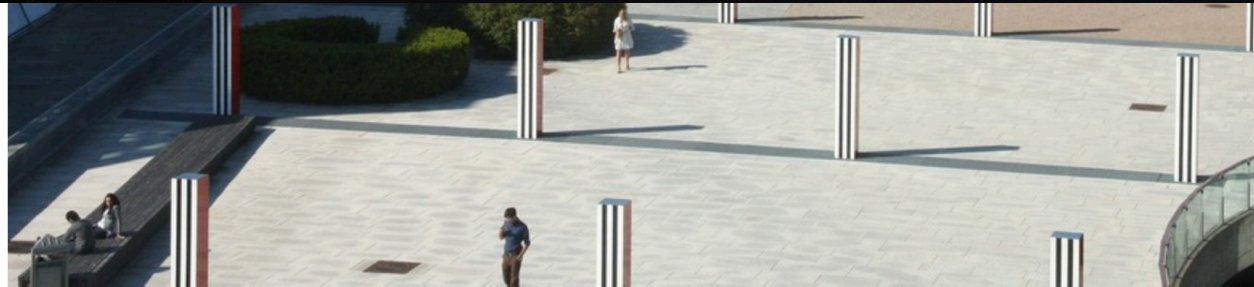




# Ville du gjort noe annerledes i dag om du viste at du kom til å bli angrepet i morgen?

Vi

Konta  
inform  
inn i d



Tekniske løsninger som antivirus og brannmur er ikke nok for å stoppe datainnbrudd, ifølge NorSIS. (Foto: Espen Zachariassen)

DATAINNBRUDET HOS TELENOR

## - Bedre opplæring kunne trolig avverget angrepet mot Telenor-ledelsen

Dataskurkene stoppes ikke av antivirus alene.



AV: ROALD RAMSDAL | ODD RICHARD VALMOTODD RICHARD VALMOT | IT | PUBLISERT: 18. MARS 2013 - 1

Facebook

0

Twitter

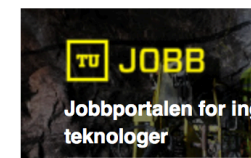
Denne helgen ble det kjent at sjefene i Telenor har blitt frastjålet store mengder sensitive data. For første gang politianmeldte selskapet industrispionasje,

27 Million

million citizens, up to 70

in 2013

t year,



2014, kl. 12:25



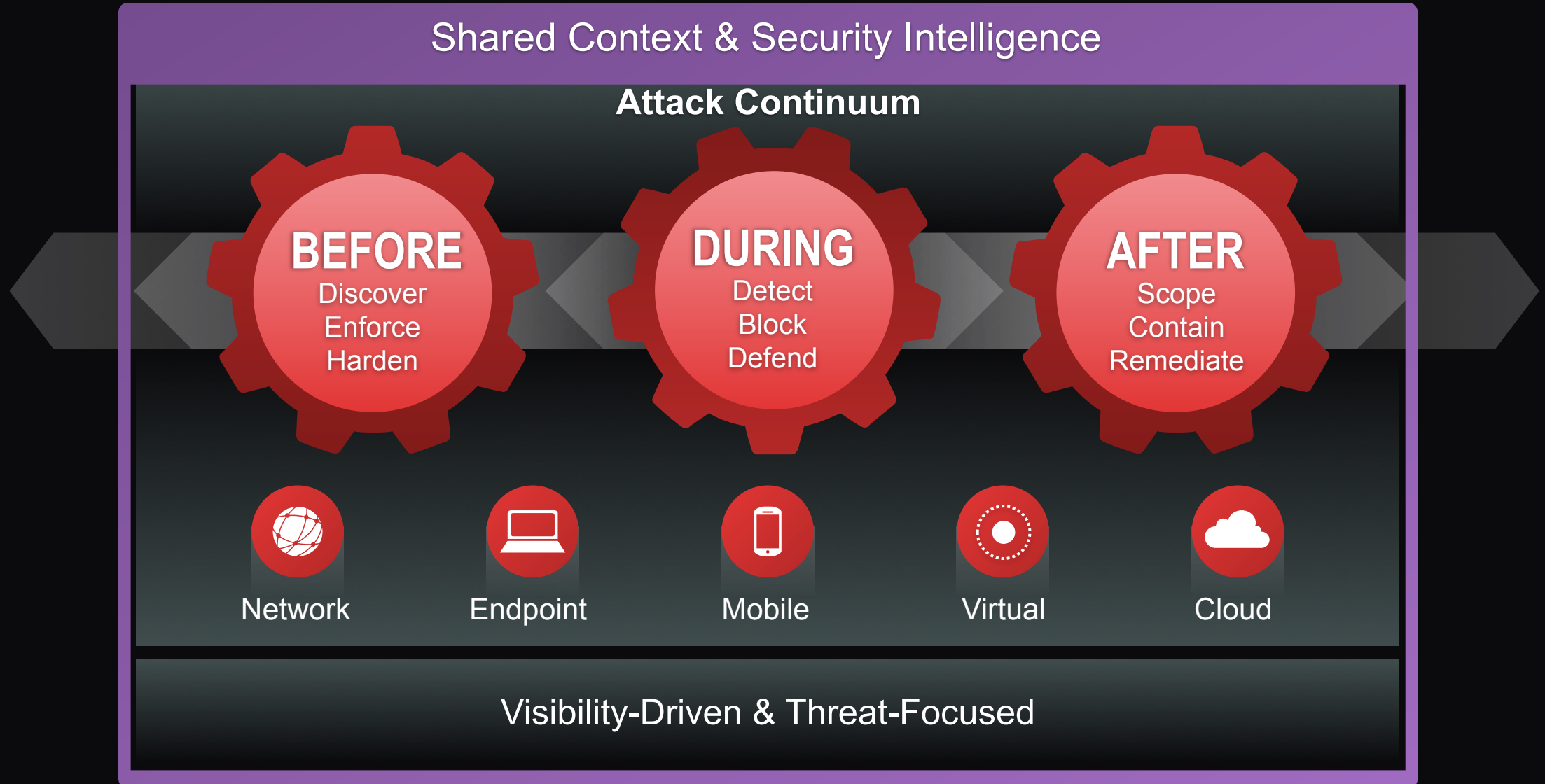
# Når bygde Noha arken?

