



USER ACTIVITY MANAGEMENT

Chris Forgan

Sales Director EMEA

Mission

- Provide complete visibility into all user network activity

Financial and Strategic Advisors

- Mohr Davidow Ventures
- Intel Capital

Accomplishments

- Broad customer adoption
- Track record of growth
- Industry recognition
 - Gartner “Top 10 Strategic Technologies for 2010”
 - Gartner 2009 Cool Vendor
 - Frost & Sullivan



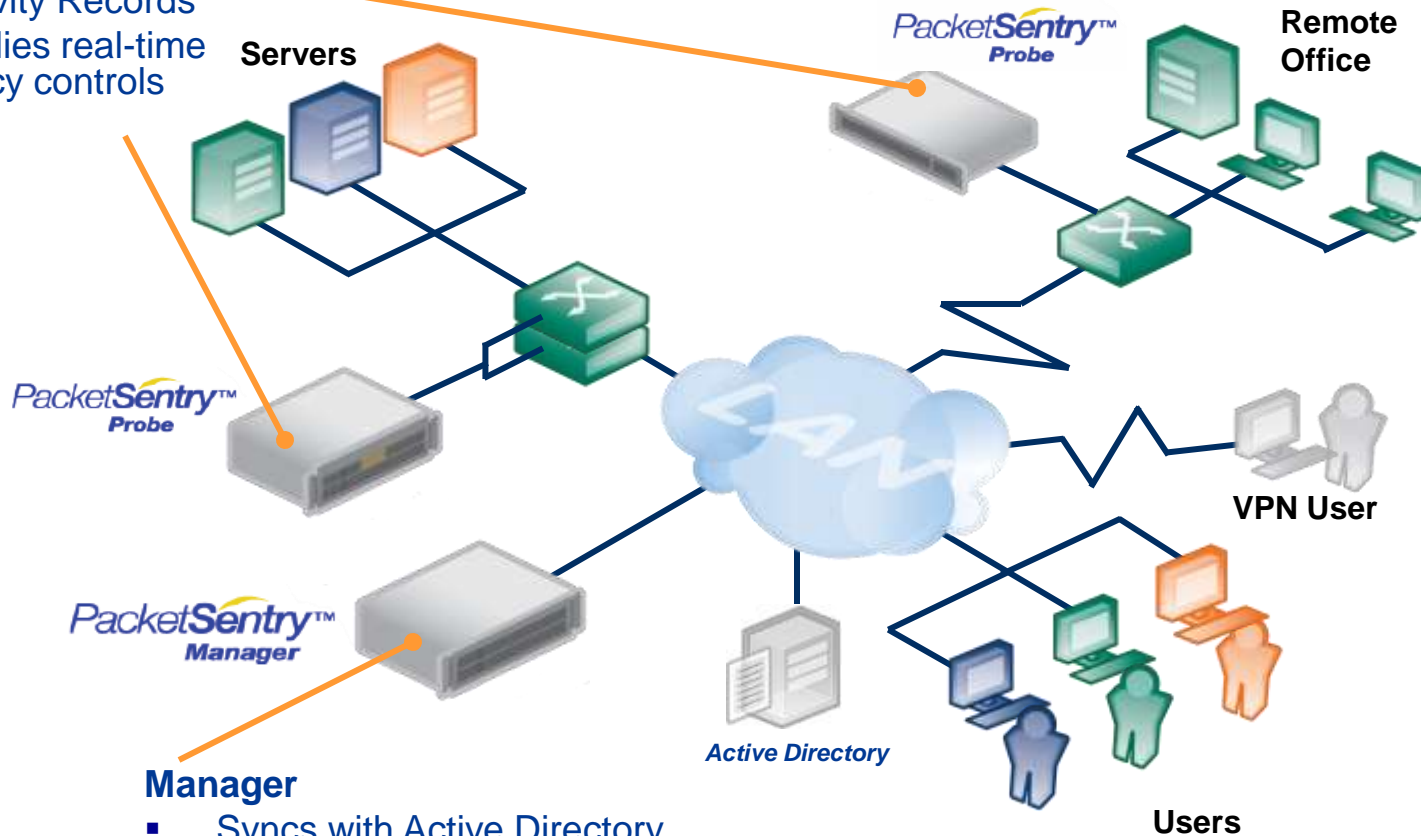
Commonly Implemented Use Cases:

