
Forcepoint Risk Adaptive Security for Healthcare

Ozgur Danisman, MBA, CISSP, CISA, CISM

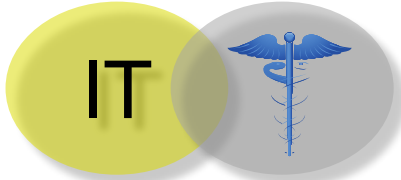
Head of Sales Engineering / Emerging Markets



Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

SECURITY IN HEALTHCARE...

Access prevails
(life-and-death matter)



Data Protection
Ignorant to Risks
Levels

Third party
and
contractors

Doctors &
Nurses

Employees

Shift to Cloud



Mobile initiatives and
medical devices



BYOD

Portable Medical
Devices

Challenges
and
Constraints

Non-patchable systems and
devices



Malware &
Cyberthreats

Insider Threats



APT

Escalated security concerns

HIPAA
Health Insurance Portability
and Accountability Act



Regulatory compliance

THE INTERSECTION OF PEOPLE AND DATA

Risk-Adaptive Protection

PEOPLE



DATA



Understanding the intersection of people, critical data and IP over networks and hybrid IT systems



WHAT WE ARE TRYING TO SOLVE?

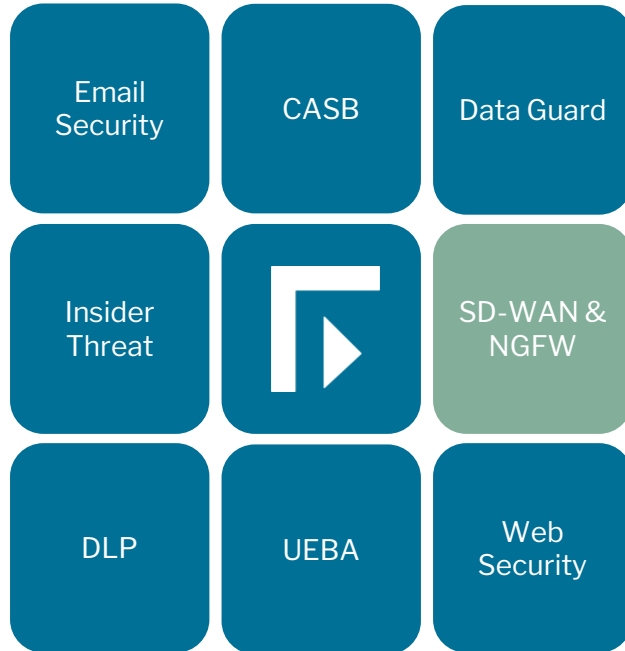
Protect important healthcare data and intellectual property wherever it resides, without:

- ▶ Frustrating users
- ▶ Overwhelming Security/IT Ops
- ▶ False positives / negatives

**WHILE ENABLING
BUSINESS TO FLOW**



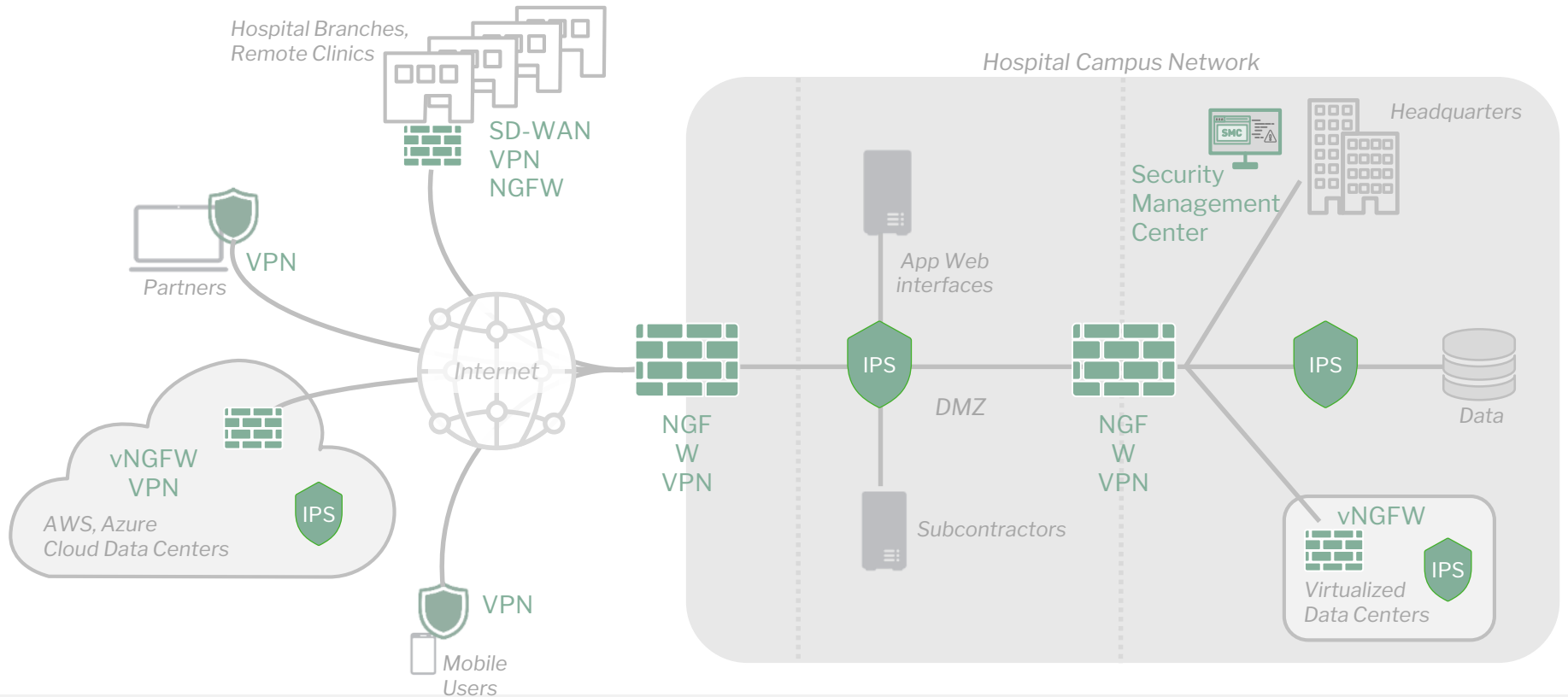
Forcepoint Security Portfolio for Healthcare



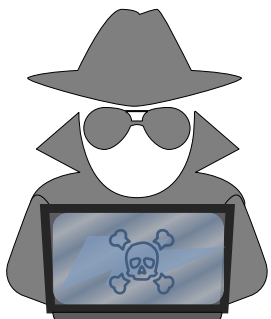
OUR VISION

Understand and respond to user intent to stop cybercrime before it occurs

One Network Security System, Many Uses



Network Security Must Defend Against Layers within Layers



Evasions

“camouflage”

App

(HTTP, SQL, etc.)

- Obfuscation
- Encoding

TCP

- Overlapping
- Extraneous

IP

- Out of Order
- Fragmentation



Exploits

“delivery vehicles”

*Unpatched
Vulnerabilities*

(SMB, Web, DB, etc.)

Zero-Days



Malware

“theft & compromise”

