

Enterprise Security: Markets, Strategy, Roadmap, Go-to-Market

Jeff Scheel, SVP, Corporate Development, Alliances, and Strategy
Balaji Yelamanchili, EVP & GM, Enterprise Security Business Unit
Amit Mital, EVP, CTO & Emerging Endpoints

Forward Looking Statements

This presentation contains statements regarding our projected financial and business results, which may be considered forward-looking within the meaning of the U.S. federal securities laws, including statements regarding our financial guidance and targets (as a combined company and by business segment); our proposed separation into two publicly traded companies; the projected market growth rates and margin expansion opportunities for the security business and the information management business; statements regarding our competitive advantages in security and information management; statements with respect to the proposed timing of the separation; and statements with respect to proposed capital allocation strategies for both Symantec and Veritas. These statements are subject to known and unknown risks, uncertainties and other factors that may cause our actual results, levels of activity, performance or achievements to differ materially from results expressed or implied in this presentation. Such risk factors include those related to: risks related to the separation of the company into the security business and the information management business; general economic conditions; maintaining customer and partner relationships; the anticipated growth of certain market segments, particularly with regard to security and information management; the competitive environment in the industries in which we operate; changes to operating systems and product strategy by vendors of operating systems; fluctuations in currency exchange rates; the timing and market acceptance of new product releases and upgrades; the successful development of new products; and the degree to which these products and businesses gain market acceptance. Actual results may differ materially from those contained in the forward-looking statements in this presentation. We assume no obligation, and do not intend, to update these forward-looking statements as a result of future events or developments. Additional information concerning these and other risks factors is contained in the Risk Factors sections of our Form 10-K for the year ended March 28, 2014 and our Form 10-Q for the quarter ended January 2, 2015.

Any information regarding pre-release of Symantec offerings, future updates or other planned modifications is subject to ongoing evaluation by Symantec and therefore subject to change. This information is provided without warranty of any kind, express or implied. Customers who purchase Symantec offerings should make their purchase decision based upon features that are currently available.

We assume no obligation to update any forward-looking information contained in this presentation.



Use of GAAP and Non-GAAP Financial Information

Our results of operations have undergone significant change due to a series of acquisitions, the impact of stock-based compensation, impairment charges and other corporate events. To help our readers understand our past financial performance and our future results, we supplement the financial results that we provide in accordance with generally accepted accounting principles, or GAAP, with non-GAAP financial measures. The method we use to produce non-GAAP results is not computed according to GAAP and may differ from the methods used by other companies. Our non-GAAP results are not meant to be considered in isolation or as a substitute for comparable GAAP measures and should be read only in conjunction with our consolidated financial statements prepared in accordance with GAAP.

Our management regularly uses our supplemental non-GAAP financial measures internally to understand, manage and evaluate our business and make operating decisions. These non-GAAP measures are among the primary factors management uses in planning for and forecasting future periods. Investors are encouraged to review the reconciliation of our non-GAAP financial measures to the comparable GAAP results, which can be found, along with other financial information, on the investor relations' page of our website at www.symantec.com/invest.

Reconciliations for our financial results and guidance can be found on Symantec's investor relations website.