Før det begynte å regne!



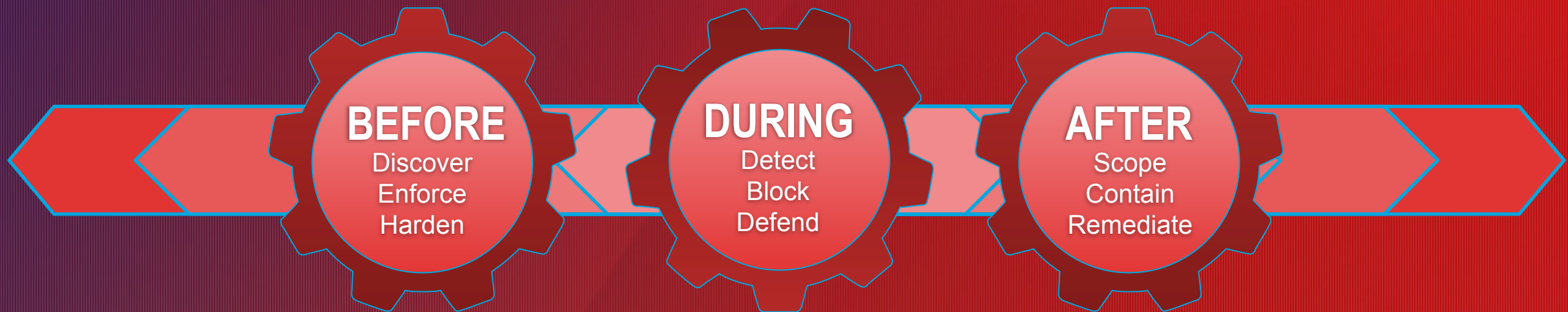
En endring i vår forståelse og innstilling er i ferd med å endres

# A Threat-Centric Security Model is Needed





# Building a Threat-Centric Cisco Security Architecture



**Attack Continuum**



Most Visited - Dagbladet.no - forsiden

13:22  
Her var det egentlig ikke plass til et hus Sjekk hva arkitektene fikk klemt inn på den lille tomta. 13:21

sabotasjen til politiet. (498 innlegg)  
Senterpartiet åpner for pappvinforbud Regjeringen er kritisk til pappvin i sin nye rusmeldingen, og stortingsrepresentant Kjersti Toppe fra Senterpartiet vil ha debatt om å forby pappvinen. (473 innlegg)

du ikke redd for flått? Her er i alle fall ett sjekketriks som ikke fungerer på sørlandsjenter.  
Her står barne TV-helten og spyr ut jødehets midt på lyse dagen Mannen bak masken har en fortid du ikke vil tro på.