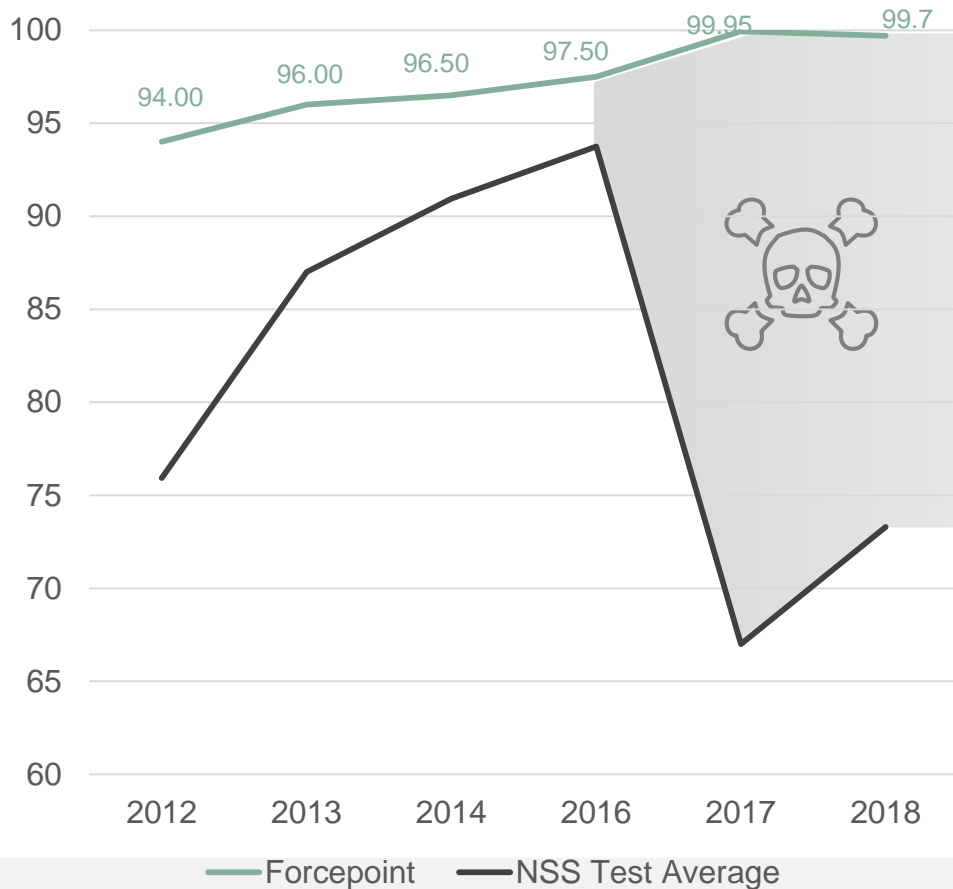
Ransomware

Data Theft

*User
Compromise*

*System
Corruption*

The Evasion Gap – Most Vendors Leave Networks Exposed



Many NGFW & IPS fail to stop evasions

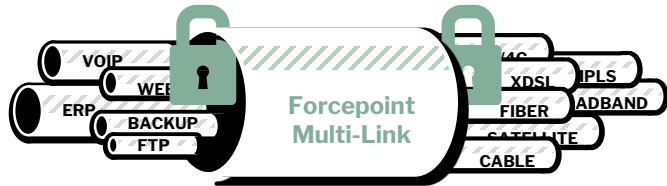
Exploit Kits now make evasions easy

- Metasploit
- Shadow Brokers leaked toolkit

Attacks combining techniques to spread

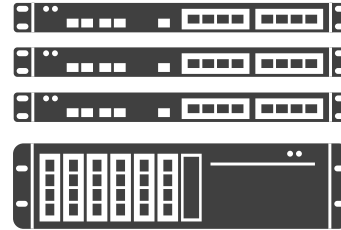
- Learning from WannaCry → Petya

High Availability & Scalability for Critical Networks



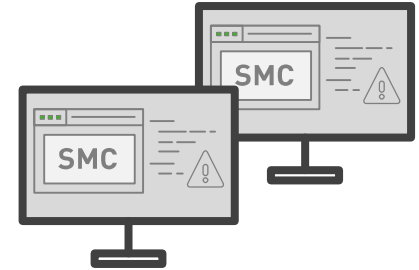
Clustered Networks

- Active-Active, transport-independent, multi-ISP
- Direct-to-Cloud high performance
- No external routers needed



Clustered Firewalls

- Active-Active, mixed devices/versions
- Scales to 16 nodes
- No external load balancers needed

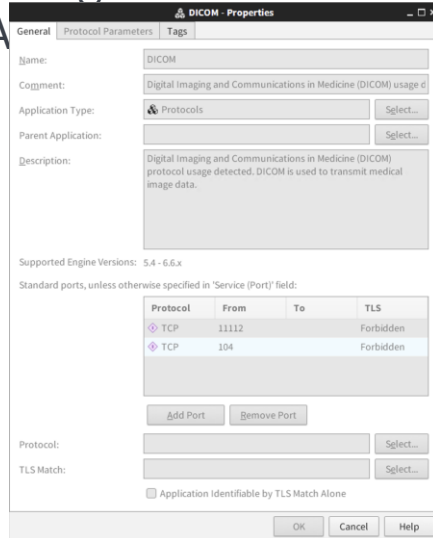


Replicated Management

- Policy-driven connectivity & security
- Failover for rapid recovery
- Distributed logs for ongoing visibility

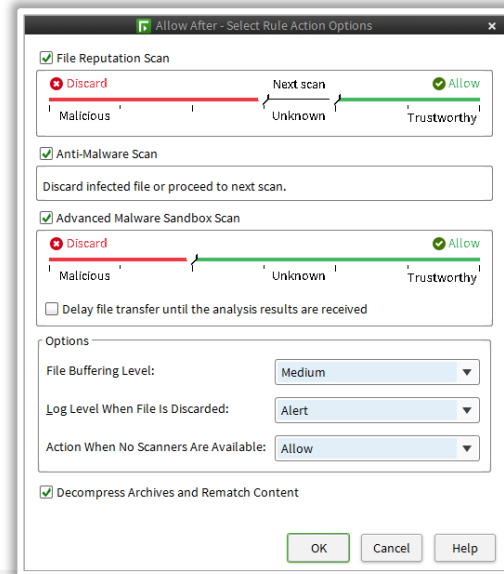
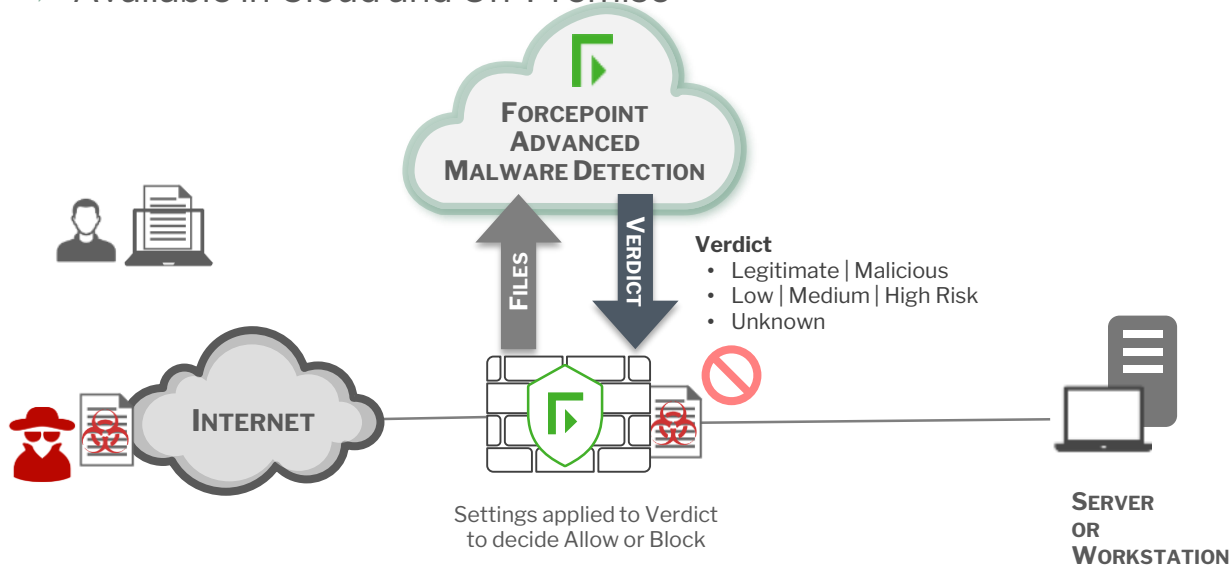
Healthcare Application Aware Segmentation Best Practices

- ▶ Group systems logically by trust levels, risk factors and security classifications independent of physical location. Each segment can have unique policies.
- ▶ Intra-segment traffic is allowed by default
- ▶ Inter-segment traffic is controlled by firewall and denied by default
- ▶ Traffic between segments is controlled based on Applications (e.g. DICOM), Users, IPS, ECA

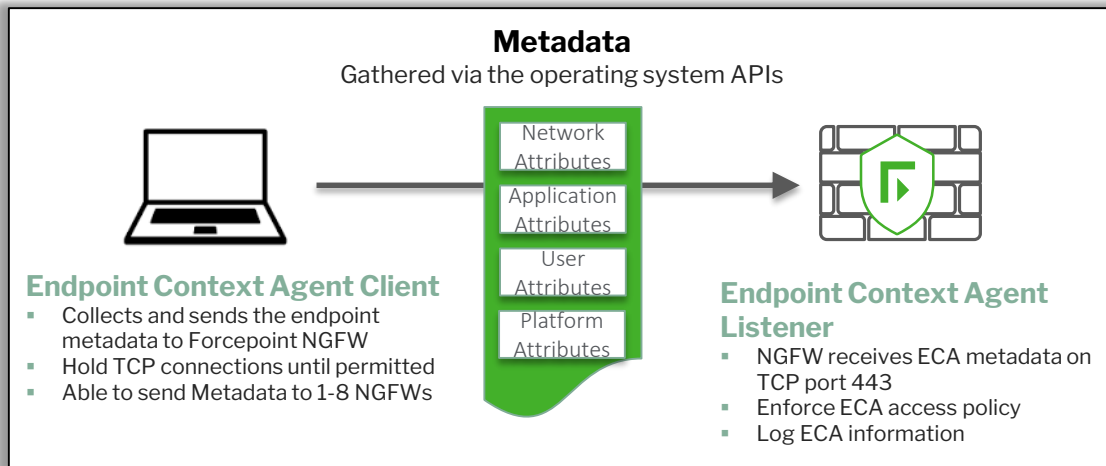


Forcepoint Advanced Malware Detection (AMD)