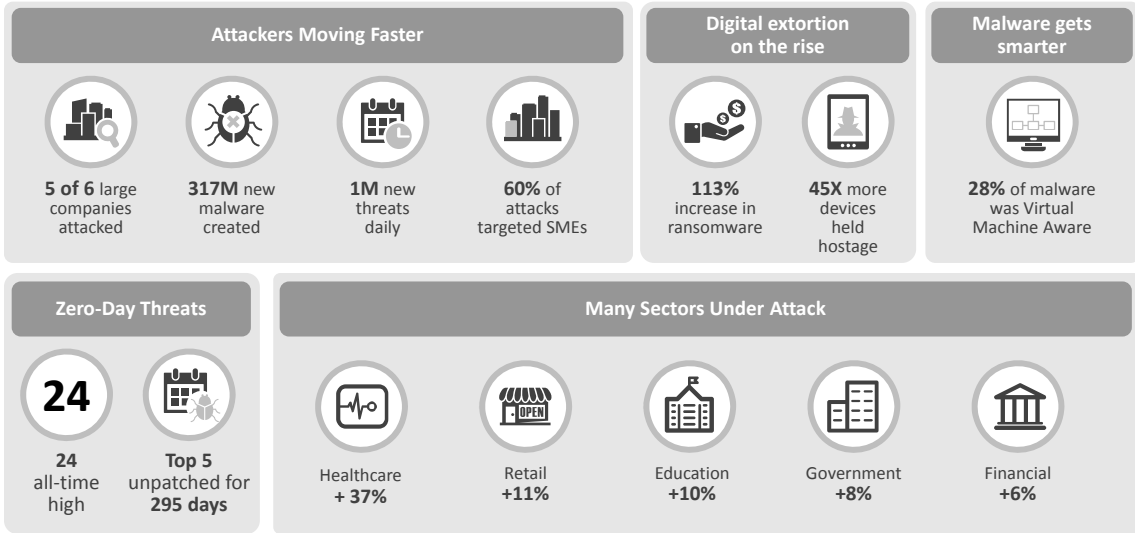
3

Agenda

1	Market Opportunity
2	Product Strategy
3	Roadmap & Go-To-Market

4

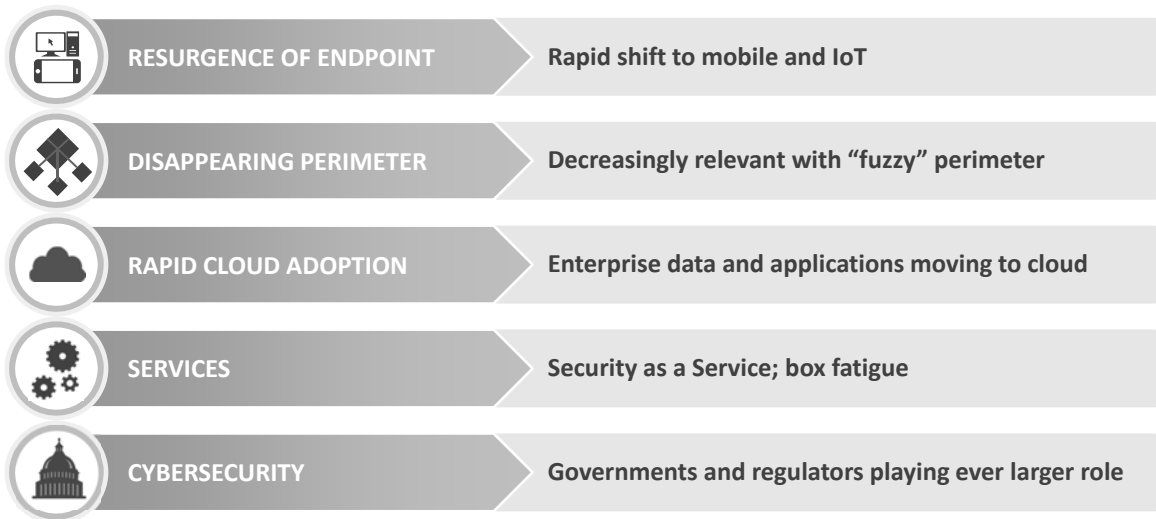
Enterprise Threat Landscape



Source: Symantec Internet Security Threat Report 2015

5

Key Trends Reshaping the Enterprise Security Market



6

Symantec Enterprise Security | STRONG FRANCHISES

 <p>Endpoint Security #1 share; AAA rating nine quarters in a row</p>	 <p>Data Protection #1 DLP share; 100% of Fortune 100</p>	 <p>Email Security #1 share; 100% uptime with <0.0003% FPs 5 years in a row</p>
 <p>Trust Services #1 share 6B certificate lookups/day</p>	 <p>Authentication & Authorization 13B validations every day 100% uptime last 5 years</p>	 <p>Managed Security Services 12 Yrs Gartner MQ leader 30B logs analyzed/day</p>

7

Symantec Enterprise Security | UNIQUE VISIBILITY

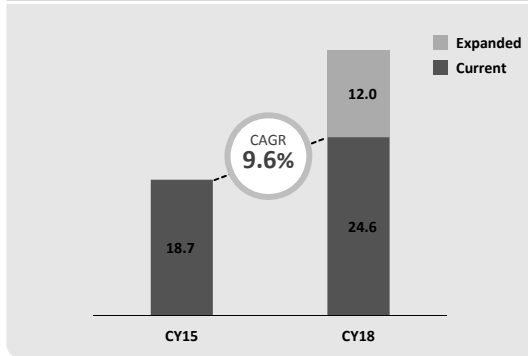
 <p>175M endpoints</p>	 <p>57M attack sensors in 157 countries</p>	 <p>182M web attacks blocked last year</p>
 <p>3.7T rows of telemetry 100 Billion more/month</p>	 <p>30% of world's enterprise email traffic scanned/day 1.8 Billion web requests</p>	 <p>9 threat response centers 500+ rapid security response team</p>

8

Symantec Enterprise Security | GROWTH DRIVERS



Addressable Market Size (\$B)



Source: IDC Security forecast, Gartner, Harbor Research, Ovum, and Symantec Analyses



Symantec Opportunity

Threat Protection

- With Advanced Threat Protection (ATP) and Cloud Workload Protection, our addressable market expands **50%** by CY 2018

Information Protection

- With Cloud Information Protection and Identity as a Service, our addressable market expands **35%** by CY 2018

Cyber Security Services

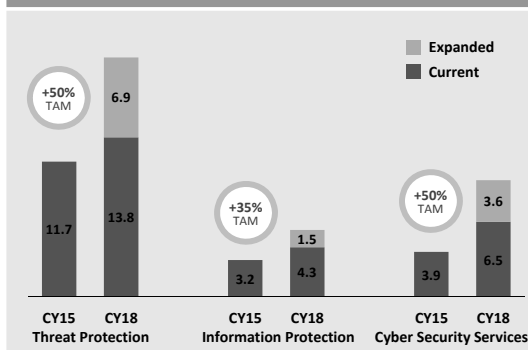
- With expanded Cyber Security Services offerings, our addressable market expands **50%+** by CY 2018

9

Symantec Enterprise Security | GROWTH DRIVERS



Addressable Market Size (\$B)



Source: IDC Security forecast, Gartner, Harbor Research, Ovum, and Symantec Analyses



Symantec Opportunity

Threat Protection

- With Advanced Threat Protection (ATP) and Cloud Workload Protection, our addressable market expands **50%** by CY 2018

Information Protection

- With Cloud Information Protection and Identity as a Service, our addressable market expands **35%** by CY 2018

