Unified Security

Stephen Trilling
Senior Vice President of Product Management, Symantec

CURRENT STATE

Managing security
is expensive

Security integration
is manual and complex

Each enterprise
is an island

Targeted attacks may go
undiscovered for months

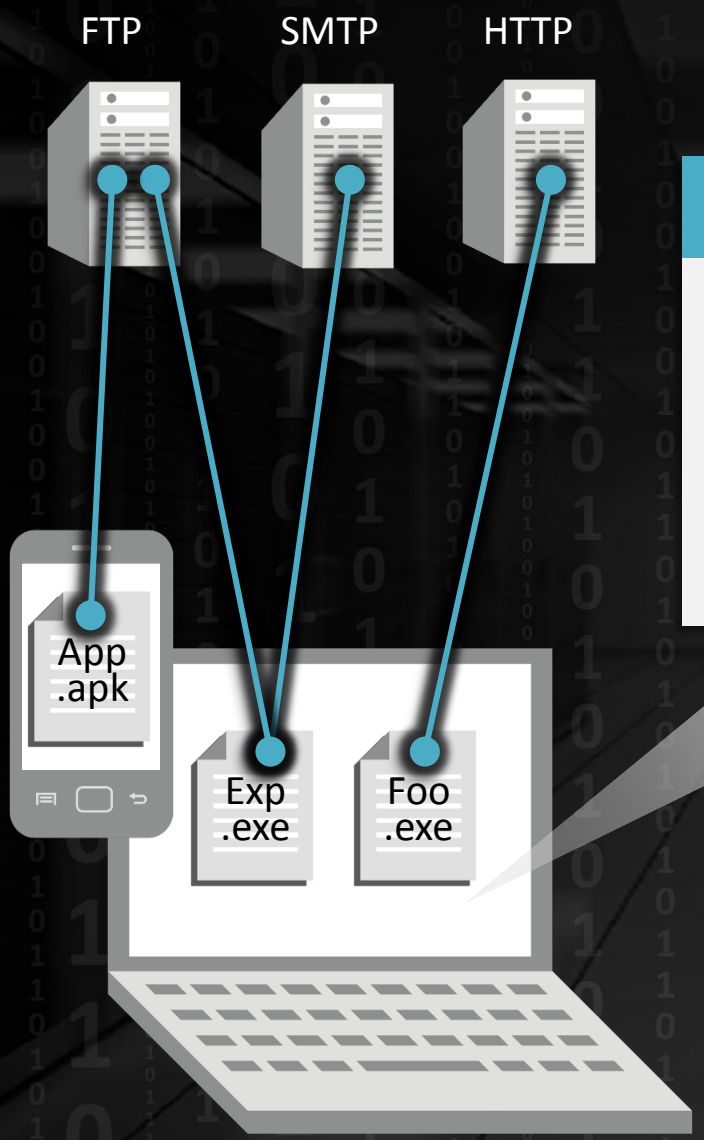
FUTURE STATE

Managing security is
simple and easy

Your security is
integrated for you

You're part of a
community

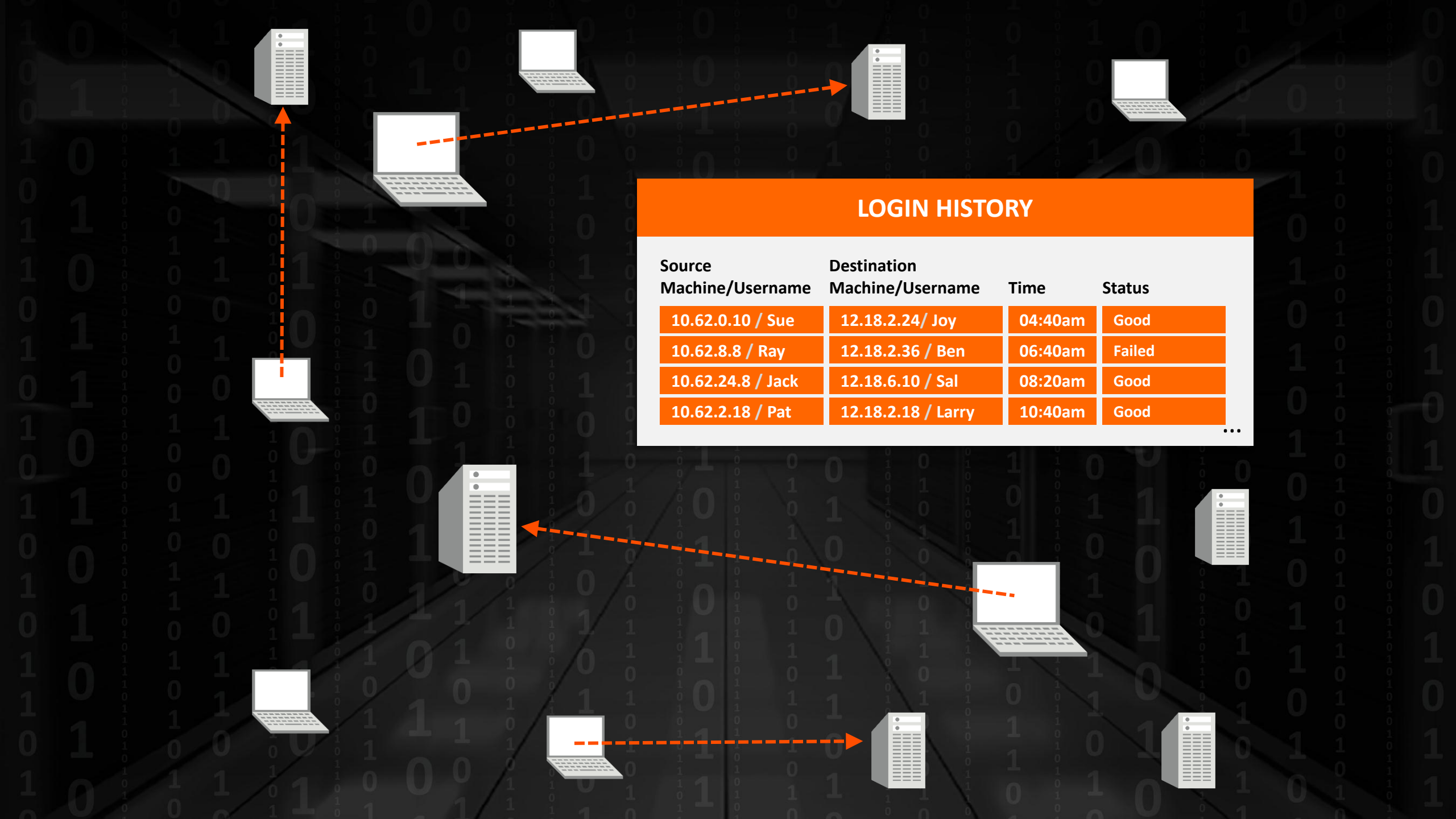
Complex attacks discovered
within minutes or hours