- ❑ Compliance & Audit Controls and Reporting
- ❑ Virtual Segmentation
- ❑ Protection of Sensitive Data
- ❑ Monitoring & Controlling IT Administrators
- ❑ Fraud Detection
- ❑ Controlling 3rd Party Remote Access
- ❑ Sensitive Data Identification
- ❑ Change Management
- ❑ Security Investigations
- ❑ Data Leakage Prevention
- ❑ Platform Protection
- ❑ Network Utilization Visibility



Probes

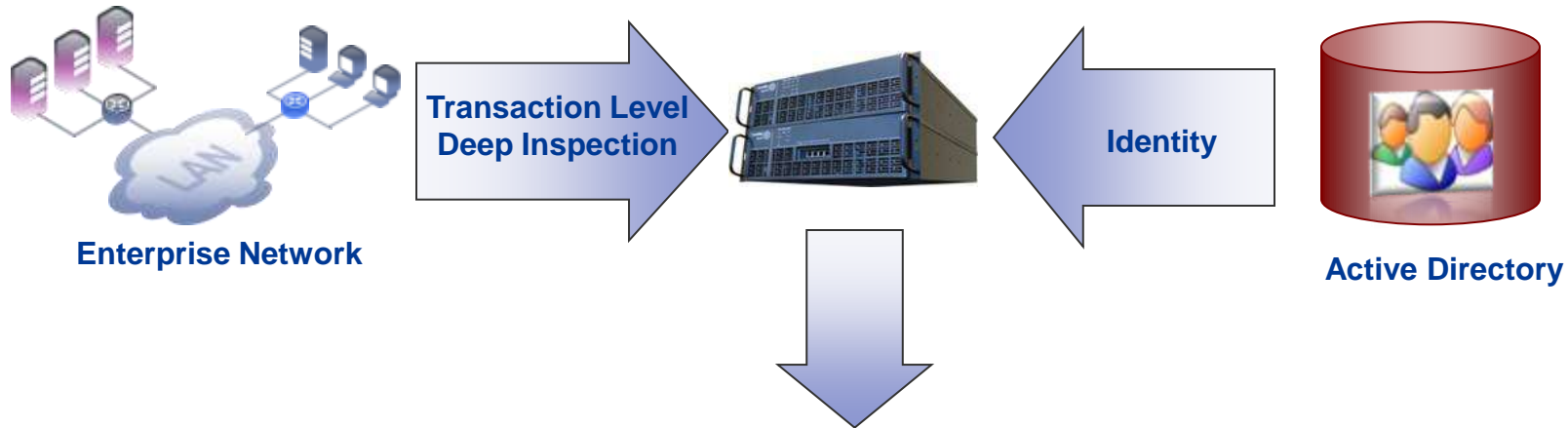
- Captures User Activity Records
- Applies real-time policy controls