Cyber Security Services

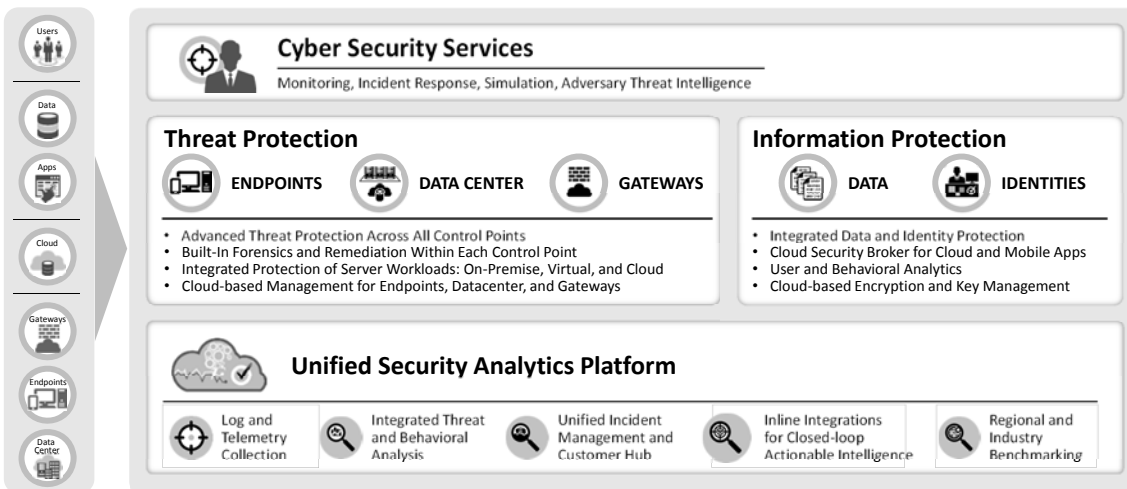
- With expanded Cyber Security Services offerings, our addressable market expands **50%+** by CY 2018

10

Agenda

1	Market Opportunity
2	Product Strategy
3	Roadmap & Go-To-Market

Enterprise Security | PRODUCT STRATEGY





Symantec. 2015
 Financial Analyst Day

THREAT PROTECTION


Cyber Security Services

Threat Protection

ENDPOINTS DATA CENTER GATEWAYS





Information Protection

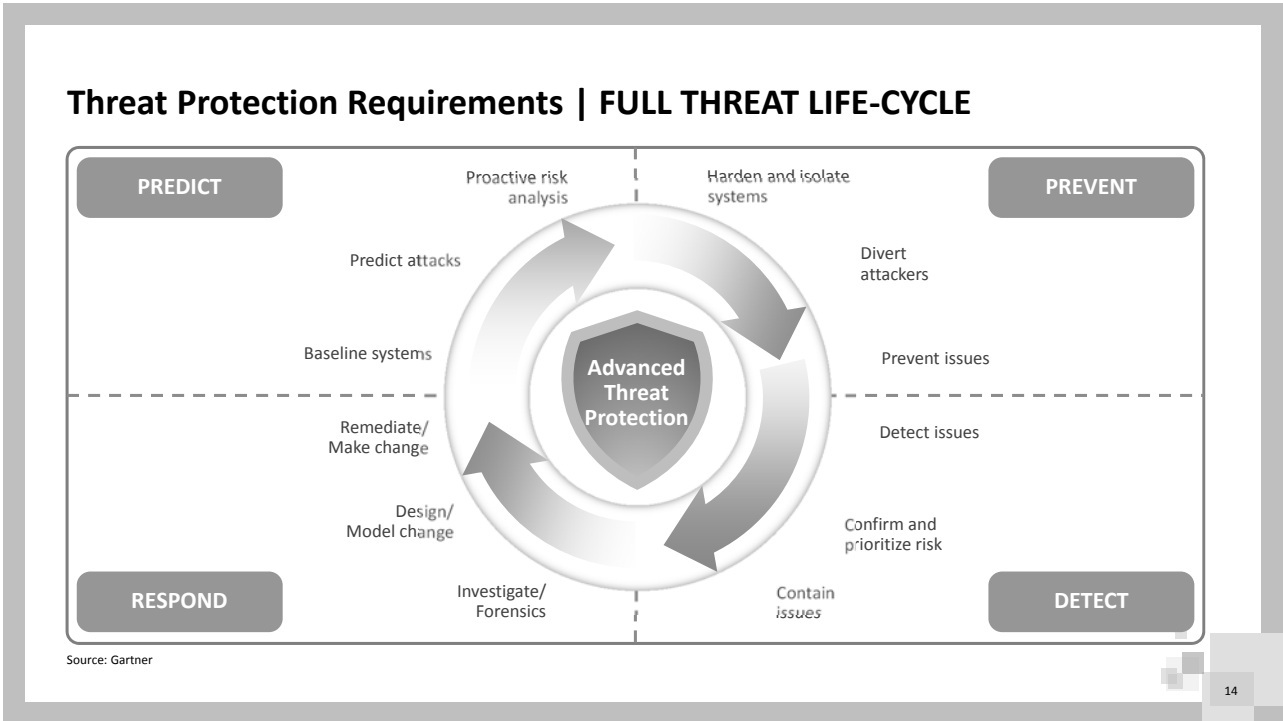
DATA IDENTITIES





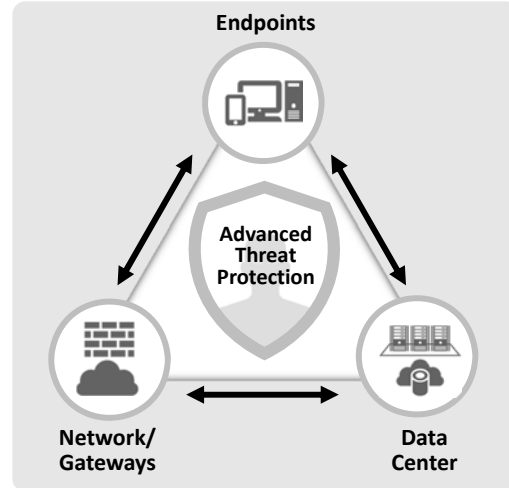
Unified Security Analytics Platform

13



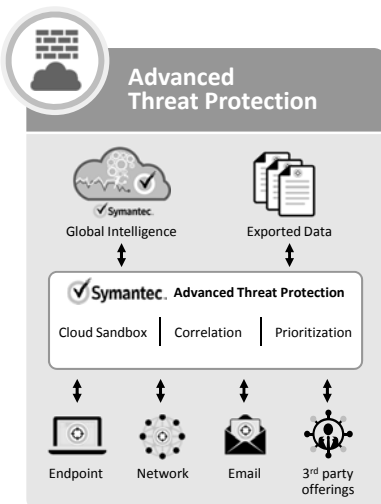
Symantec Threat Protection | STRATEGY

- Advanced Threat Protection Across Control Points
- Built-in Forensics and Remediation Within Each Control Point
- Integrated Protection of Server Workloads across On-Premise, Virtual, and Cloud
- Cloud-based Management for Endpoints, Datacenter, and Gateways