- ▶ Advanced Persistent Threats, Zero-Day Threats, and Advanced Malware
- ▶ Provide deep content inspection analyzes for unknown objects
- ▶ Available in Cloud and On-Premise



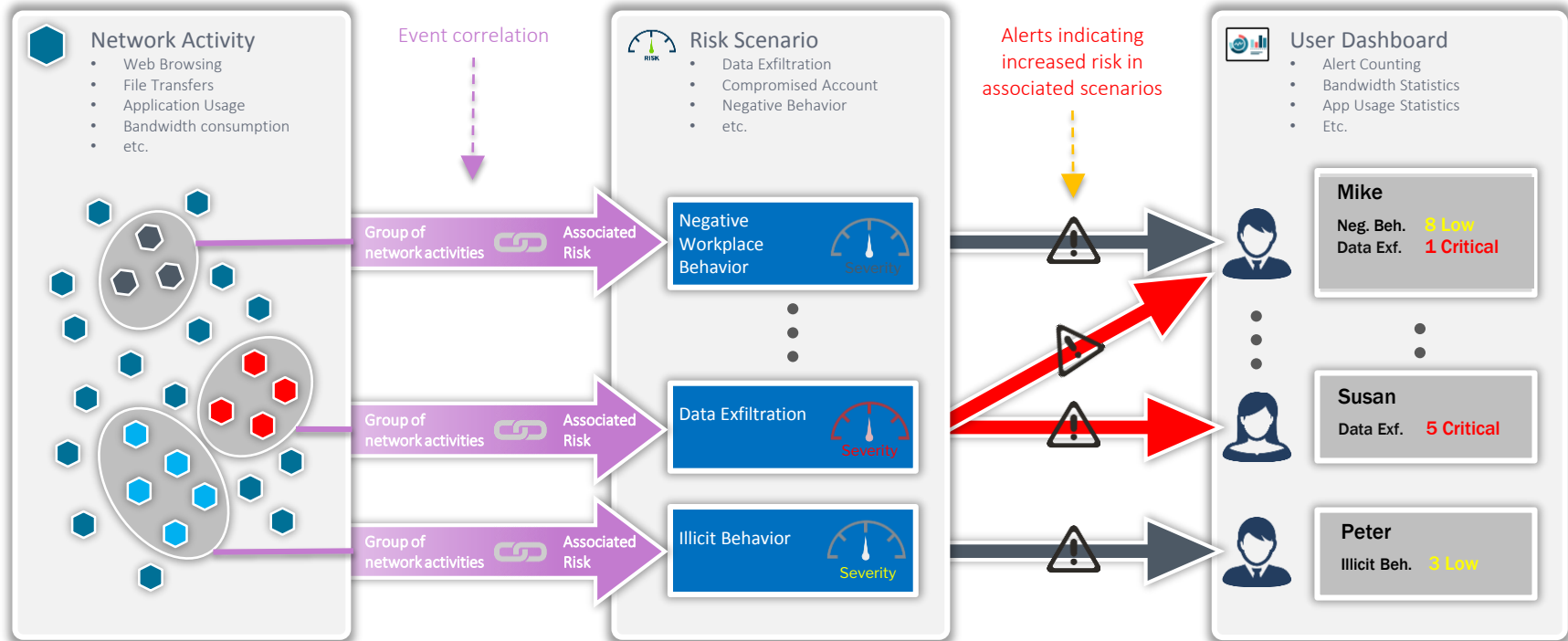
Whitelist Critical Client Applications on NGFW with Endpoint Context Agent (ECA)



CATEGORY	METADATA
Application Attributes	Executable binary name read from the signed executable file (String)
	Executable checksum(SHA-256/MD5)
	Executable product name (String)
	Executable version (String)
	Fingerprint of the signer certificate or public key
	Signature check result from OS (OK, not OK or not checked)
Platform Attributes	Signer name (String)
	AV status
	BIOS serial number
	Endpoint load (CPU, memory, disk)
	Full computer name
	Listening sockets, their interfaces and ports
	Local FW settings
	OS updates
	OS version
	User login/logout event
User Attributes	User Domain Name (String)
	User Group Information (String Array)
	User ID (String)
	User Type

ID	Source	Destination	Service	Action	Authentication	QoS Class	Logging
Automatic Rules Insert Point							
5.1	±± ANY	±± ANY	⚡ ANY	→ Continue			Transient No Closing Executable Enforced
5.2	🔗 ECA-Internet_Explorer_11	±± ANY	⚡ ANY	✅ Allow			
5.3	🔗 ECA-Internet_Explorer_10	±± ANY	⚡ ANY	❌ Discard			
	🔗 ECA-Internet_Explorer_4						
	🔗 ECA-Internet_Explorer_5						
	🔗 ECA-Internet_Explorer_6						
	🔗 ECA-Internet_Explorer_7						
	🔗 ECA-Internet_Explorer_8						
5.4	±± ANY	±± ANY	⚡ ANY	✅ Allow			
Discard all							

User Behavior Alerts



User Dashboard Drilldown

The screenshot shows the Forcepoint NGFW Security Management Center interface. The user 'kkuster' is selected in the 'Users' list on the left. The main dashboard displays 'AD Information' and 'Endpoint Information' for the user, along with 'Top Bandwidth by Application' and 'User Behavior Events'.

AD Information:

- Name: Kristian Kuster
- IT Technician
- Helsinki Office
- Email: kkuster@forcepoint.com
- Phone: +60675124334
- Member of: Helsinki

Endpoint Information:

- Name: kkuster
- IP Address: 44.43.194.24
- Operating System: Windows 7
- Operating System Updated: 4 months ago
- Anti-virus Status: Enabled, and virus definitions are up-to-date

Top Bandwidth by Application:

Application	Bandwidth	Percentage
TLS-1.2	7.91 kB	27.1%
AliExpress	6.88 kB	23.6%
Hao123	5.48 kB	18.8%
WhatsApp	5.01 kB	17.2%
Tumblr	3.60 kB	12.3%
Application-Unknown	278 B	0.9%

User Behavior Events:

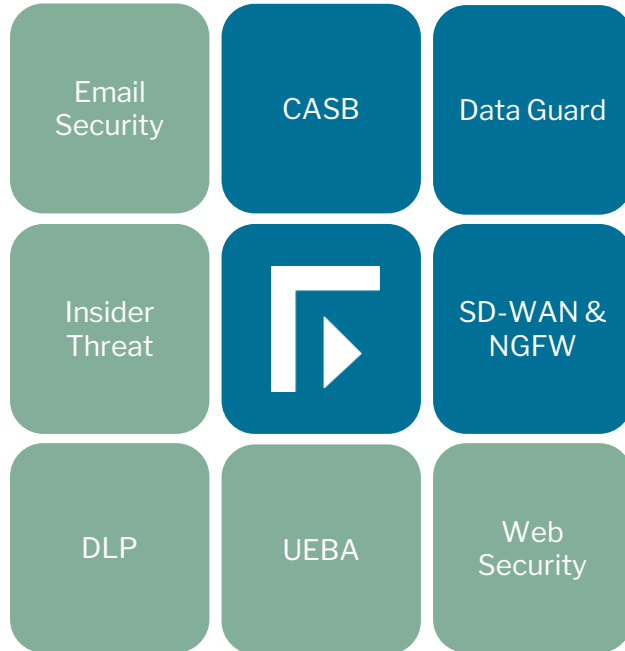
Time	Activity	User
14:33:07	User is using Skype	user04
14:32:37	User is using Skype	user04
14:32:07	User is using Skype	user04
14:31:37	User is using Skype	user04
14:28:20	Blocked Web Content	user03
14:23:20	Blocked Web Content	user03
14:14:29	User is using obsoleted web browser	user03
14:13:59	User is using obsoleted web browser	user03
14:13:29	User is using obsoleted web browser	user03
14:11:40	Blocked Web Content	user02