11 Elizabeth Olsen  
SISTE: - Jeg bor ikke med dem, og de kler meg ikke opp

13 Lea Michele  
SISTE: «Glee»-stjerna stilte med nattas høyeste splitt

Dagbladet.no siste 48 timer

annonse



SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco security threat information, access to the web site http://ib.adnxs.com/getuid?http://dp2.specificclick.net/sync/?pid=4&pu=\$UID has been blocked by the Web Security Appliance (WSA) to prevent an attack on your browser. The Cisco Security Intelligence Operations (CSIO) Web Reputation Score for this site indicates that it is associated with malware/spyware, and poses a security threat to your computer or the corporate network.

In order to cater for a growing number and variety of devices on the Cisco network, malware protection has shifted from the endpoint, deeper into the network. In order to offer the most effective protection to computing assets on the Cisco network, CSIRT and Cisco IT jointly rolled out the Cisco Ironport WSA solution on all Cisco Internet Points of Presence (IPoPs). These WSAs are configured to block access to sites whose Web Based Reputation Score (WBRS) shows that they are serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this page was misclassified, please open a case with Infosec, providing the corresponding debug information below:

Table with 2 columns: Field (Date, Time, Client IP address, Request URL, User-Agent) and Value (Thu, 28 Jun 2012 12:04:28 GMT, 1340885068.712, 173.38.133.8, http://ib.adnxs.com/getuid?http://dp2.specificclick.net/sync/?pid=4&pu=\$UID, Mozilla/5.0 (Macintosh; U: Intel Mac OS X 10.6; en-US; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6)

Se.no Se hele tv-guiden! 20:00 Allsang på grensen (2) Allsang på grensen er tilbake med nye folkekjære artister fra Fredriksten festning i Halden. Øystein Dolmen er gjestprogramleder, og ellers tar Plumbo, Elvira Nikolaisen, Franklin, Tone Damli og Eric Saade turen til Halden denne sommerkvelden. (20:00 på TV 2) Se dagens høydepunkter Filmguide Serieguiden

Se og forstå det sammensatte bilde!



# Evne til å se ting i perspektiv og retrooperspektiv

- Hvis noe kommer seg inn på nettet hos oss eller på en av våre maskiner forde vi ikke vet om det er farlig
- ...Fordi det er *helt nytt* og ingen har sette det før....
- Men, i morgen så vet vi mer og kan nå slå fast at det er et “virus” ...
- Ville ikke du da helst vite om det?
  - Hvem lastet det?
  - Hvor er det nå? –Hvor har det spredd seg



# Nettverket ser alt



Vi må integrere mer effektivt for å  
skape en virkningsfull  
sikkerhetsløsning.

# Det krever arkitektur



# Utfordringer

- Ikke noe av dette virker hvis alt må være på plass for at noe skal virke
- Hver enkel løsning/produkt må kunne “stå på egne ben” og være blandt de beste, hver for seg

Når Cisco løsningen settes sammen vil de skape mulighet for å bruke hverandres innsikt og innsyn til å berike hverandre

*“Our fundamental job is to reduce complexity and increase capability”*



# Superior Intelligence to battle Advanced Threats

Cisco®  
SIO

1.8 million  
global sensors

35%  
worldwide email traffic

100 TB  
of data received per day

13 billion  
web requests

180 million+  
deployed endpoints

24x7x365  
operations

600+  
engineers, technicians,  
and researchers

40+  
languages

Talos  
Cisco Collective  
Security Intelligence



Pervasive across Portfolio

Sourcefire  
VRT®

200,000+ File Samples per Day  
FireAMP™ Community, 3+ million

Advanced Microsoft  
and Industry Disclosures

Snort and ClamAV Open Source  
Communities

Honeypots

Sourcefire AEGIS™ Program

Private and Public Threat Feeds

Dynamic Analysis

# Oppsummert

## Collective Security Intelligence

Covers the entire Attack Continuum

**BEFORE**

Discover  
Enforce  
Harden

**DURING**

Detect  
Block  
Defend

**AFTER**

Scope  
Contain  
Remediate

### STRATEGIC IMPERATIVES

#### Visibility-Driven



Network-Integrated,  
Broad Sensor Base,  
Context sharing and  
Automation

#### Threat-Focused



Continuous Advanced  
Threat Protection,  
Cloud-Based Security  
Intelligence

#### Platform-Based



Leading products working  
together as a system  
Built for Scale, Consistent  
Control, Management

Takk for meg!