15

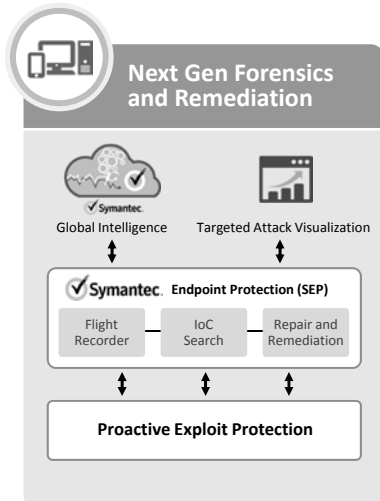
Symantec Threat Protection | ADVANCED THREAT PROTECTION



- Single detection platform across endpoint, network, and email
- Cross correlation and incident prioritization
- Cloud-based payload detonation
- Closed-loop remediation
- Unified incident management
- Key differentiator: high efficacy with least false positives and low TCO

16

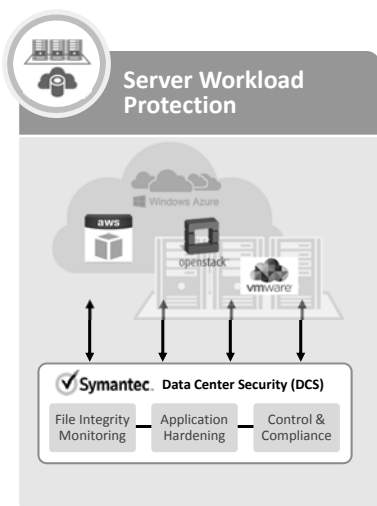
Symantec Threat Protection | FORENSICS & REMEDIATION



- Extensions built within existing agent technology
- Granular flight recorder
- Fine-grained remediation policies
- Common management console with centralized activity logs
- Known and unknown exploit detection
- Key differentiator: no new agent, easy to upgrade

17




Symantec Threat Protection | INTEGRATED SERVER WORKLOAD PROTECTION



- Integrated protection across on premise, virtualized, and cloud-based workloads
- Consistent enforcement of app control, lockdown, and other hardening policies
- Common management and orchestration as workloads move to and from cloud
- Support for VMWare (NSX/ESX) and Amazon, Azure, and OpenStack Clouds

18

Symantec Threat Protection | SUMMARY OF KEY CAPABILITIES

 Advanced Threat Protection	 Next Gen Forensics and Remediation	 Server Workload Protection
<ul style="list-style-type: none"> • Single platform • Cloud-based payload detonation • Cross-control point correlation and incident prioritization • Closed-loop remediation • Unified incident management 	<ul style="list-style-type: none"> • Granular flight recorder • Fine-grained remediation policies • Known and unknown exploit detection • Common management console with centralized activity logs • Closed-loop remediation • No new agent (easy upgrade) 	<ul style="list-style-type: none"> • Integrated protection across on premise, virtualized, and cloud-based workloads • Consistent application of lockdown, app control, and lockdown policies • Common Management/orchestration as workloads move to and from cloud • Support for VMWare (NSX/ESX) and Amazon, Azure, and OpenStack
Cloud-based management with single extendable agent technology, self-service BYOD provisioning, and native encryption & key management		

19

Symantec Threat Protection | KEY REVENUE OPPORTUNITIES

Installed Base

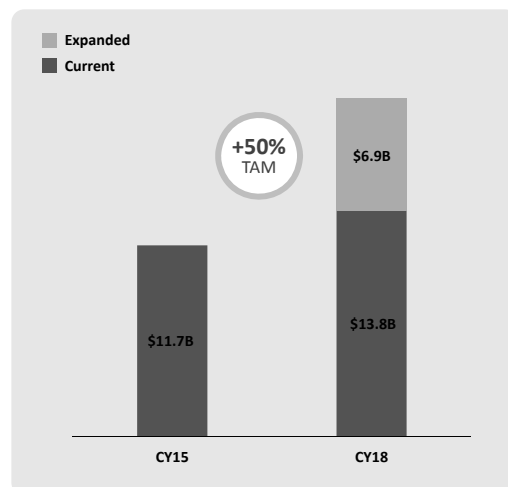
- Endpoint customers: Endpoint ATP and Forensics & Remediation add-ons
- Email customers: Email ATP add-on
- Both: Full ATP including Endpoint, Email, and Network

Net New Customers

- ATP with cross-correlation value proposition
- Replacement of manual IR projects with automated tools for Forensics and Remediation

Customers moving to Cloud and BYOD

- Protection for Cloud workloads (e.g. Amazon, Azure)
- Cloud-based management of endpoint, server, and BYOD devices with self-service capabilities




Source: IDC Security forecast, Harbor Research, Ovum, and Symantec Analyses

20






INFORMATION PROTECTION

INFORMATION PROTECTION


Cyber Security Services



Threat Protection


ENDPOINTS DATA CENTER GATEWAYS

Information Protection





DATA IDENTITIES


Unified Security Analytics Platform

21

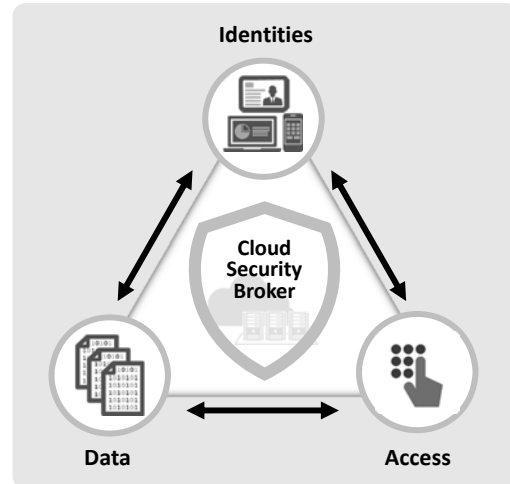
Information Protection Requirements | CLOUD AND MOBILE FOCUS