Identity and contact information from Active Directory

Detailed endpoint information from Forcepoint ECA



Forcepoint Security Portfolio for Healthcare



OUR VISION

Understand and respond to user intent to stop cybercrime before it occurs

Forcepoint Approach to Data Protection

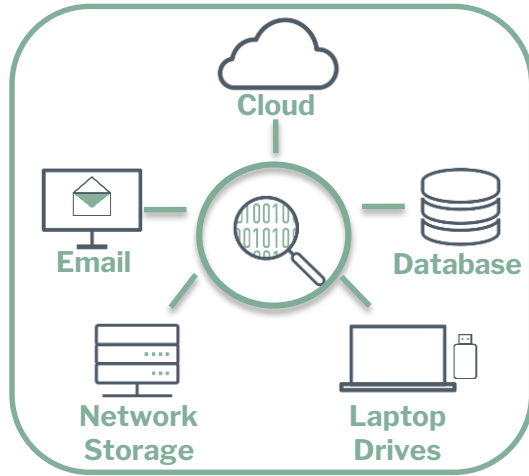


Single console management across all channels for optimal visibility and control

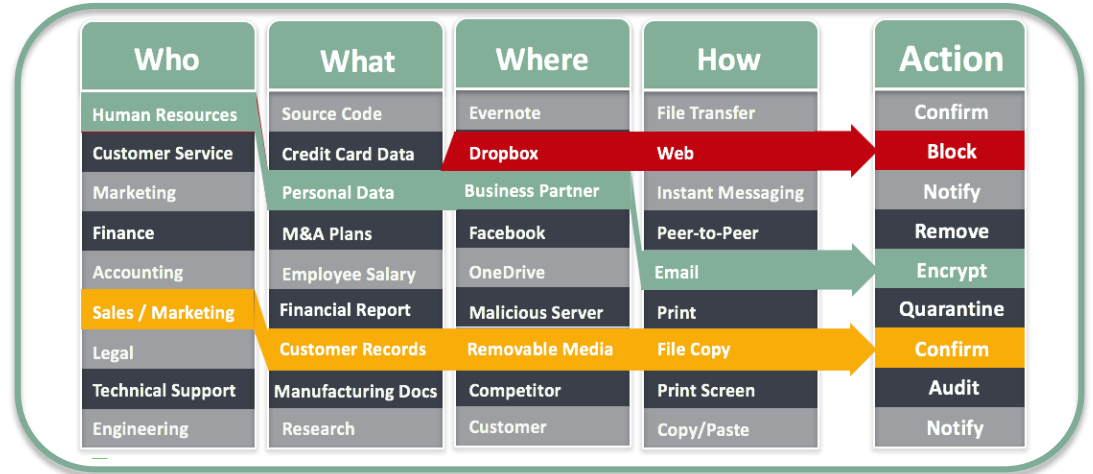


INVENTORY

Data Discover

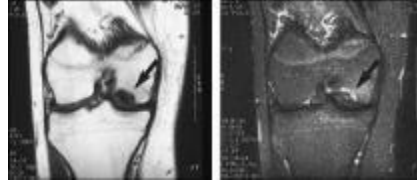


Map and Manage Personal Data Flows



Have clear visibility on your data and enforce end to end governance

DATA LEAKAGE PROTECTION EVOLUTION



2003

Data Fingerprints

Pre-defined IP and Compliance Policies

Endpoint fingerprints

2010

OCR and Cumulative (DRIP) DLP

Apple OS X DLP endpoint

2015

Insider Threat DLP Detection

Insider Threat

Incident Risk Ranking

2018

Dynamic Data Protection

DLP SECURES SENSITIVE DATA IN USE & IN MOTION

Who	What	Where	How	Action
Doctors	Source Code	Evernote	File Transfer	Confirm
Customer Service	Credit Card Data	Dropbox	Web	Block
Marketing	ePHI	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	Peer-to-Peer	Remove
Accounting	Employee Salary	OneDrive	Email	Encrypt
Sales / Marketing	Financial Report	Malicious Server	Print	Quarantine
Legal	Patient Records	Removable Media	File Copy	Confirm
Technical Support	Manufacturing Docs	Competitor	Print Screen	Audit
Engineering	Research	Customer	Copy/Paste	Notify

IP AND COMPLIANCE POLICIES

The image displays two screenshots of the 'Regulatory & Compliance Policy Wizard' interface. The first screenshot shows the 'Regions' step, where a list of geographical regions is presented. A green callout bubble with the text 'Select Region' points to the 'California' checkbox, which is checked and highlighted in yellow. The second screenshot shows the 'Industries' step, where a list of industry categories is presented. A green callout bubble with the text 'Select Industry' points to the 'Retail' checkbox, which is checked. The 'Public Company' checkbox at the bottom is also checked. The interface includes a breadcrumb trail at the top, a progress indicator with steps 'Welcome', 'Regions', 'Industries', and 'Finish', and navigation buttons like 'Cancel', '< Back', and 'Next >'.

DLP Policies > Manage Policies > Regulatory & Compliance Policy Wizard

Welcome > **Regions** > Industries > Finish

Select the geographical regions to include in your policy preferences:

- Africa
- APAC (Asia and Pacific)
- CALA (Central and Latin America)
- Canada
- Europe
- Middle East
- USA
 - Alaska
 - Arizona
 - Arkansas
 - California
 - Colorado
 - Connecticut
 - Delaware
 - District Of Colombia
 - Florida
 - Georgia
 - Hawaii
 - Idaho

Cancel

DLP Policies > Manage Policies > Regulatory & Compliance Policy Wizard

Welcome > Regions > **Industries** > Finish

Select the industries to include in your policy preferences:

- Educational
- Energy and Infrastructure
- Entertainment and Media
- Finance and Banking
- Government
- Hardware
- Healthcare and Pharma
- Insurance
- Manufacturer
- Retail
- Software
- Telco
- Transportation
- Other

Public Company

Cancel < Back Next >

IP AND COMPLIANCE POLICIES

Types of IP to secure

Common Healthcare Compliance & Regulations

Manage Policies > Data Loss Prevention Policy Templates

View Refresh

Select the regulatory & compliance policies to apply in your organization, then click Use Policies.
Highlight a policy and click Details to see details about it. You can show all or only commonly used policies.

Standard version: 7.7.0.74592
Custom version: 7.6.3.732815

Displaying policies from 5 industries in 49 regions Category: All categories

130 Policies: Search for:

Name	Category	Version
<input type="checkbox"/> c_Custom		
<input type="checkbox"/> Data Types		
<input type="checkbox"/> Acceptable Use		
<input type="checkbox"/> Company Confidential and Intellectual Property		
<input type="checkbox"/> Software Source Code and Design		
<input checked="" type="checkbox"/> Business and Technical Drawings Files	Company Confidential and intellectual property	733909
<input checked="" type="checkbox"/> Network Security Information	Company Confidential and intellectual property	733909
<input checked="" type="checkbox"/> Patents	Company Confidential and intellectual property	733909
<input type="checkbox"/> Strategic Business Documents	Company Confidential and intellectual property	733909
<input type="checkbox"/> Credit Cards		
<input type="checkbox"/> Financial Data		
<input type="checkbox"/> PHI: Protected Health Information		
<input type="checkbox"/> PII: Personally Identifiable Information		
<input checked="" type="checkbox"/> Regulations, Compliance and Standards		
<input type="checkbox"/> Financial Regulations		
<input type="checkbox"/> PCI		
<input checked="" type="checkbox"/> PCI	PCI DSS	733909
<input type="checkbox"/> PCI Audit	PCI DSS	733909
<input type="checkbox"/> Privacy Regulations		
<input type="checkbox"/> US and Canada Federal Regulations		

Policy: PCI

Description: Policy for promoting compliance with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an industry standard, accepted internationally by all major credit card issuers and is enforced on companies and organizations that accept credit card payments or process, store, or transmit cardholder data. The standard includes the mandate that credit card numbers and cardholder data should be highly secured and that transactions comprising PCI data should be encrypted.

Rules (enabled: 2, total: 4)

- 1. PCI: Credit-Card Numbers**
 - 1.1 PCI: Credit-Card Numbers (wide) (733909) - Disabled**
A permissive rule for detecting potential credit-card-numbers, based only on format and validation. This rule may cause false positives and is not selected by default.
 - 1.2 PCI: Credit-Card Numbers (default) (733909)**
Rule for detecting valid credit card numbers employing various heuristics involving credit card related terms and use of delimiters. By default, only the first 4 digits and the last 4 digits are shown in the reports. This rule is selected by default.
 - 1.3 PCI: Credit-Card Numbers (narrow) (733909) - Disabled**
A restricted rule for detecting credit card numbers, tuned in order to minimize false positives. This rule requires additional evidence, such as credit-card related terms in proximity, in order to qualify number as a credit-card number. The rule is not selected by default.
- 2. PCI: Credit Card Magnetic Strips (733909)**
Rule for detection of the strings encoded on 1st, 2nd and 3rd magnetic tracks of a credit card. The string encoded on the 1st magnetic track of a credit card contains the card number, and

NOTE: For a rule to take effect, you must enable it. To enable a rule, highlight it in the Policy Management tree view, select Edit, and click Enabled.

Legend:

- Unused policy
- Used policy
- Folder with no used policies
- Folder with used policies

Use Policies Cancel

Explanation

INTEGRATED DLP INCIDENT RISK RANKING

- DLP industry's first Security Analytics Capability
- Incidents are clustered together into Cases
 - A Case can be a single incident or series grouped together
 - Each case gets a risk score of 0-10
- Incident Risk Ranking allows you to see and react to the most urgent cases

The screenshot displays a web-based dashboard for 'Incident Risk Ranking - Top Cases'. The interface includes a navigation sidebar on the left with options like 'Main', 'Status', 'Reporting', 'Policy Management', 'Logs', and 'Settings'. The main content area shows a grid of incident cases, each with a risk score (e.g., 7.6, 7.5, 7.3, 6.8, 6.3) and a brief description. A detailed view of a case with a risk score of 9.1 is shown in the foreground, providing specific information about the incident.