Manager

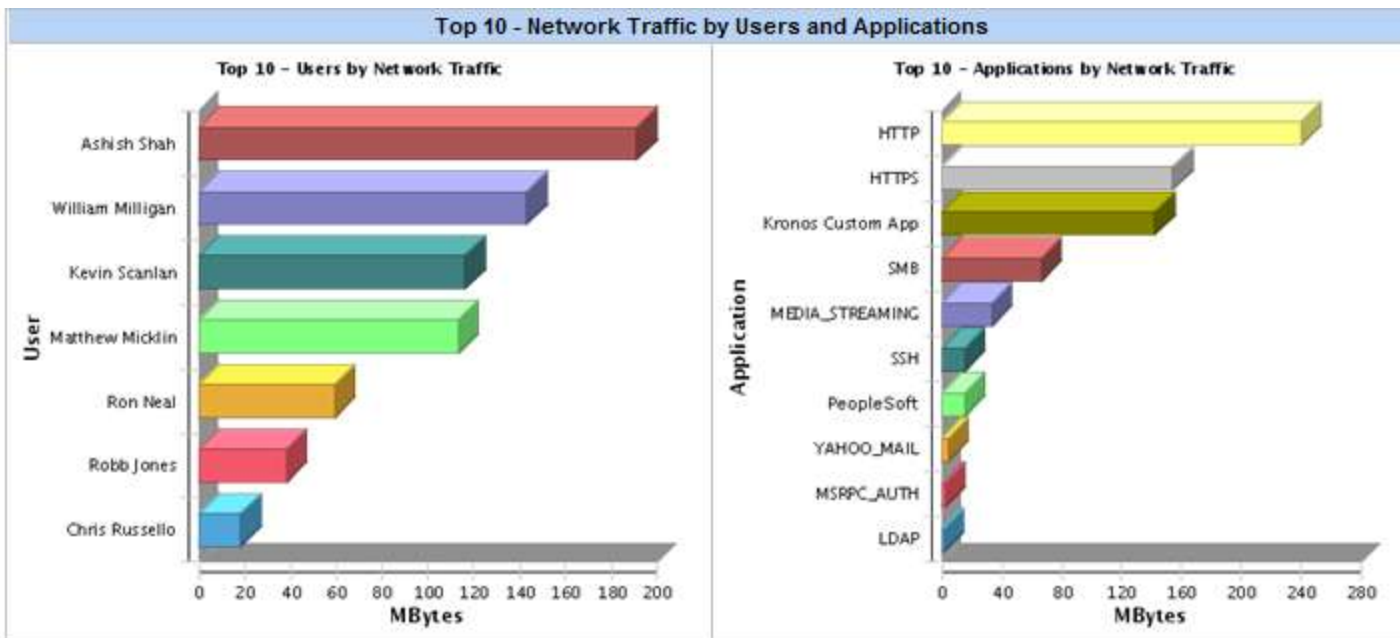
- Syncs with Active Directory
- Collects User Activity Records from probes
- Provides reports, full-text search, rules via GUI

No agents and no in-line appliances



- 9:14 am **Jon White** logs in to Active Directory
- 9:30 am **Jon White** reads file **forecastQ1** in directory **\forecasts\2010** on server **finHost1**
- 10:02pm **Jon White** emails file **forecastQ1** to **jw@gmail.com** with subject “**Unreleased Guidance?!**”
- 10:15am **Jon White** browses **www.youtube.com**
- 1:21am **Jon White** copies all files from **\\salesServer\salesOperations\pendingQuotes** to his laptop
- 2:20am **Ed Cho** logs into Oracle server **patientRecords** as **SYS** via **VPN01**
- 3:02am **Ed Cho** leapfrogs from server **Fin001** to server **HR002** using **RDP**
- 3:27am **Ed Cho** deletes from **Oracle** table **patientData** with query “**DELETE from table...**”