↑ USERS ARE MOVING	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>With the advent of mobile and BYOD devices, more users are accessing and consuming information when outside the firewalls</p> </div> </div>	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>With more data in cloud and more mobile users, information protection across cloud and mobile, combined with behavioral analytics, is a critical imperative</p> </div> </div>
↓ USERS ARE MOVING	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>Historically data was created and consumed on premise; most users would create and consume this data from inside firewalls</p> </div> </div>	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>With more applications and workloads migrating to public clouds, more and more data is created and consumed on cloud</p> </div> </div>
← DATA AND APPS ARE MOVING →		

22

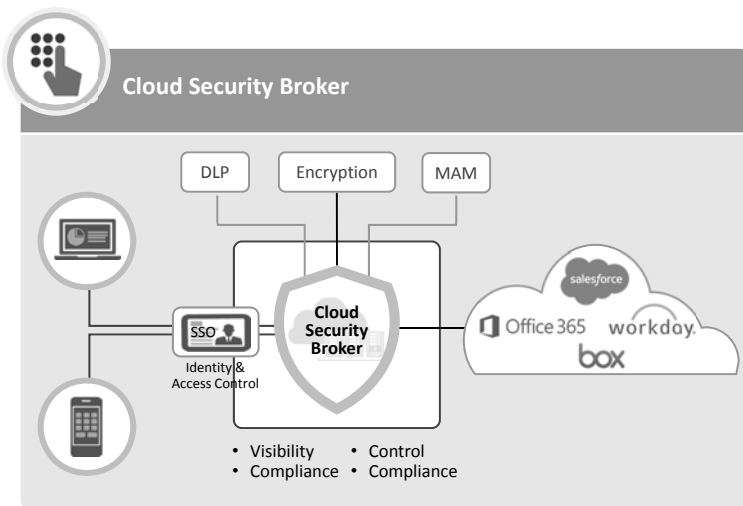
Symantec Information Protection | STRATEGY

- Extend Data and Identity protection regardless of where data resides: On Premise, On Mobile, In the Cloud
- Common SSO and Access Management regardless of where applications reside: On Premise, On Mobile, In the Cloud
- Integrated user and behavioral analytics to detect and prevent insider and outsider (APT) threats



23

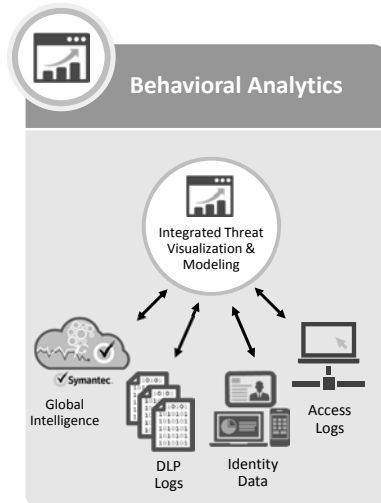
Symantec Information Protection | CLOUD SECURITY BROKER



- A new cloud-based control point that integrates DLP, Identity, and Analytics
- Ensures identity and data protection between mobile users and cloud apps, independent of perimeter
- Highly contextual protection by connecting user, device, location, and data loss prevention policies
- Cloud-based SSO with biometric authorization
- Scan and remediation of data already in cloud apps

24

Symantec Information Protection | USER AND BEHAVIORAL ANALYTICS



- Integrated analytics to track and profile behaviors and data flow
- Content, Context, and Identity aware
- Pre-built threat models and big-data analytics to quickly detect and prevent incidents
- Prioritized incident management based on risk profile, risk timeline, and risk comparison
- Industry and global intel correlation to detect coordinated attacks

25

Symantec Information Protection | SUMMARY OF KEY CAPABILITIES



Cloud Security Broker

- Data and identity protection between mobile and cloud, with no perimeter
- Highly contextual protection by connecting user, device, location, and data loss prevention policies
- Cloud-based SSO with biometric authorization
- Scan and remediation of data already in cloud apps



User and Behavioral Analytics

- Integrated analytics to track and profile behaviors and data flow
- Prioritized incident management
- Pre-built threat models and big-data analytics to quickly flag and detect incidents
- Industry and global intel correlation to detect coordinated attacks

26

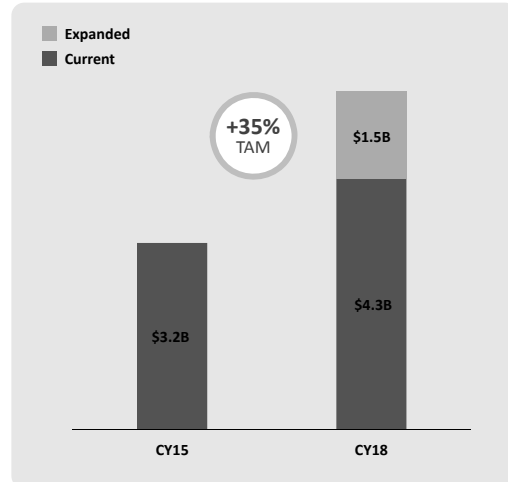
Symantec Information Protection | KEY REVENUE OPPORTUNITIES

Installed Base

- Cloud Security Broker combining identity, DLP, analytics (increasing ARPU)
- Individuals add-ons such as DLP for Cloud apps, Cloud SSO, and Behavioral Analytics