9.1 Suspected data theft
15 Sep. 2016, 10:12 AM ID: 164150

Source: jdoe@mycompany.com
Destination: extemail@gmail.com
Files: visa-leak.txt (222.6KB)

1 incidents >

TRADITIONAL DATA LEAKAGE PROTECTION

STATIC POLICIES BASED ON PRE-DEFINED RULES



Kate is giving a presentation to senior leadership and tries to copy her slides to a USB stick

**Traditional
DLP Policy**

Policy: **block** files from being copied to USB drives, alert gets sent to IT

USER IMPACTS

Kate is frustrated because simple tasks are blocked

Kate will find another way to solve her problem

The data protection system becomes ineffective

ADMINISTRATOR IMPACTS

The admin needs to track down the alert

Thousands of alerts come in overwhelming the security admin team

The security team turns off the DLP policy because there are too many false positives

STATIC VS DYNAMIC POLICIES IN ACTION

ACTIONS VARY BASED ON THE RISK LEVEL OF PEOPLE AND THE VALUE OF DATA



Kate is giving a presentation to senior leadership and tries to copy her slides to a USB stick

Kate begins to bulk copy files to her local machine at off hours.

She gets a supplier's query about an order she doesn't remember placing and then logs into the supplier's website to check on it

Kate begins accessing highly sensitive drug formula data and attempts to copy it off the corporate network

High
Risk Group

Policy: **observe** Kate's every user & machine detail and **block** all data transfers or copies anywhere

Medium
Risk Group

Policy: Rather than just create an alert, take action and **notify** the administrator

Low
Risk Group

Policy: **encrypt** fingerprinted files to USB drives but allow others to be copied.

CLOUD ADOPTION OUTCOMES IMPORTANT TO OUR NHS CUSTOMER

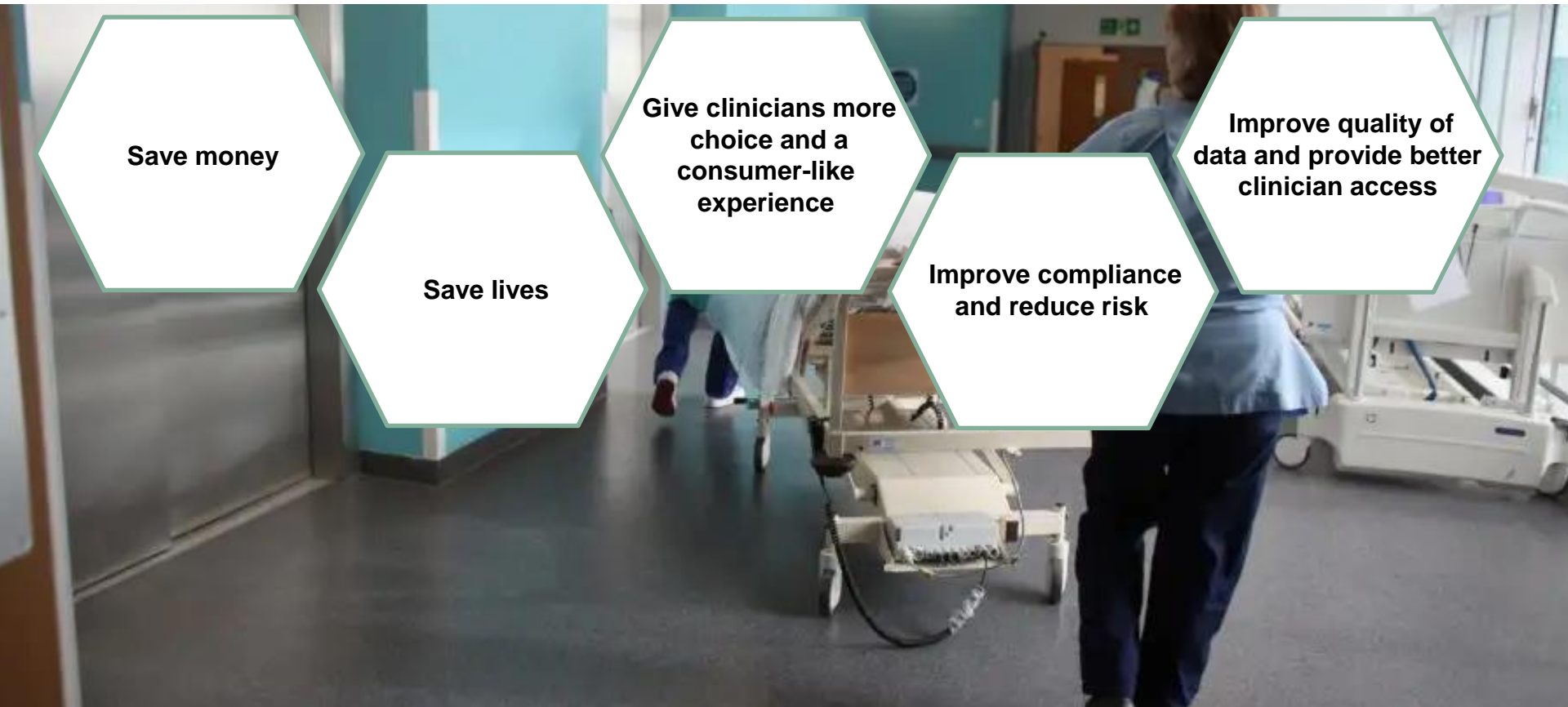
Save money

Save lives

Give clinicians more choice and a consumer-like experience

Improve compliance and reduce risk

Improve quality of data and provide better clinician access



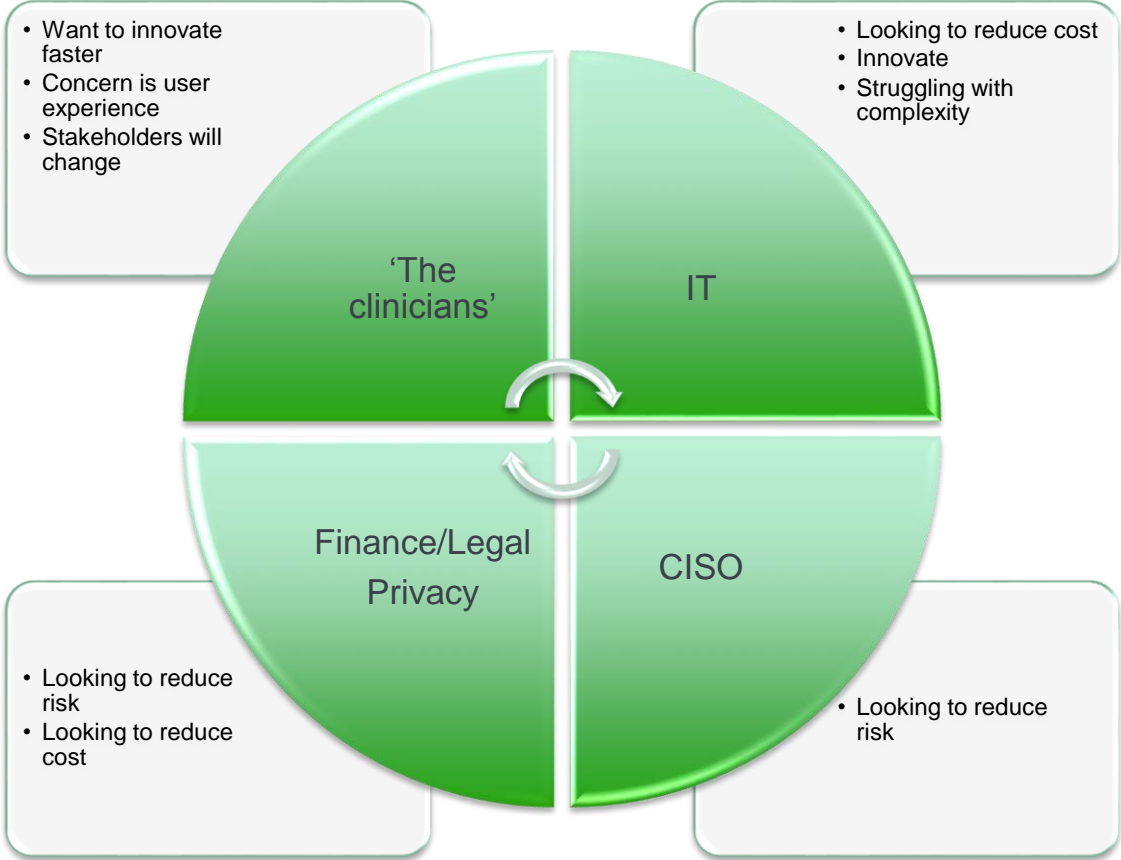
Forcepoint Security Portfolio for Healthcare