CONNECTION HISTORY

Source Machine/Username	Destination Machine/Type	Time	File
Laptop-8 / Fred	12.18.2.22 / FTP	04:00pm	Exp.exe
Laptop-8 / Fred	36.16.2.38 / HTTP	06:30pm	Foo.exe
Android-4 / Sue	07.72.6.10 / FTP	08:20pm	App.exe
Laptop-8 / Fred	88.42.2.8 / SMTP	10:20pm	Exp.exe

...



LOGIN HISTORY

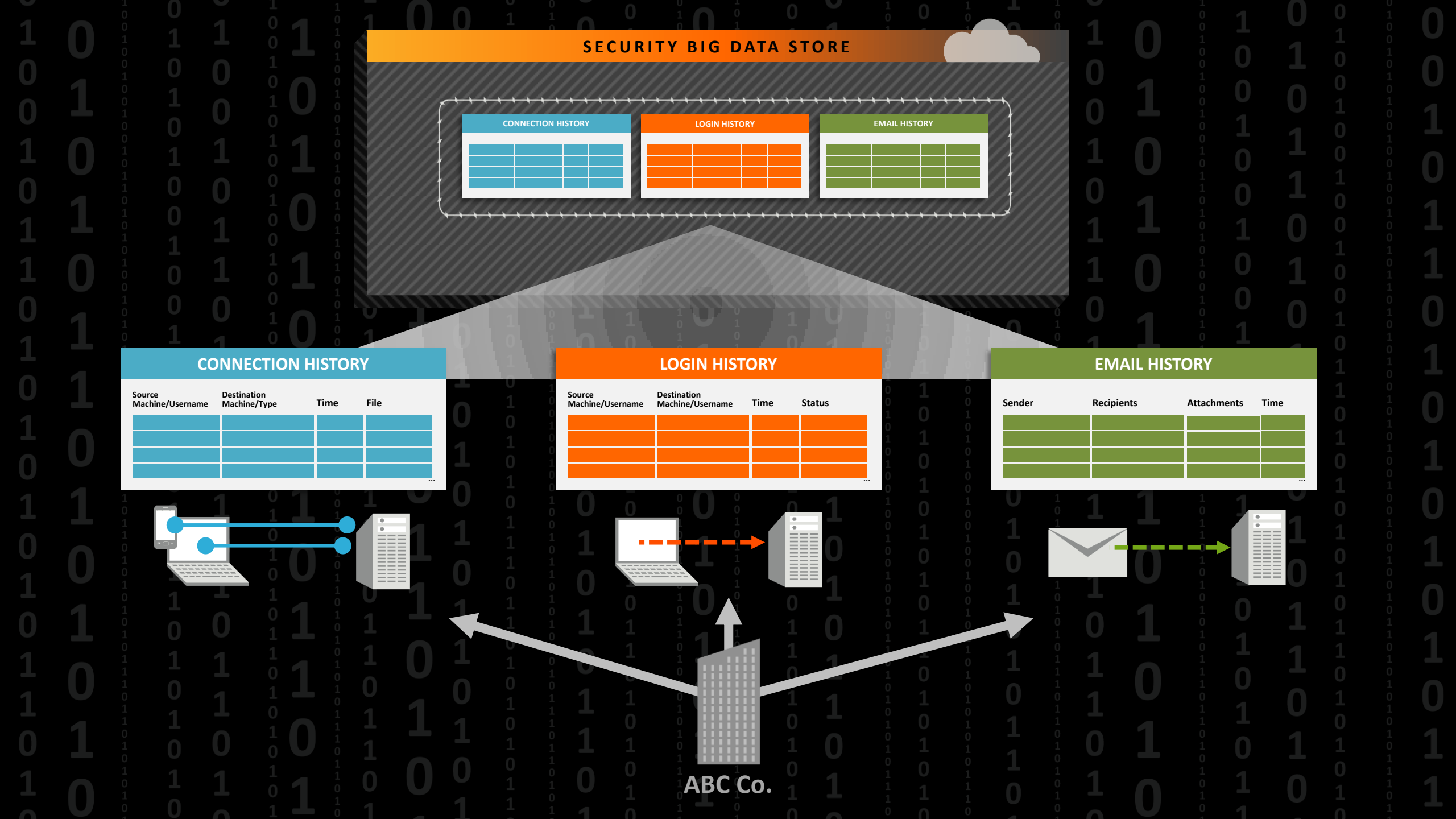
Source Machine/Username	Destination Machine/Username	Time	Status
10.62.0.10 / Sue	12.18.2.24/ Joy	04:40am	Good
10.62.8.8 / Ray	12.18.2.36 / Ben	06:40am	Failed
10.62.24.8 / Jack	12.18.6.10 / Sal	08:20am	Good
10.62.2.18 / Pat	12.18.2.18 / Larry	10:40am	Good