Net New Customers moving to Cloud

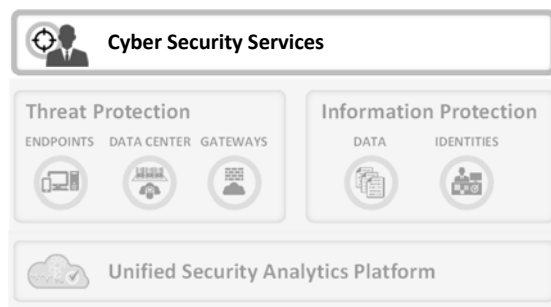
- Cloud Security Broker combining identity, DLP, analytics
- Individual solutions: DLP for Cloud apps, Cloud SSO, and Behavioral Analytics



Source: IDC Security forecast and Symantec Analyses

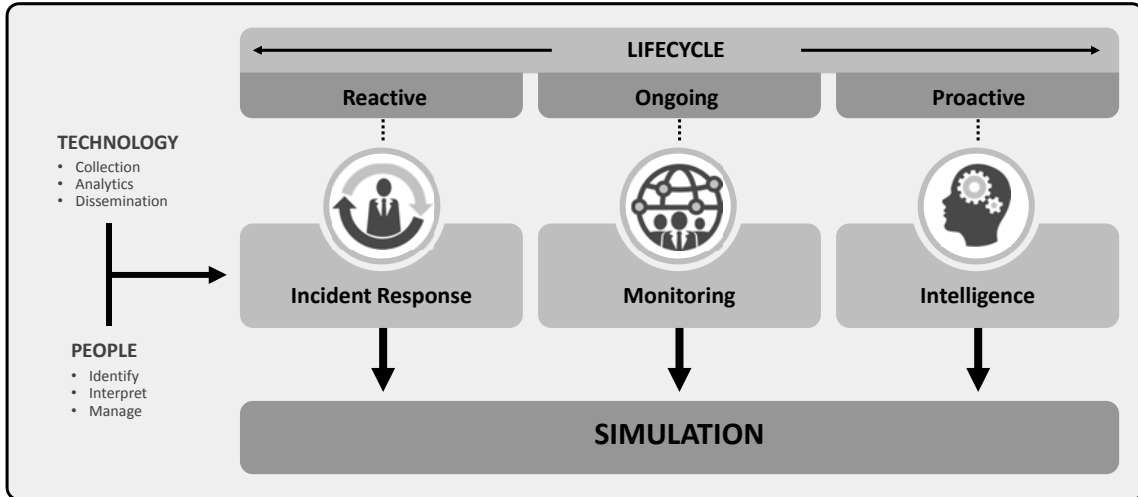
27

CYBER SECURITY PROTECTION



28

Cyber Security Services Market | PRIORITY ON FULL LIFECYCLE



29

Symantec Cyber Security Services | STRATEGY

Expanded services

- Incident Response and Forensics services
- Security Simulation Services for security preparedness and overall health checks

Scale up of existing and new services with core tech

- Big Data-based streaming & batch analytics
- High speed ingestion of large and ever growing log data

Expanded global footprint

- Expansion of number of SOCs globally to address demand as well as regulatory requirements



30

Symantec Cyber Security Services | SUMMARY OF KEY CAPABILITIES

 Security Monitoring Services	 IR and Simulation Services	 Threat Intelligence Services
<ul style="list-style-type: none"> • Key technology IP for log collection, analytics, and incident investigation • Tailored to customer maturity/industry • High-touch 24x7 service model • Integration with next gen security infrastructure to detect advanced threats 	<ul style="list-style-type: none"> • Global team with extensive experience in forensics investigation • Emergency/Retained/Managed options • Integrated with SOCs to provide end to end service • Realistic live fire training missions delivered as a SaaS solution 	<ul style="list-style-type: none"> • Global Intelligence Network • Early warning Portal • Adversary threat intelligence • Integrated IoCs from internal and external feeds
<p align="center">Global team of 500+ threat and intel experts with unique knowledge of attack actors; Supported by Cloud-based Big Data analytics infrastructure</p>		

31

Symantec Cyber Security Services | KEY REVENUE OPPORTUNITIES

Net New Customers

- Integrated suite of services covering monitoring, IR, threat intelligence, and security simulation

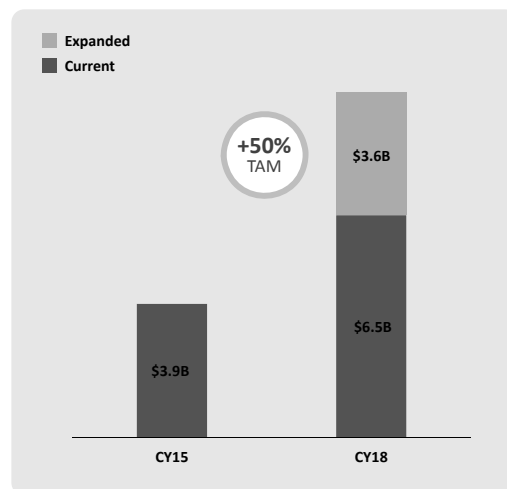
Installed Base

- Cross-selling of IR and Simulation Services into Monitoring service installed base

Specific opportunities within Public Sector


- Security best practices and solutions tailored for agencies

Data residency and regulatory compliance enables expansion into new geographies




Source: Gartner and Symantec Analyses

32


Symantec. | 2015 Financial Analyst Day




UNIFIED SECURITY ANALYTICS

UNIFIED SECURITY ANALYTICS


Cyber Security Services



Threat Protection


ENDPOINTS DATA CENTER GATEWAYS

Information Protection


DATA IDENTITIES


Unified Security Analytics Platform


33

Security Platforms Market | FOCUS SHIFTING TO ANALYTICS




ATTACKS ARE INCREASINGLY SOPHISTICATED

- Micro-targeted
- New techniques and zero day attacks
- Stealthy to remain undetected