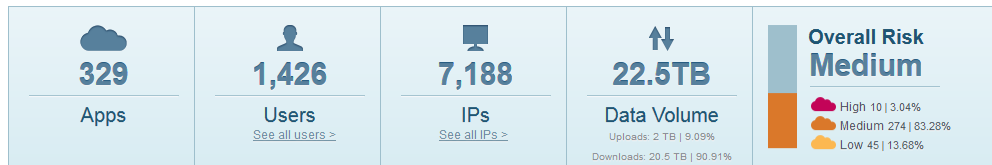
OUR VISION

Understand and respond to user intent to stop cybercrime before it occurs

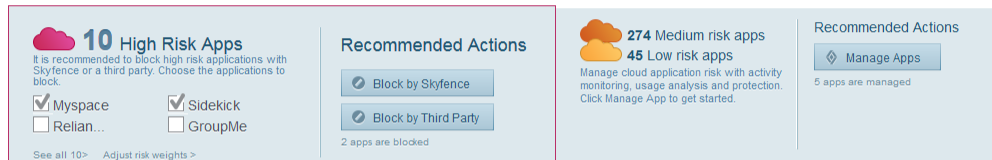
STEP 1: ASSEMBLE KEY STAKEHOLDERS



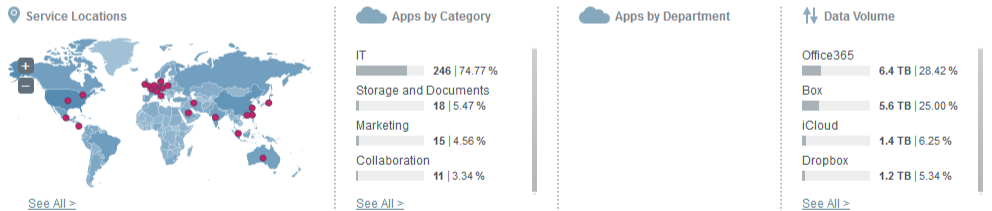
Step 2: GAIN CLOUD USAGE VISIBILITY



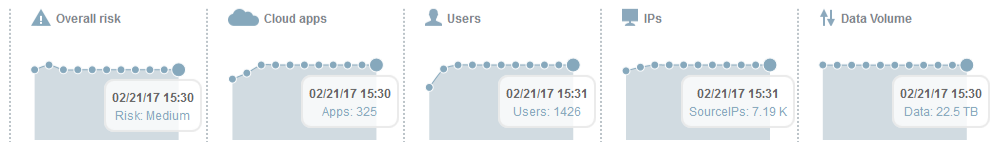
Recommended Actions







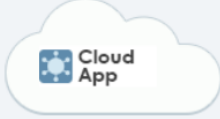

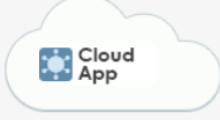

Analytics



Trends



STEP 2: GATHER THE SHADOW IT USAGE DATA





				Sort By ↓ Users ↓	
126 apps found		1-20 of 126 < >			
	Cloud9 IDE Discovered 08/31/18 10:00  Medium Risk	Category: Collaboration Description: Cloud9 IDE is a cloud-based Integrated Development Environment that enabl...	Users: 3,578 58.66% IPs: 5,779 44.81% Activities: 7,971,344 65.47% Data Volume: 1.1GB Uploads: 738.4MB 64.06% Downloads: 414.3MB 35.94% Last Seen: 09/04/18 02:38	Actions ↓ Application Details	
	Google Docs Discovered 08/31/18 10:13  Low Risk	Category: Collaboration Description: Google Docs is a text editor to create and format documents and work on t...	Users: 976 16.00% IPs: 866 6.71% Activities: 174,872 1.44% Data Volume: 4.9GB Uploads: 4.7GB 96.17% Downloads: 193MB 3.83% Last Seen: 09/04/18 02:35	Actions ↓ Application Details	
	GoToMeeting Discovered 08/09/18 05:07  Medium Risk	Category: Collaboration Description: GoToMeeting is a web-hosted service, online meeting, desktop sharing, and...	Users: 902 14.79% IPs: 4,774 37.02% Activities: 662,340 5.44% Data Volume: 25.4MB Uploads: 24.2MB 95.41% Downloads: 1.2MB 4.59% Last Seen: 08/09/18 06:02	Actions ↓ Application Details	
	JIRA Discovered 12/16/15 12:06  Medium Risk	Category: Collaboration Description: JIRA - provides bug tracking, issue tracking, and project management func...	Users: 882 14.46% IPs: 4,739 36.74% Activities: 671,376 5.51% Data Volume: 65.6GB Last Seen: 12/17/15 08:35	Actions ↓ Application Details	



STEP 3: MATCH CLOUD APP WITH CUSTOMISED RISK

FORCEPOINT Cloud App Directory [Learn about our cloud app control](#) [Can't find an App?](#) casb-emea


[Home](#) > Compare apps [Export to PDF](#)


Compare				
Title	Vivocha	GoToMeeting	Atlassian	Google Docs
Category	COLLABORATION	COLLABORATION	IT	COLLABORATION
Risk Level	Medium Risk	Medium Risk	Medium Risk	Low Risk
Description	Vivocha is a cloud service that enables businesses to seamlessly communicate with customers right on the website, using any combination of VoIP, chat, callbacks and collaboration tools like assisted browsing and form sharing.	GoToMeeting is a web-hosted service, online meeting, desktop sharing, and video conferencing software that enables the user to meet with other computer users, customers, clients or colleagues via the Internet in real time.	Atlassian is a provider of collaboration, development, and issue tracking software for teams.	Google Docs is a text editor to create and format documents and work on them together with other users.
Website	http://www.vivocha.com	http://gotomeeting.com	http://atlassian.com	http://docs.google.com
Provider	Vivocha, Inc.	Citrix Systems, Inc.	Atlassian	Google Inc.
Location	One Market Plaza Steuart Tower 5th Floor San Francisco, CA 94105 USA	7414 Hollister Ave Goleta, CA 93117, USA	Level 6, 341 George St Sydney, NSW, 2000, Australia	1600 Amphitheatre Parkway, Mountain View, CA 94043, United States
v Compliance				
v Security Settings				
v General Information				