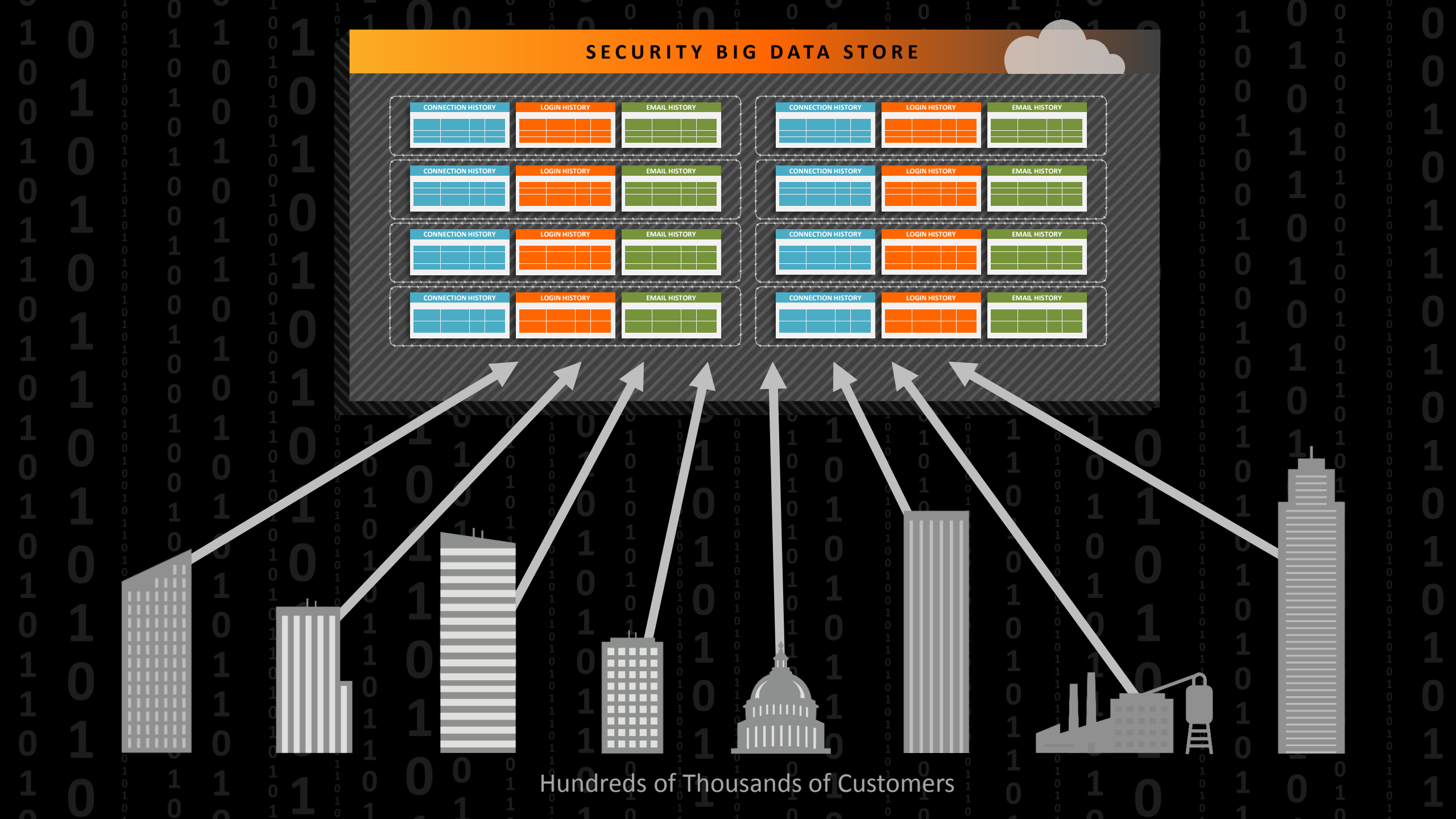
...

EMAIL HISTORY

Sender	Recipients	Attachments	Time
Joe@acmeco.com	Sam@industry.com	Exp.exe	8:30pm
Bob@acmeco.com	Max@industry.com	Foo.exe	9:20pm
Sue@bravoco.net	Lou@industry.com	graph.pdf	10:20pm
Kay@delta.org	Ron@industry.com	debt.doc	2:00am

...


SECURITY BIG DATA STORE
CONNECTION HISTORY
LOGIN HISTORY
EMAIL HISTORY
CONNECTION HISTORY
Source Machine/Username
Destination Machine/Type
Time
File
LOGIN HISTORY
Source Machine/Username
Destination Machine/Username
Time
Status
EMAIL HISTORY
Sender
Recipients
Attachments
Time
ABC Co.