“User Activity Records” Contain Precise Details of User Actions



Network Traffic for Users

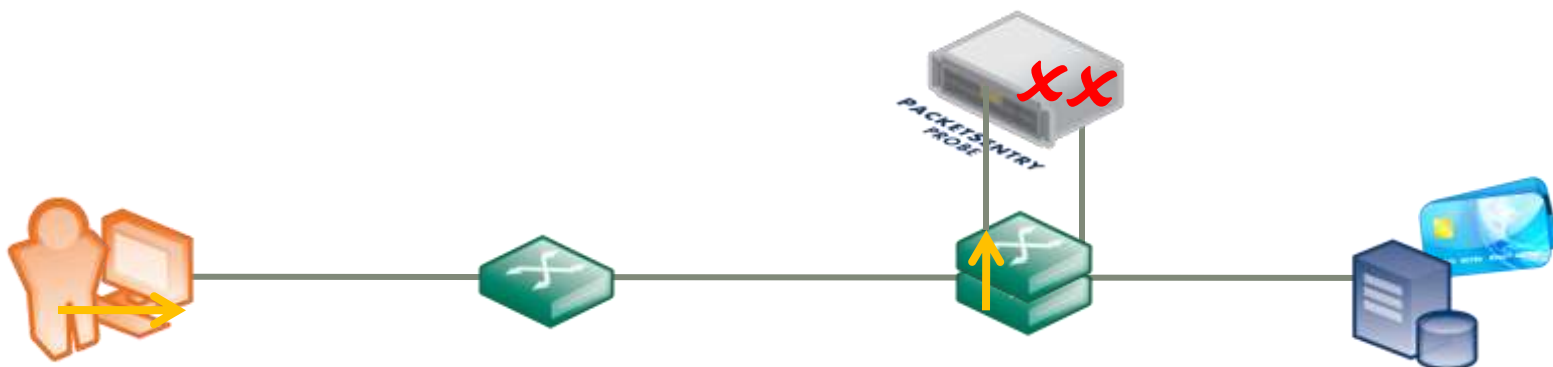
Account Id / User Name	Traffic (MB)	Top 10 Applications by Traffic		Top 10 Clients by Traffic		Top 10 Servers by Traffic	
		Application	MB	Client	MB	Server	MB
ashah / Ashish Shah	191	HTTPS	94	LT-ASHAH/172.16.2.20	154	PM-MGR-109/10.0.101.109	84
		Kronos Custom App	33	ENGG-0033/172.16.2.42	25	PMI00EXF01/172.16.1.45	33
		HTTP	32	172.16.2.20	11	PMI00FIL02/172.16.1.29	9
		SSH	15	172.16.2.19	0.115	PMI00SYM01/172.16.2.176	4
		SMB	10			74.125.19.136	3
		PeopleSoft	1			96.6.242.26	3
		MEDIA_STREAMING	1			63.169.44.100	2
		YAHOO_MAIL	0.882			PMI00DCS03/172.16.1.4	1
		KERBEROS	0.422			208.113.233.117	1
		YIM	0.311			216.115.220.254	1
wmilligan / William Milligan	143	HTTP	60	LT-WMILLIGAN/172.16.3.96	76	PMI00EXF01/172.16.1.45	37
		Kronos Custom App	37	172.16.2.31	40	65.54.87.173	30
		HTTPS	22	172.16.3.35	27	PM-MGR-109/10.0.101.109	22
		SMB	16	172.16.3.96	0.03	PMI00FIL02/172.16.1.29	15

4 Core Use Case for Global Organizations

- Internal Virtual Segmentation (Use Case 1)
 - PCI Credit Card Data
 - HR Data
 - Production vs. Development
 - Intellectual Property Data
 - HIPAA Data
 - Customer Data
 - Sales, Revenue, Expense, Data
- Offshore Privileged Users Data (Use Case 2)
 - Also Prevent Leap-Frogging
- Add Identity to Citrix Environments (Use Case 3)
- Fraud (File Share / DB Auditing) (Use Case 4)



Internal Virtual Network Segmentation



- Easily segment sensitive assets and user groups without spending \$\$\$\$ on internal firewalls
- Create identity-based policies to block all traffic that violate policy
- Immediately send connection resets (within 1 millisecond) to kill connections that break policy *as they are being set-up*
- Segment PCI assets, 3rd party VPN network access, financial and HR systems; anything subject to compliance regulations or fraud within the enterprise
- Adapts to rapidly changing business needs