STEP 4: GO ASK THE USERS ABOUT THEIR USE

93 Users (on Vivocha) ✕



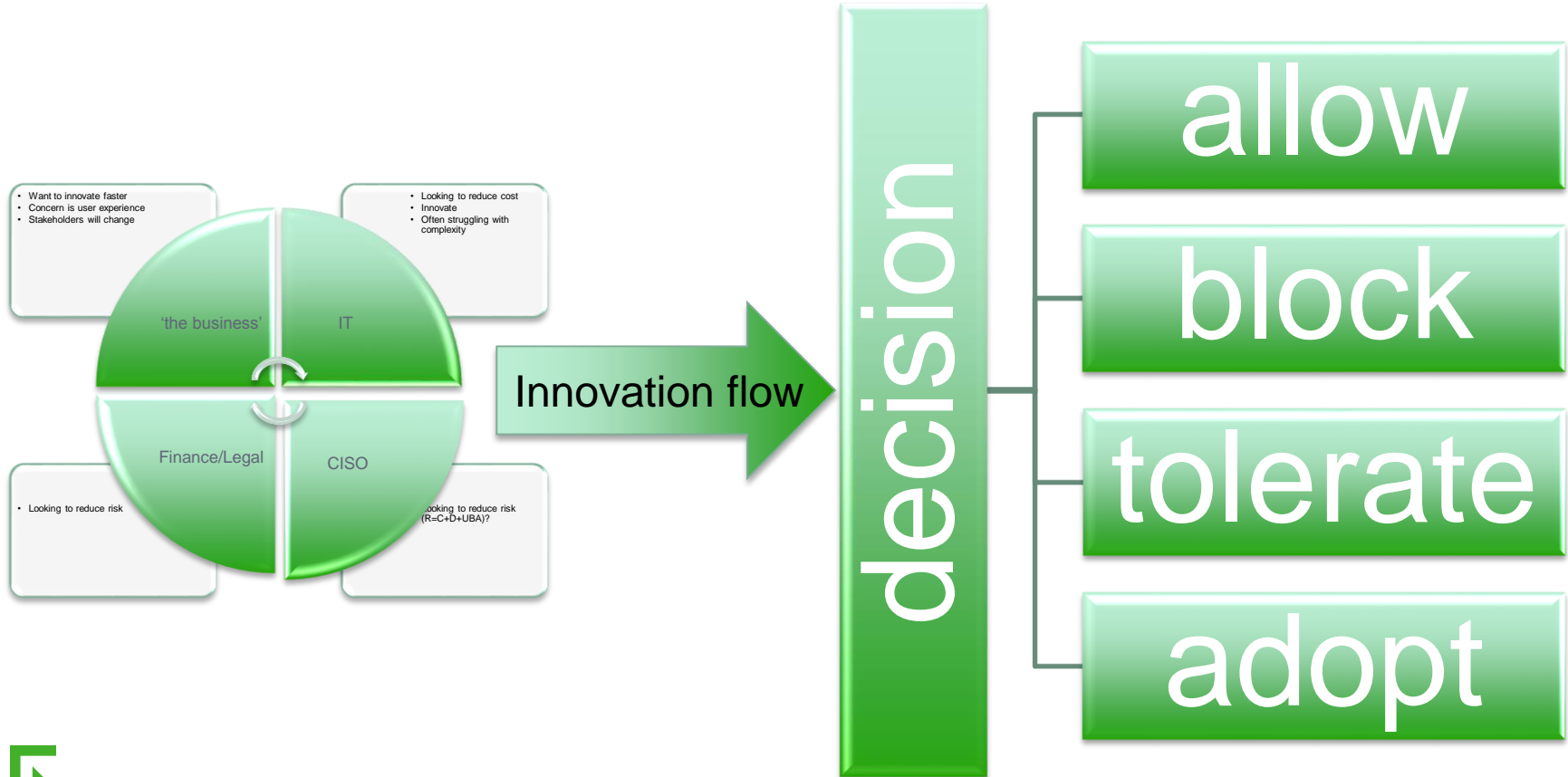
Sort By ↓ Data Volume 

93 items listed 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | >

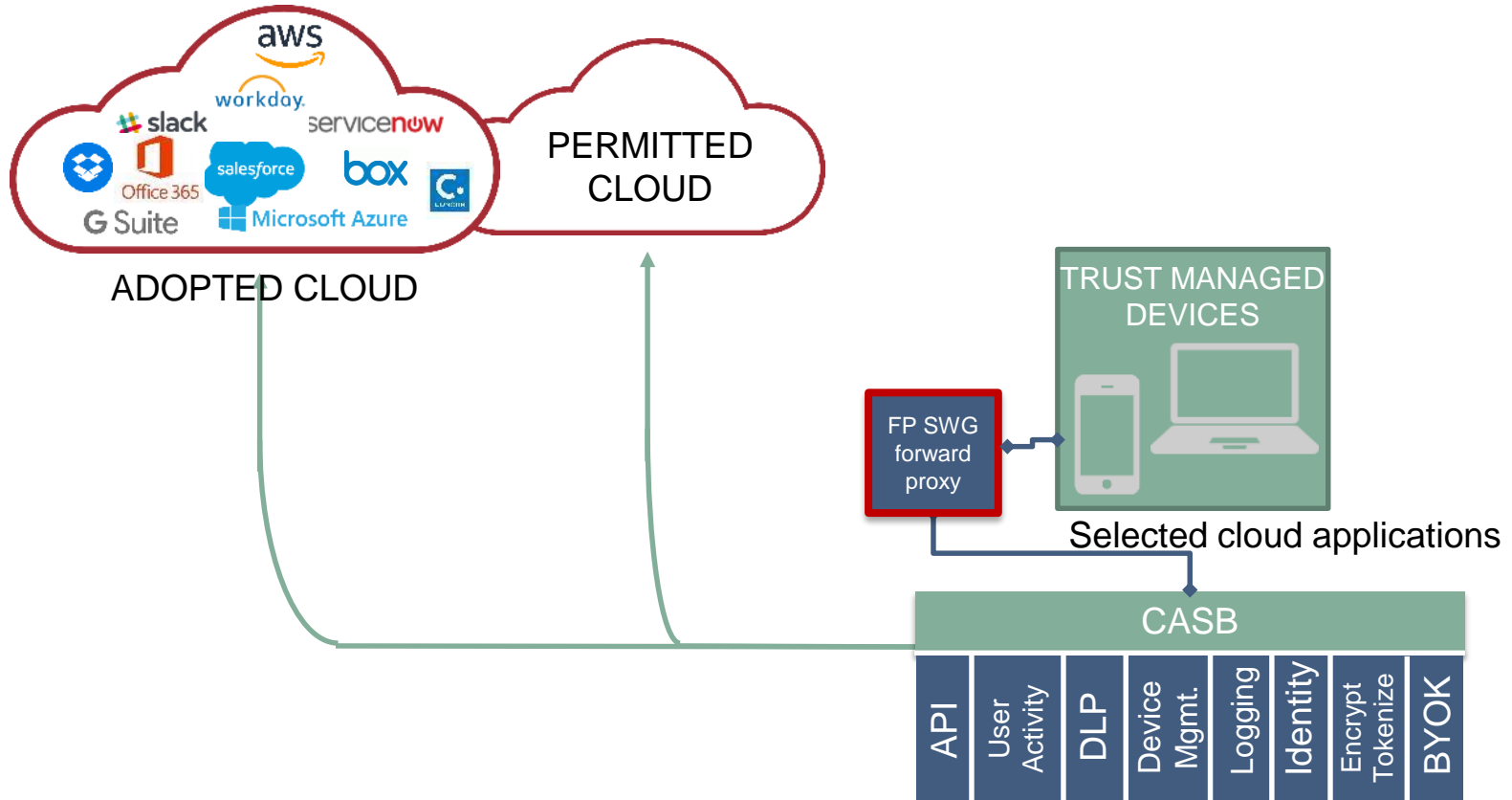
Username	Full Name	Last Access	Department	Title	Admin	Email	Activities	Data Volume	Uploads	Downloads
Nanni St...		04/20/18 08:35			User		505	14.7MB	13MB	1.7MB
Caponigr...		04/19/18 14:44			User		99	2.5MB	1.3MB	1.1MB
Sarti Ma...		04/17/18 18:08			User		28	1.7MB	1.2MB	471.9KB
Kamagaew...		04/18/18 14:18			User		260	886.8KB	680.5KB	206.3KB
Tiozzo L...		04/18/18 16:26			User		31	779.5KB	544.9KB	234.7KB
Melli Ma...		04/18/18 11:37			User		56	768.2KB	640.7KB	127.5KB
Sgarzi L...		04/20/18 11:04			User		70	521.4KB	443.4KB	78.1KB
Kohut Je...		04/12/18 10:18			User		26	451KB	388.2KB	62.7KB
Flori Se...		04/16/18 10:56			User		8	419.2KB	252.8KB	166.3KB
Orlandi ...		04/12/18 12:02			User		18	367KB	336.6KB	30.4KB



STEP 5: CLOUD GOVERNANCE TEAM TO DECIDE



REDUCING THE RISK OF CLINICIANS 'SHADOW IT'



O365 PROJECT: WHAT DID THE STAKEHOLDERS WANT

"I need to prevent malware attacks using O365"

"I need to control Privileged users such as Admins"

"I need to give clinicians unmanaged device access"

"I need to stop outsiders accessing our cloud assets"

"I need to provide safe cloud file sharing and collaboration"