SECURITY BIG DATA STORE
CONNECTION HISTORY
LOGIN HISTORY
EMAIL HISTORY
Hundreds of Thousands of Customers

Symantec | attack graph generation system

http://symantec/attack_graph_generation_system

Web Search | Go | Favorites | Page | Safety | Tools

symantec | attack graph generation system

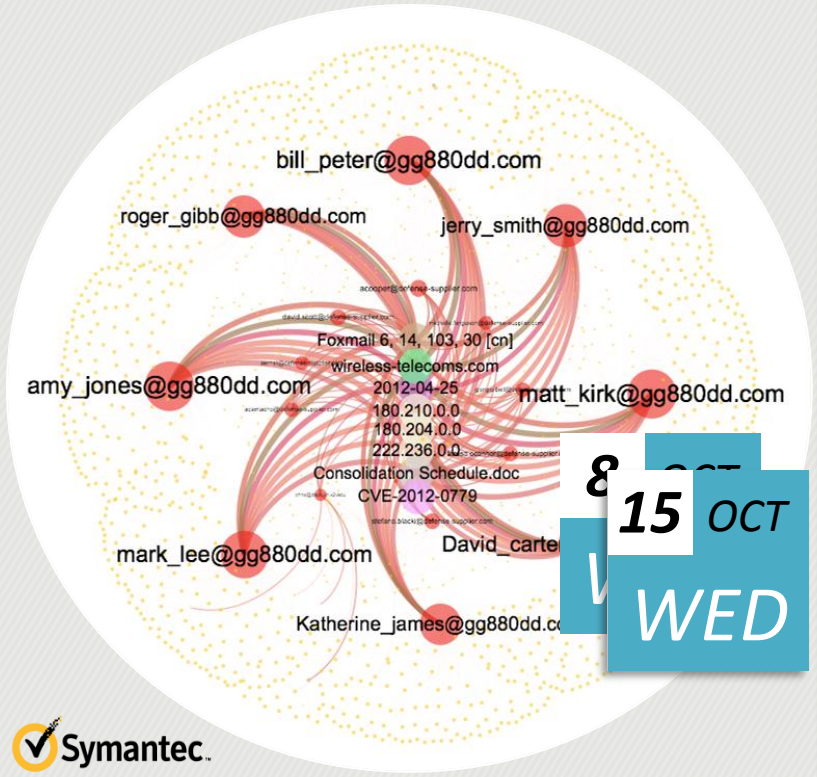
!! High-priority Security Incidents !!

Attack ID	Severity	Time	Comments
173528	High	18:08	Potential targeted attack linked to other financial sector firms
[redacted]	[redacted]	[redacted]	[redacted]

VIEW FORENSICS

...

Forensic Graph for Attack ID 173528



Employees who connected to this IP: 180.204.0.0

Employee login names:

Bill_Neuman	Joe_Spearman
Jane_Simpson	Rebecca_Painter
Barbara_Smith	Tara_Layton
Frank_Pearson	Edward_Miller
Richard_Neymann	Bella_Johnson
Howard_Gleason	Gena_Gladstone

Employees and file names attached to each email:

Employee:	File:
Bill Neuman	YT28AB.exe
Jane Simpson	Hiring Plan.docx
Barbara Smith	Order #448.pdf
Frank Pearson	Foo.exe
Richard Neymann	Agenda.docx
Howard Gleason	Q2-financials.xlsx

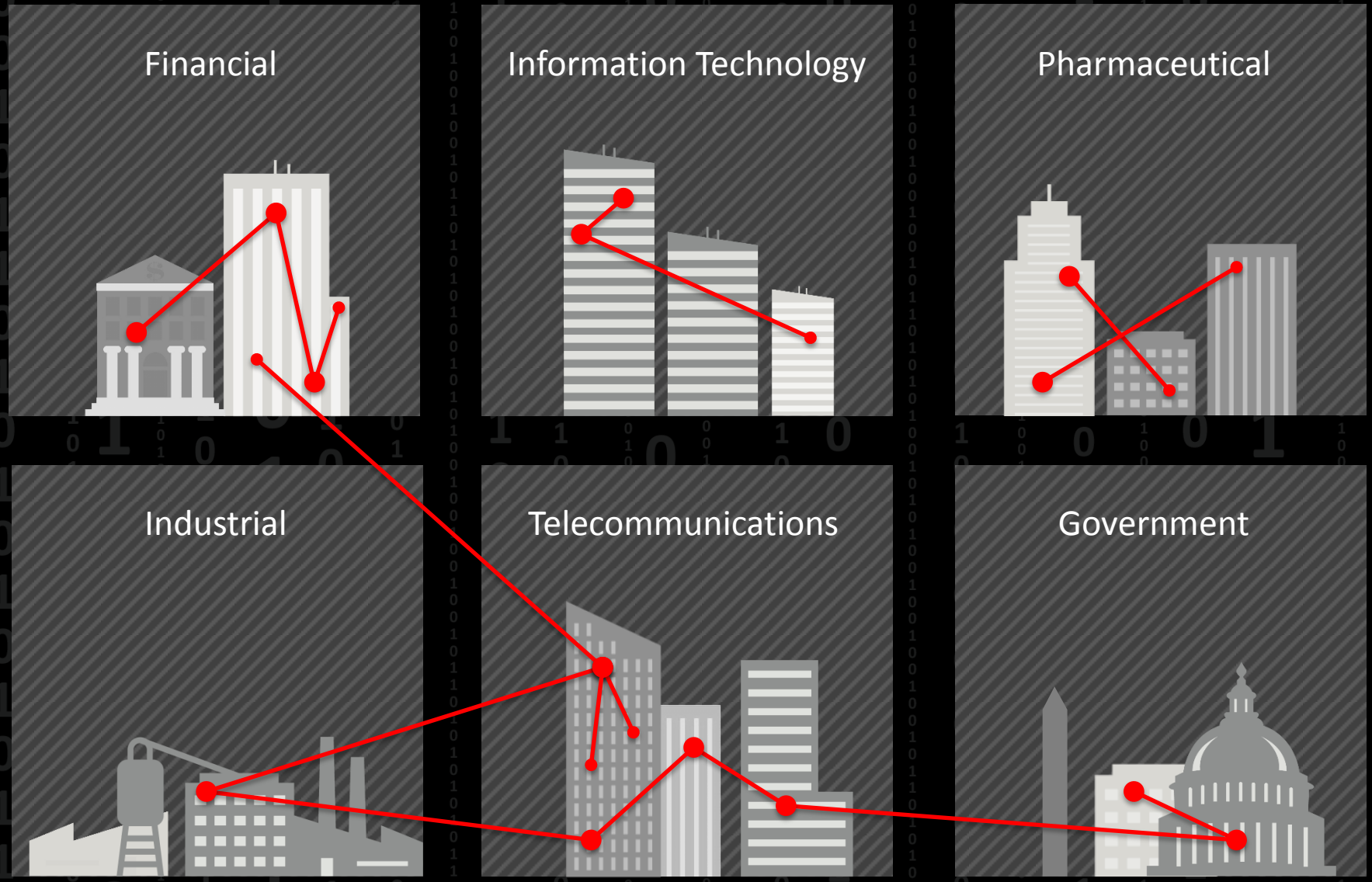
Done | Internet | Protected Mode: Off | 100%