EXISTING TECHNOLOGY CAN'T KEEP UP

- Reactive methods
- Insufficient data to find subtle trends and patterns
- Isolated approaches without broader context



ANALYST FATIGUE IS RAMPANT

- Too many alerts and false positives
- Slow and manual detection, forensics, and remediation



RISE OF SECURITY BIG DATA ANALYTICS

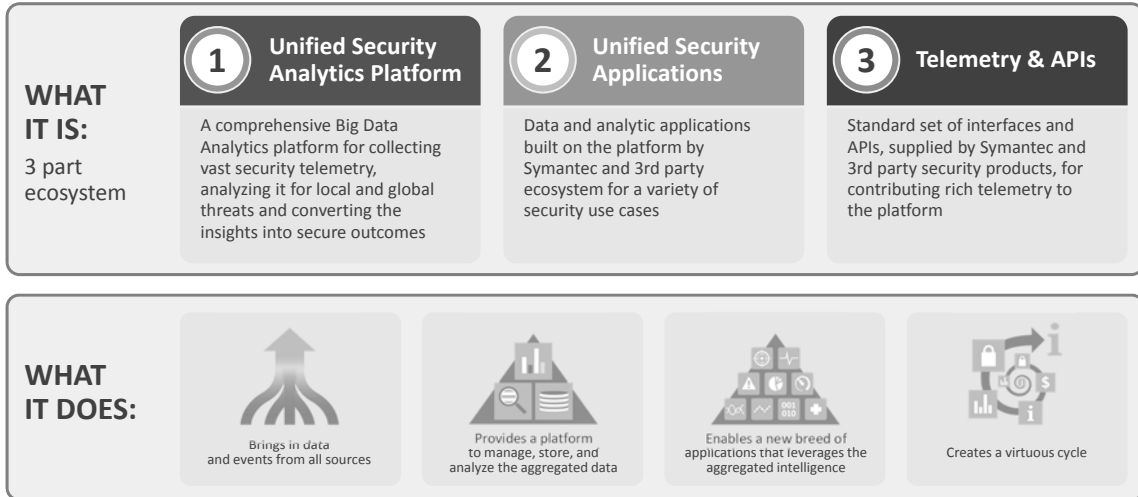
Big data, analytics, and machine learning techniques needed to address these challenges

34

ENTERPRISE SECURITY

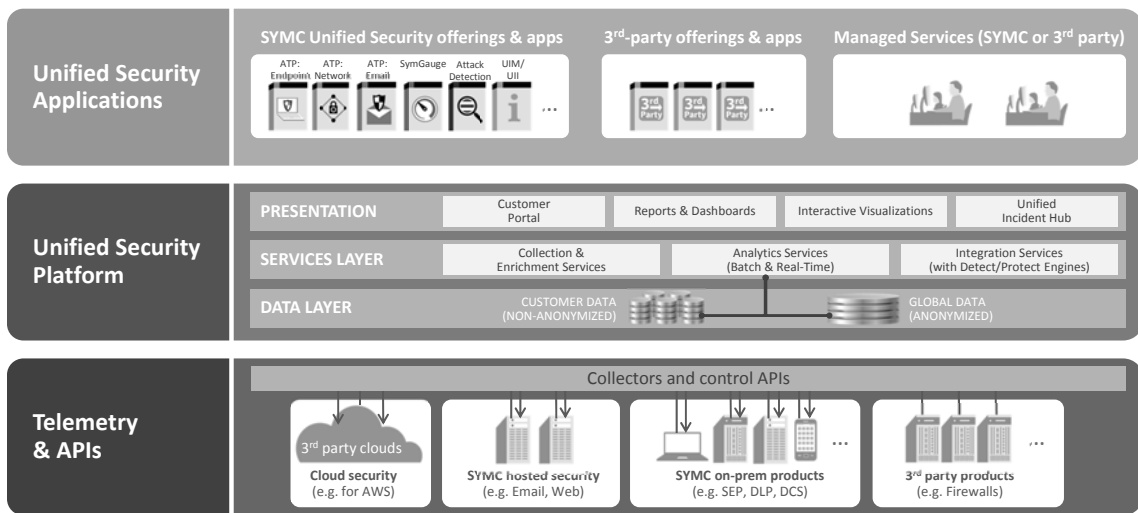
17

Symantec Unified Security in a Nutshell



35

Unified Security Analytics Blueprint



36

Scale Drives Unified Security Analytics



Enables solving a whole new class of customer use cases:

- Identify attacks through richer analytics and algorithms
- Increased visibility by connecting the dots across global telemetry
- Realization of better security outcomes



Changes the basis of competition:

- Scale of security data we collect across endpoints, gateways, applications, and users
- Ecosystem that is difficult to replicate
- Uniquely differentiated offerings
- We already operate the largest civilian threat intelligence network on the planet





Accelerant for continued innovation:

- Platform and telemetry
- Robust set of services with cloud-scale architecture
- Enablement of 3rd parties to innovate on our platform

37

Value Created Through Scale

	How We'll Monetize 	Additional Value We Capture 
Unified Security Analytics Platform	<ul style="list-style-type: none"> • Access to the platform 	<ul style="list-style-type: none"> • Drive cross-sell through increased value of all of our offerings
Unified Security Analytics Applications	<ul style="list-style-type: none"> • Encourages new analytics applications built on our vast intelligence 	<ul style="list-style-type: none"> • Revenue share from 3rd parties
Telemetry & APIs	<ul style="list-style-type: none"> • More effective detecting, blocking, and remediating of attacks than anyone else 	<ul style="list-style-type: none"> • Increased telemetry from our product drives synergy across the ecosystem

38

Sample Unified Security Analytics Applications



SymGauge

- Risk Advisor and Benchmarking App
- Measures and benchmarks security health, including risks arising from compromised end-users



Incident Investigation

- Drill into incidents to get all associated events across security control points, building out the full attack chain
- Ex: Discover when and how a threat first entered the environment



Targeted Attack Detection

- Crawls through global telemetry to find targeted attack IOCs and detect brand-new targeted attacks
- Ex: find all emails sent from a given address, all files attached to those emails, all events associated with those files, etc.