I'm the CISO

I manage network

I'm a clinician and I just want to get my job done



Forcepoint Solutions Help Organizations Accelerate Digital Transformation

Transforming Networks

Enable Direct-to-Cloud Connectivity and Security for Remote Offices

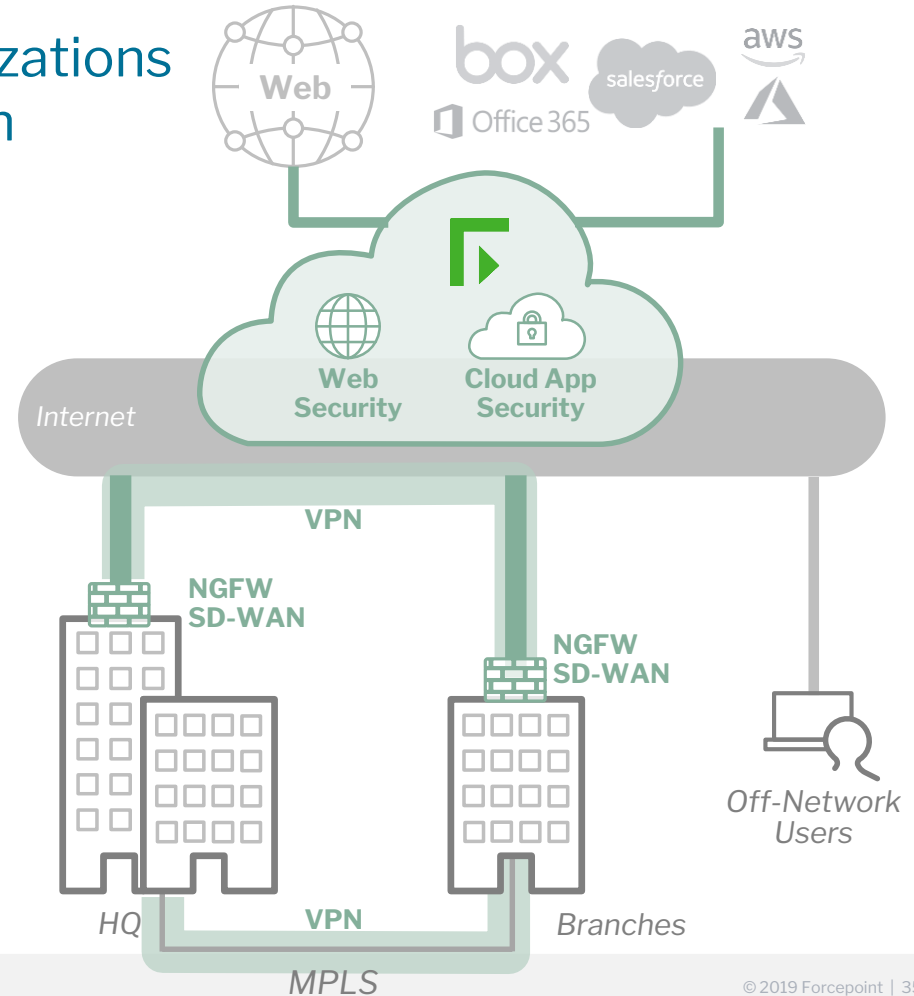
Modernize Hybrid IT Networks

Transforming Security

Secure the Adoption of SaaS and Public Clouds

Protect Off-Network Users

Deploy a Converged Security from the Cloud



Full Visibility into SD-WAN Connections

SMC - Store 100 NGFW
SEARCH (Ctrl+F)
FORCEPOINT
NGFW Security Management Center

Store 100 NGFW

NGFW Engines

SD-WAN

Filter

- Branches (21)
- DC-1 Helsinki NGFW
- DC-2 Saint Paul NGFW
- DC-3 Plano NGFW
- DC-4 Santa Clara NGFW
- NSX-Server 1-Virtual NGFW
- NSX-Server 2-Virtual NGFW
- Store 100 NGFW
- Store 101 NGFW
- Store 102 NGFW
- Store 103 NGFW
- Store 104 NGFW
- Store 105 NGFW
- Store 106 NGFW
- Store 107 NGFW
- Store 108 NGFW
- Store 109 NGFW
- Store 110 NGFW
- Store 111 NGFW
- Store 112 NGFW
- Store 113 NGFW
- Store 114 NGFW
- Route-Based VPN Tunnels (1)

26 rows

Users

Others

Store 100 NGFW
Edit

ISP Information

Store 100 - Verizon

23% **19%**

INBOUND TRAFFIC OUTBOUND TRAFFIC

11.53 Mbit/s 9.81 Mbit/s

72 821 Connections

Store 100 - Comcast

28% **21%**

INBOUND TRAFFIC OUTBOUND TRAFFIC

14.03 Mbit/s 10.82 Mbit/s

21 184 Connections

Store 100 - AT&T

15% **21%**

INBOUND TRAFFIC OUTBOUND TRAFFIC

7.83 Mbit/s 10.85 Mbit/s

95 911 Connections

Top Applications by ISP - 1 hour

Facebook	3.60 Mb (10.8%)
LinkedIn	3.47 Mb (10.4%)
Gmail	3.33 Mb (10.0%)
YouTube	3.11 Mb (9.3%)
BitTorrent	2.78 Mb (8.3%)
Twitter	2.76 Mb (8.3%)
Salesforce.com	2.26 Mb (6.8%)
GoToMeeting	2.15 Mb (6.4%)
Dropbox	2.10 Mb (6.3%)
Hulu	1.89 Mb (5.6%)

Tunnels

VPN	Branch A	Endpoint A	Branch B	Endpoint B	Status	Health	Traffic	Packet Loss	Latency	Jitter
▼ DC-1 Helsinki NGFW-Store 100 NGFW										
Store VPN	DC-1 Helsinki ...	10.1.1.254	Store 100 NGFW	10.1.9.254	Idle	87%	8.04 Mbit/s	7.91%	419 ms	55 ms
Store VPN	DC-1 Helsinki ...	10.1.1.254	Store 100 NGFW	172.31.9.254	Idle	90%	9.65 Mbit/s	6.64%	478 ms	54 ms
Store VPN	DC-1 Helsinki ...	10.1.1.254	Store 100 NGFW	192.168.9.254	Idle	89%	9.42 Mbit/s	8.48%	435 ms	51 ms
Store VPN	DC-1 Helsinki ...	172.16.12.41	Store 100 NGFW	10.1.9.254	Idle	68%	8.59 Mbit/s	7.59%	444 ms	50 ms
Store VPN	DC-1 Helsinki ...	172.16.12.41	Store 100 NGFW	172.31.9.254	Idle	82%	10.25 Mbit/s	8.49%	371 ms	47 ms
Store VPN	DC-1 Helsinki ...	172.16.12.41	Store 100 NGFW	192.168.9.254	Idle	93%	7.56 Mbit/s	8.4%	462 ms	55 ms
Store VPN	DC-1 Helsinki ...	172.31.1.254	Store 100 NGFW	10.1.9.254	Idle	80%	6.79 Mbit/s	9.86%	342 ms	31 ms
Store VPN	DC-1 Helsinki ...	172.31.1.254	Store 100 NGFW	172.31.9.254	Idle	91%	7.68 Mbit/s	7.8%	461 ms	27 ms
Store VPN	DC-1 Helsinki ...	172.31.1.254	Store 100 NGFW	192.168.9.254	Idle	91%	10.28 Mbit/s	8.02%	213 ms	35 ms
▶ Store 100 NGFW-DC-4 Santa Clara NGFW										
					Idle	74%				

Ready
john@127.0.0.1
Default

The top 5 O365 problems THAT FORCEPOINT CASB solves out of the box

Users **oversharing data** in OneDrive

Employees and 3rd-parties accessing Office365 from **BYOD** devices

Attackers stealing credentials and **weak O365 security policy** e.g. long password reset time

Discovery and control of Personal Data in O365 for **GDPR** purposes

Audit and control inappropriate **Admin** actions

EXAMPLE OUT OF

Disable Office 365 se

Office 365 advanced security n
beh

Malicious or Compro

Rules in this
malicious au

Settings

Ad

Privi
indic



! Asset governance API / Web connection is not configured. [Configure asset conne](#)

User Risk Dashboard > Data Classification Dashboard > Governance Policies

Governance Policies

Account lockout

The time that the user account is locked before automatic release

30 minutes

i Relevant section in active policy

Relevant sections in ISO 27002/27018:
9.3.1 Use of secret authentication information

Implementation guidelines:
When passwords are used as secret authentication

Password expiration

Maximum password age. 0 means that the password never expires

90 days

i Relevant section in active policy

Relevant sections in ISO 27002/27018:
9.3.1 Use of secret authentication information

Implementation guidelines:
When passwords are used as secret authentication

Ransom

Renaming of several files wi
modification.

Dashboard

Policies



Encryption Broker >



Predefined Policies

CJIS - Criminal Justice Information Services

CSA - CCM v3.0.1

HIPAA

ISO 27002/27018

MONETARY AUTHORITY OF SINGAPORE-TRMG

NIST 800-53 R4

PCI DSS V3.01

Custom Policies

mjt-pci-clone

tion settings that must be in place in
ents.

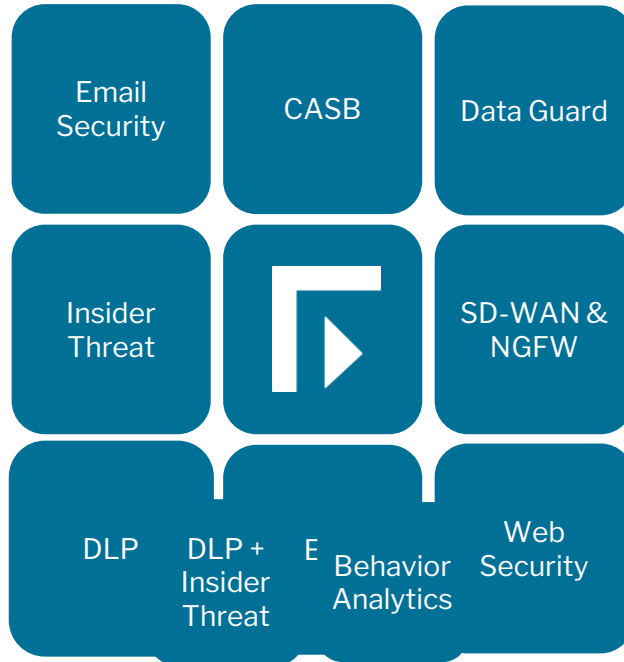
Human Point System is Here Today



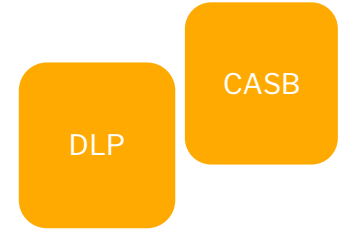
Add critical data & IP exfiltration protection to web and email security



Integrate SaaS visibility into core Web Security



More robust detection of anomalous activity



Uniform means to protect data on-premises & cloud



Enable Secure Cloud Adoption



Thank you...

ozgur.danisman@forcepoint.com