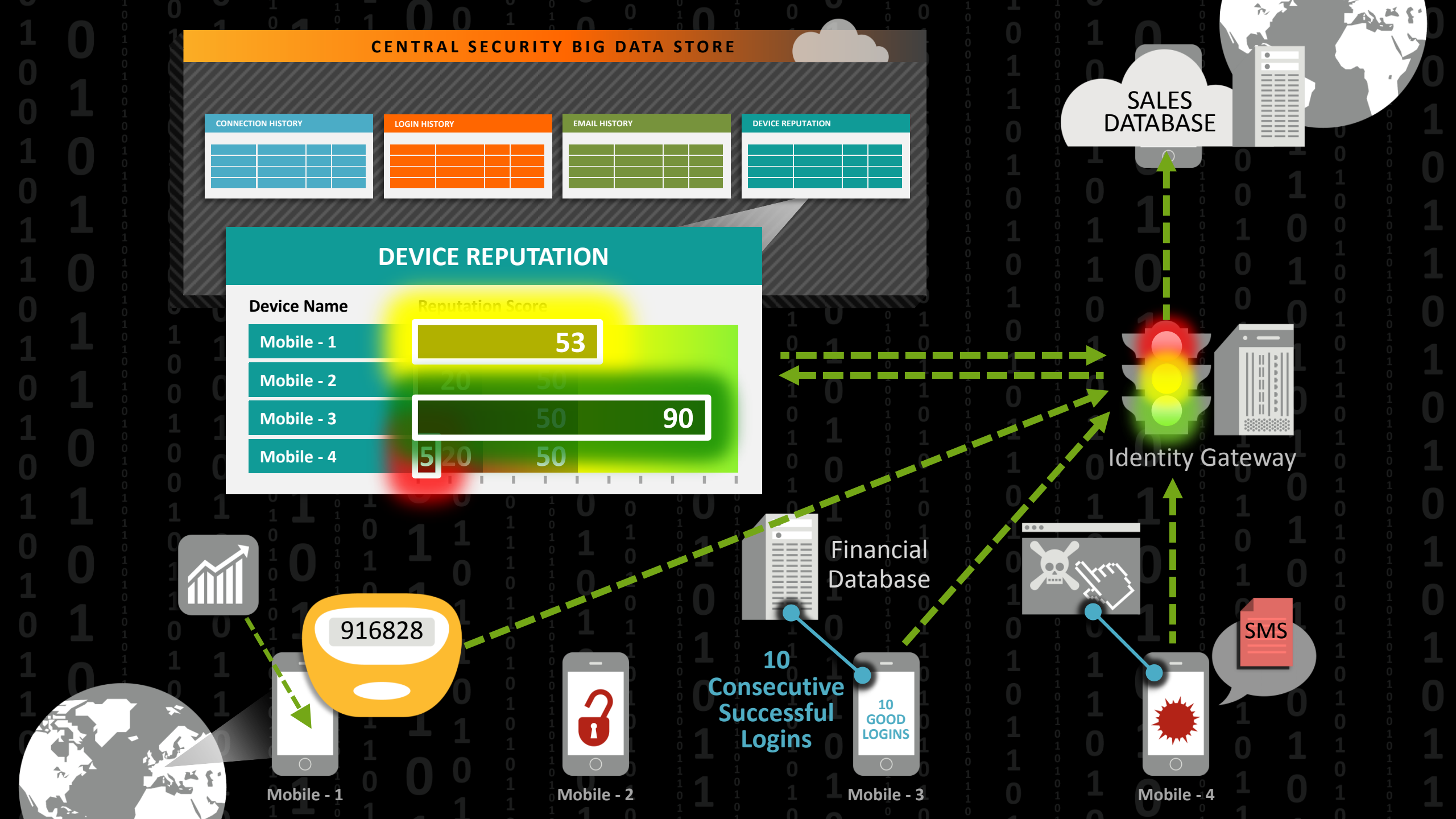
Source

Source

Company 1

Company 2


Financial
Information Technology
Pharmaceutical
Industrial
Telecommunications
Government


CENTRAL SECURITY BIG DATA STORE
CONNECTION HISTORY
LOGIN HISTORY
EMAIL HISTORY
DEVICE REPUTATION
DEVICE REPUTATION
Device Name
Reputation Score
Mobile - 1
53
Mobile - 2
Mobile - 3
90
Mobile - 4
5
20
50
SALES DATABASE
Identity Gateway
Financial Database
916828
10 Consecutive Successful Logins
10 GOOD LOGINS
SMS
Mobile - 1
Mobile - 2
Mobile - 3
Mobile - 4