Internal Virtual Network Segmentation Case Study

- Major Retailer
 - Fortune 25; \$50B+ revenue; thousands of stores; multiple divisions
- Solution Requirement
 - PCI DSS
 - Separate out ~100 credit card systems (mainly SQL Server) from rest of network in two data centers
- Competition: Firewalls, Database Agent
- Why PacketSentry?
 - Low risk, easy integration (two week evaluation period)
 - No agents, not in-line
 - Multi-level policies
 - If not in correct Active Directory group -> No Access
 - If DB admin account access not from correct AD group and location -> Alert
 - If in-scope systems transmit on “risky” ports - > Alert
 - Strategic value of solution beyond PCI
 - E.g. DB activity audit, Windows Server administrator auditing



Internal Virtual Network Segmentation Case Study

PacketSentry™

PCI-DSS 1.3 - Prohibit Unauthorized Access to Data

Audit all accesses and prevent any unauthorized access to sensitive PCI data

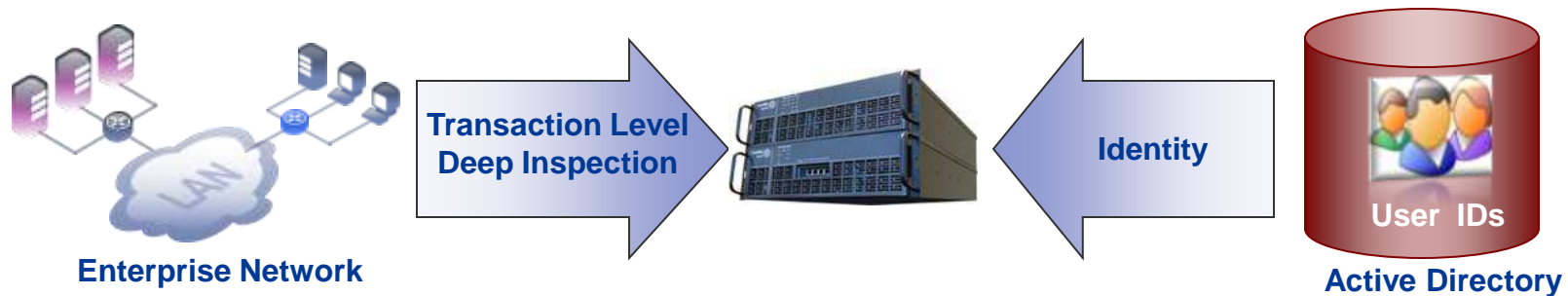
PCI Related Rules Information

#	Rule Name	Status	Last Changed By	OU/Group/User	Application	Action	Source Custom Group of IP	Destination Custom Group of IP	Severity	Email	Enforce	Last Violation On
1	No FTP on PCI-Hosts	Active	PSADMIN		FTP			PCI-DB-Host-Group	Critical	YES	YES	JUN 20, 2008 08:29 AM
2	PCI CardHolder Data Access	Active	PSADMIN	NOT PCI-Authorized-Users				PCI-Servers	Critical	YES	YES	JUL 28, 2009 04:19 PM
3	PCI DSS 1.3 - Limited Access	Active	PSADMIN	PCI-Authorized-Users		FILE DELETE		PCI-Servers	Minor	YES	YES	JUL 24, 2009 04:03 PM

Rules Violation Information

#	Severity	Rule Name	Timestamp	Server Host/IP	Asset Name	Asset Type	Application	Action	Client Host/IP	User
1	N/A	PCI CardHolder Data Access	JUL 27, 2009 05:52 PM	PMI00FIL02/172.16.1.29	WPMI00FIL02 \\PUBLIC\SE\CardHolder-Data\Credit Card Transactions\test	File	SMB	FILE OPEN	LT-ASHAH/172.16.2.10	Ashish Shah
2	Critical	PCI CardHolder Data Access	JUL 28, 2009 04:19 PM	PMI00FIL02/172.16.1.29	WPMI00FIL02 \\PUBLIC\SE\CardHolder-Data\CustomerPAN.xls	File	SMB	FILE READ	LT-ASHAH/172.16.5.59	Ashish Shah
3	Critical	PCI	JUL 28, 2009	PMI00FIL02/172.16.1.29	WPMI00FIL02	File	SMB	FILE	LT-	Ashish Shah