Moneyball

- Correlate security outcomes across customers with differing security controls, policies, and settings
- Quantify ROI for potential new security investments

39

SymGauge (“Taste Test”) Application



Validating Our Unified Security Hypothesis

Three questions to answer

- How useful is our data?
- Can we analyze the data to find significant threats?
- What’s the best way to monetize?



“Taste Test” Experiment with a Large Bank

Analyzed our global SEP telemetry

- Found targeted attack activity
- Provided analysis of exploits in use
- Calculated security ranking

Analyzed our global Norton data

- Identified active phishing campaigns
- Found “spoofed” banking apps
- Showed “hygiene” of customers accessing the bank’s site

Result: “Shocked” CISO and landed multi-million dollar deal with a suite of offerings



SymGauge Automated Taste Test

- Taste Test took 2 analysts > 6 weeks... this doesn’t scale
- Solution: automate!
- Now developing SymGauge, an automated Risk Advisor and Benchmarking application
- Narus acquisition accelerating implementation



40

Agenda

1	Market Opportunity
2	Product Strategy
3	Roadmap & Go-To-Market

41

Symantec Enterprise Security | RAPID RELEASE CYCLES

18 MONTH ROADMAP					
THREAT PROTECTION	ATP (Network)	ATP (Email, Endpoint)	Cloud Endpoint Management	Cloud Workload Protection	
	Email Security with DLP	Endpoint Forensics	Endpoint Remediation		Datacenter Security As a Service
INFORMATION PROTECTION	DLP/ Office365	DLP/ Box.Net	DLP/ SFDC & WDAY	DLP As a Service	Cloud based Key Management
	Biometric Authentication	Cloud Security Broker	User Behavioral Analytics	Identity As a Service	
CYBER SECURITY SERVICES	IR Retainer Service	Simulation Service		IR Managed Service	
	ATP Monitoring Service	MSS Self-Service Admin Portal	IR Readiness Assessment		MSS Log Mgmt As a Service
UNIFIED SECURITY ANALYTICS		SymGauge App (TasteTest)	Targeted Attack Detection App	Incident Investigation App	Moneyball App
		Analytics Platform Internal Preview	Analytics Platform Customer Preview	Analytics Platform Gen. Availability	Analytics Platform 3 rd Party SDK
	New Product	Enhanced Product	Preview Releases		

42



Symantec Enterprise Security | FOCUSED GO TO MARKET



1,750

Strong
Enterprise Security
Sales Team

DEDICATED SALES



40%

More
Quota Carrying Field
Reps

MORE FEET ON THE STREET



3X

More
Solution
Architects

MORE SECURITY EXPERTS



3X

Increase
in Coverage for
Global Key Accounts

KEY ACCOUNT PROGRAM

Complemented by Partner and Channel ecosystem with rewards re-aligned to growth;
Commercial growth through Inside Sales, with focus on SaaS, Subscriptions, and Renewals

43

Symantec Enterprise Security



Large market with **35%-50%** increase in TAM driven by new product pipeline targeting growth segments



Increasing momentum through dedicated sales focus and more quota carrying reps



Unrivalled threat intelligence and telemetry drives innovative platform, products, and services



Leverage from large installed base in key segments will accelerate growth

44

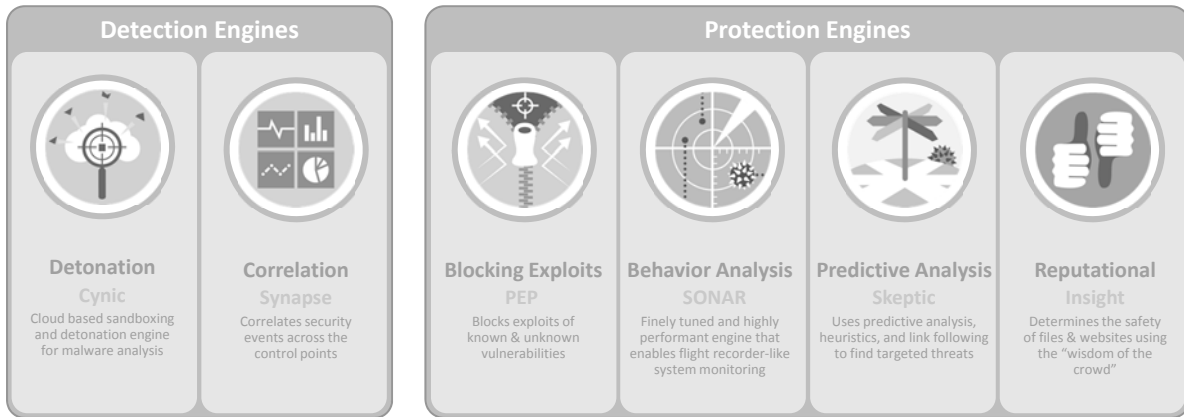
Q&A

Jeff Scheel, SVP, Corporate Development, Alliances and Strategy
Balaji Yelamanchili, EVP & GM, Enterprise Security Business Unit
Amit Mital, EVP, CTO & Emerging Endpoints

45

Appendix

Symantec Threat Protection | PROVEN AND INNOVATIVE TECHNOLOGIES



47

Symantec Info Protection | PROVEN AND INNOVATIVE TECHNOLOGIES



48