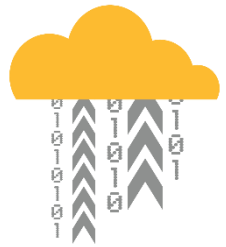
Apps

Industry peer discussion boards

Threat news

- Featured
- C&C
- Targeted Attack
- Insider
- Compliance
- Detection

Featured



C&C Detector
Supercoil Software
★★★ $8,000

Load Look
Level18 Studio
★★★★★ $10,000

Target Sweep
GO Getit EX
★★ $10,800

Best Sellers

UNIFIED SECURITY
VISION

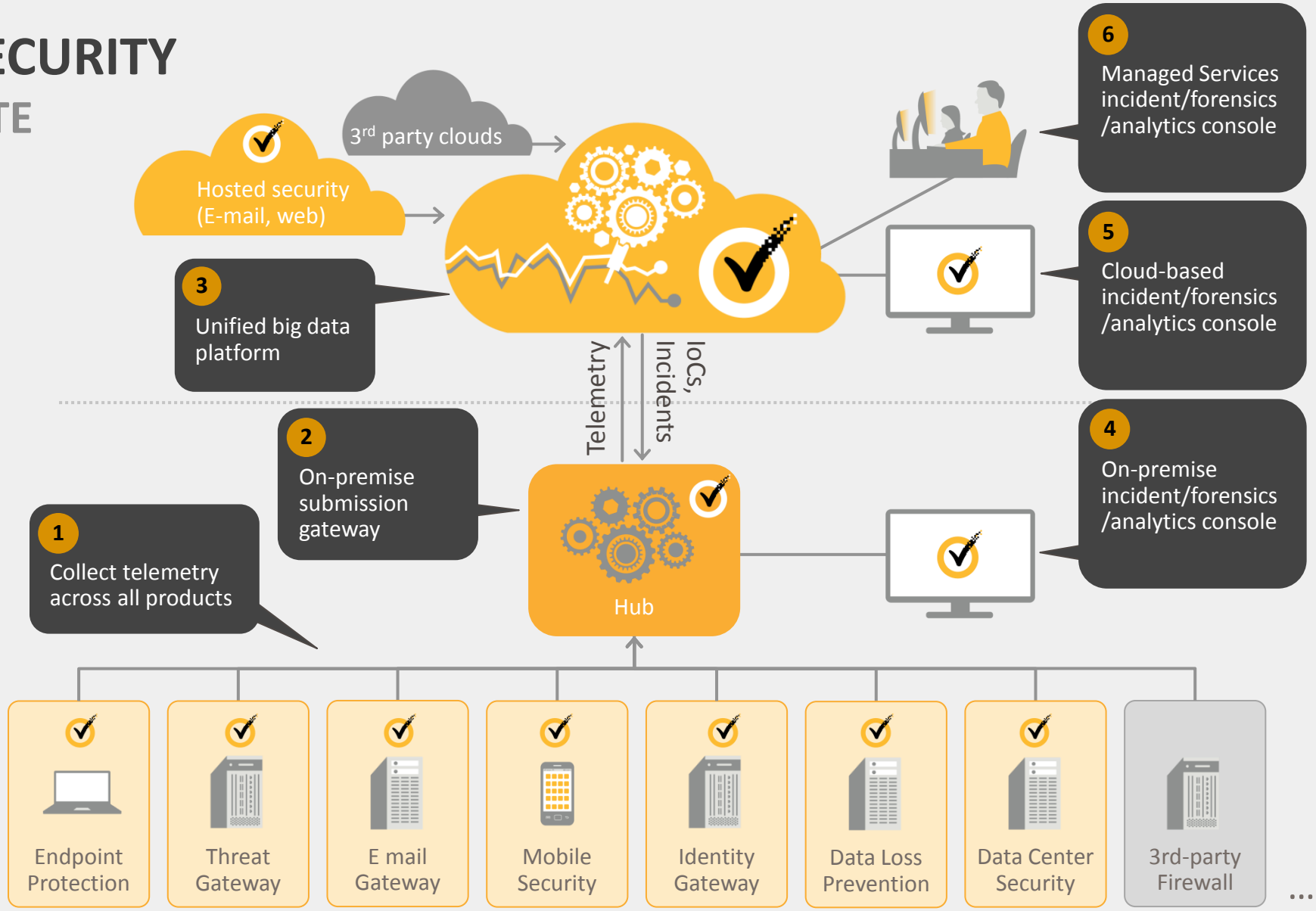
Symantec will provide a
unified security platform

that leverages the combined **visibility** and **intelligence**
of all of our offerings (augmented by 3rd-party data)

to **block**, **detect**, and **remediate attacks**,
and **protect information**, better than anyone else.

UNIFIED SECURITY

FUTURE STATE



SYMANTEC'S BIG DATA SYSTEM TODAY

- **100s of millions** of contributing users/sensors
- **3.7 trillion** rows of security telemetry
- Over **7 billion** file, URL and IP classifications
- We ingest **200,000** new rows of security data every second!