Offshore Privileged Users (without Logging)



- Complements SIEM solutions by providing complete visibility in to every type of user including offshore privileged users
 - Doesn't collect logs
- Tracks all user activity into databases, applications, servers, intellectual property
 - Independent audit trail
 - Deep Packet Inspection and Identity correlation
 - Doesn't require in-line appliances or agents
- Delivers comprehensive alerts and reports on user activity
 - Email activity, "access denied/failed logins", improper access attempts, baseline and threshold reports, whitelist exception reporting
- Protects against insider data breaches and non-compliance



Offshore Privileged User Case Study

- Financial Services
 - Top 10 Bank world-wide; 437 domestic and 15 overseas branches; 22,000+ employees
- Solution Requirement
 - Needed visibility into developer activities in Brazil, Russia, India and China. SIEM solution was in place to monitor and log activities, but couldn't be turned on to log offshore users who remained invisible.
- Competition
 - SIEM
- Why PacketSentry
 - Comprehensive audit trail of developer activity world-wide
 - Real-time enforcement controls to limit use of admin accounts to authorized staff, and to alert or block attempts to access sensitive data
 - “Leapfrogging” reports and real-time controls to detect or prohibit developers from using the systems they support as launch points for unauthorized activity.
 - Detection of unauthorized admin account sharing



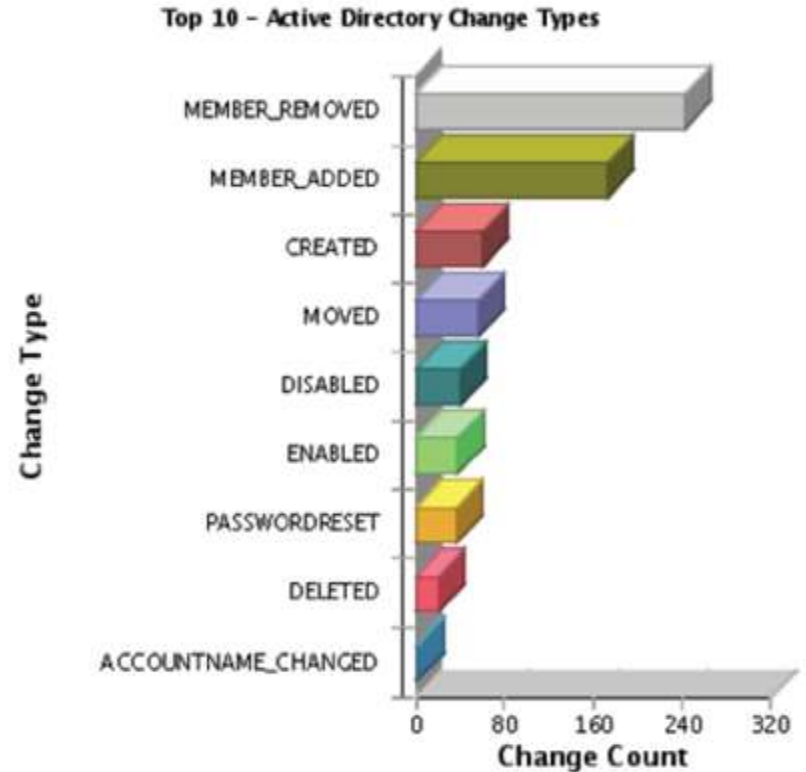
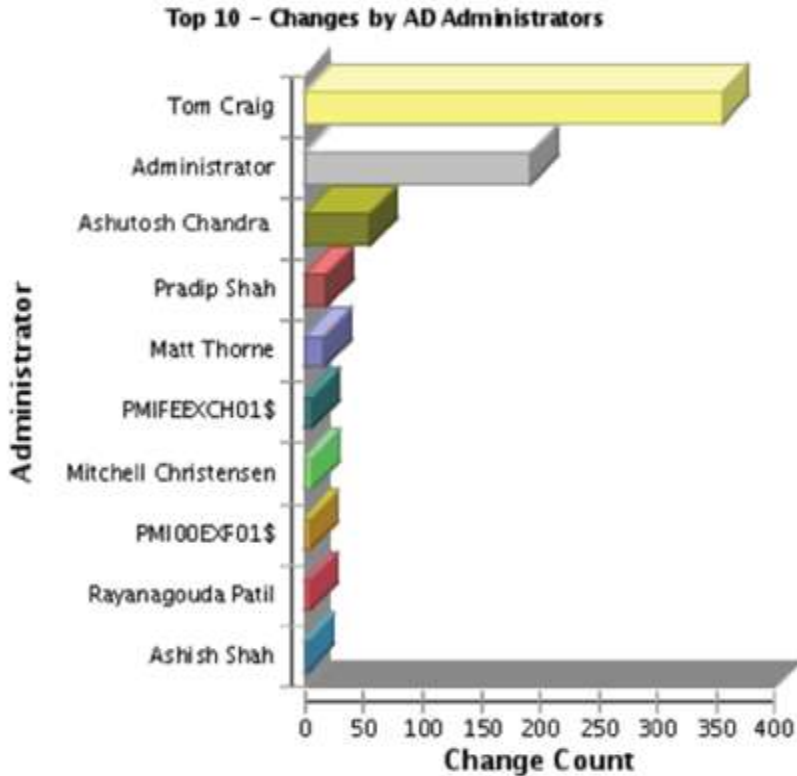
Offshore Privileged User Case Study