UNIFIED SECURITY NEXT STEPS

Symantec Gateway Security: Threat Defense

Provides a prioritized list of suspicious activity discovered at the gateway

Symantec Email Security.cloud: ATP

Provides analysis of targeted attack activity observed in email

Symantec Endpoint Security: ATP

Provides a prioritized list of suspicious activity across all endpoints

Managed Security Services ATP

Correlates endpoint data with events from 3rd-party network security vendors, to discover suspicious activity

SYMANTEC ENDPOINT SECURITY: ATP
TARGETED ATTACK PROTECTION

Our endpoint presence is a huge advantage

- SEP is installed on **120 million endpoints**
- The endpoint has **unparalleled visibility** into **threat activity** in the enterprise
  - Behavior of all running programs, all connections, all downloads, all attempted logins, etc.
  - We have **3.7 trillion pieces of security data** in STAR's back-end big data system, largely from endpoints
- This same endpoint visibility **provides forensic history** after an attack

And, a big opportunity

- Our new **Symantec Endpoint Security: ATP** offering will provide sophisticated **targeted attack** detection and **forensic** capabilities on a **per-customer** basis
  - We will correlate our massive global attack telemetry with local data from each customer to uncover attacks that are specifically targeting that customer
- This requires **no new client software**
- This is a big step towards delivering on our broader **Unified Security** strategy

SYMANTEC ENDPOINT SECURITY: ATP

TARGETED ATTACK PROTECTION

How it works

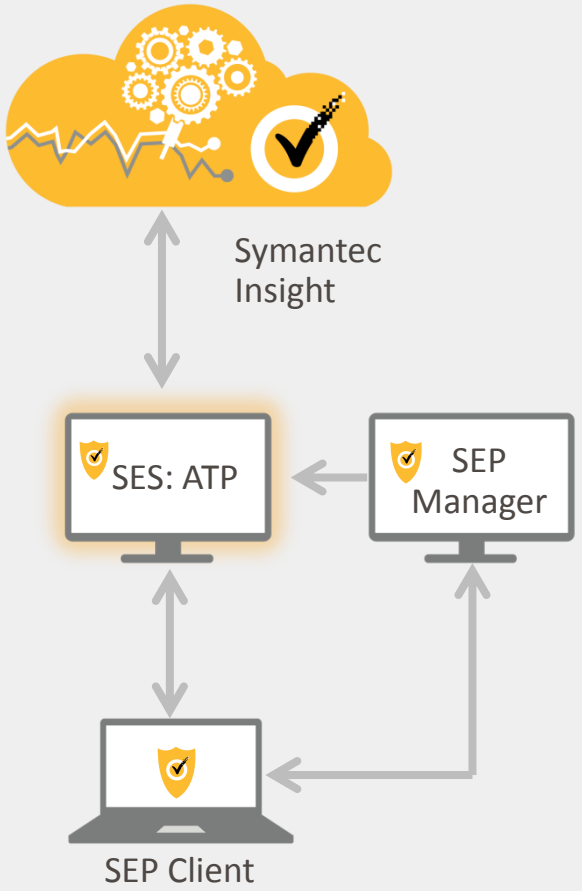
- Sees all queries/responses between SEP endpoints and the Symantec Insight cloud
- Gathers data from SEP Manager

Who it's for

- Primary user is the "Targeted Attack Admin" rather than the "Endpoint Admin"

Primary customer benefits

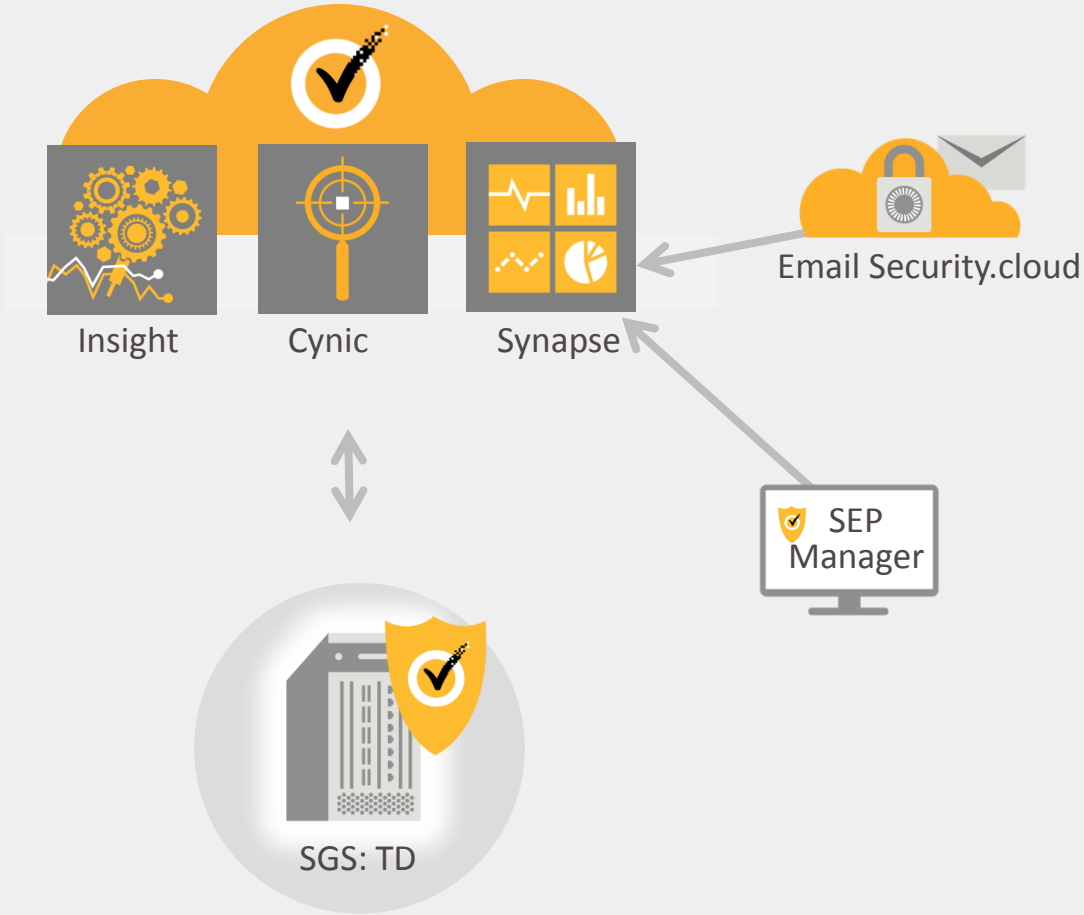
- Correlates suspicious activity across all endpoints to **discover new targeted attacks**
- Provides **forensic information** to help customers discover the overall scope of an attack
- Helps customers **recover from attacks** by blacklisting bad files across the environment
- Helps **reduce false positives** by allowing customers to whitelist good files
- Provides customers with **visibility and control** of data submitted to Symantec



SYMANTEC GATEWAY SECURITY: THREAT DEFENSE

TARGETED ATTACK PROTECTION

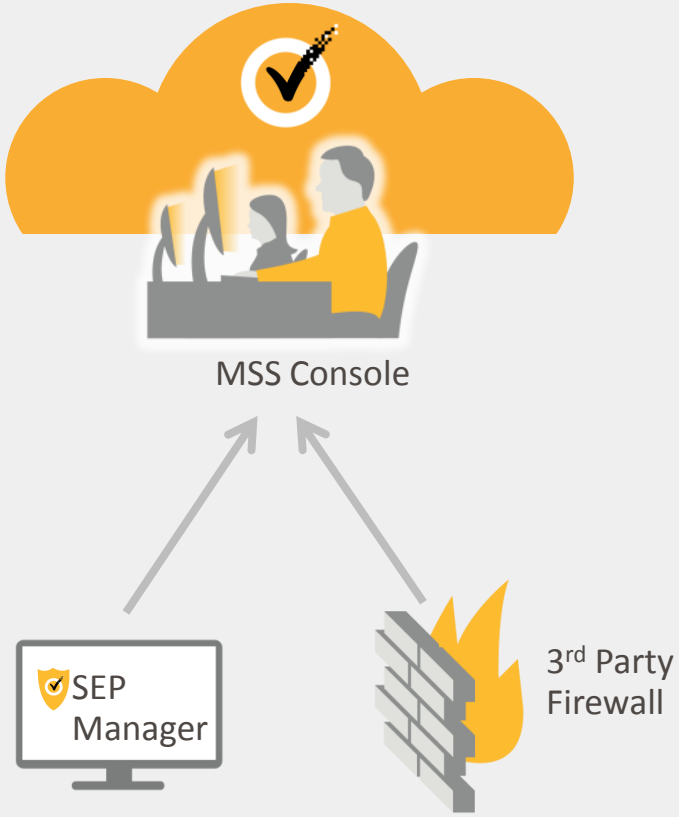
- Scans/blocks incoming gateway traffic with all of Symantec's industry-leading protection technologies (Insight, Intrusion Prevention, etc.)
- Leverages an entirely new virtual execution service to uncover complex targeted attacks ("Cynic")
- Correlates suspicious gateway activity with endpoint and email activity (via "Synapse")
  - Provides a prioritized list of suspicious events for the gateway administrator to investigate
- Will be delivered as either a physical or virtual appliance



MANAGED SECURITY SERVICES ATP

TARGETED ATTACK PROTECTION

- New offering for our Managed Security Service customers
- Correlates data from 3rd-party network security products with…
  - events from Symantec Endpoint Protection,
  - and with Symantec's global attack telemetry
- Enables customers to more quickly investigate, contain, and remediate targeted attacks
- Network Partners: Checkpoint, Palo Alto Networks, Sourcefire/Cisco
- Shipped June 2014



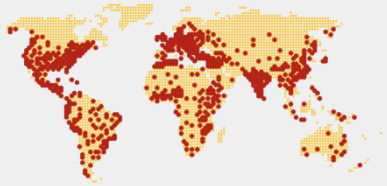
RECENT AND NEAR-TERM PRODUCT UPDATES

Endpoint Protection	Encryption	Data Loss Prevention	Data Center Security
• SEP 12.1.5 added protection and management enhancements with integrated Power Eraser (October 2014) • Improvements for embedded systems, new web-based SEPM console, integration of encryption (Targeted 2015)	• Endpoint Encryption 11 integrated PGP and GuardianEdge platforms into a single offering (October 2014) • Adding management support for 3rd-party encryption platforms, support for cloud-based encryption (Targeted 2015)	• Extending DLP support to the cloud with integration with Microsoft Exchange Online • Targeted December 2014	• New Data Center Security: Operations Director will help automate security processes on VMware NSX • Targeted March 2015

RECENT AND NEAR-TERM PRODUCT UPDATES

Identity	Mobility	Converged Management/Security
• New Symantec Identity Access Manager 2.0 makes accessing cloud applications simple and secure • Targeted Jan 2015	• Mobility Suite 5.0 provides integrated device management, app management, and security, in a single modular offering • October 2014	• Symantec Cloud Security: Endpoint and Mobility • Cloud-based offering built for channel partners, provides endpoint/mobile security and management • Targeted for Q2 2015

UNIFIED SECURITY: WHY SYMANTEC?



Symantec has the data footprint

- 100s of millions of contributing sensors

Symantec has the data diversity

- We will collect data across every control point
  - Desktop, server, cloud, mobile, etc.
- We will collect data across all of our products
  - Endpoint protection, gateway protection, data loss prevention, identity gateway, mobile management, encryption, compliance, etc.

Symantec has the big data experience

- Spent the last 6 years developing our advanced security big data system
  - Provides real-time protection to 100s of millions of systems
  - Holds 3.7 trillion security events, and collects 200,000 new events every second
- We will build on this experience to collect much more data across all of our products moving forward

Thank you!