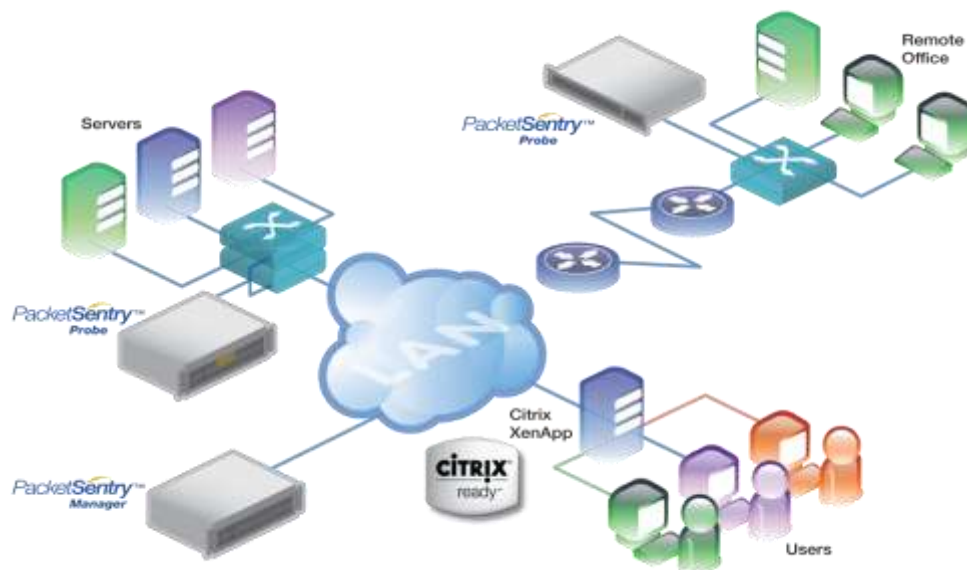
Report Changes to Users and Groups in Active Directory

Alert on any changes made by the Domain Admin group

Top 10 - Active Directory Changes by Administrators and Change Type



Monitor and Identify all User Traffic Including Citrix



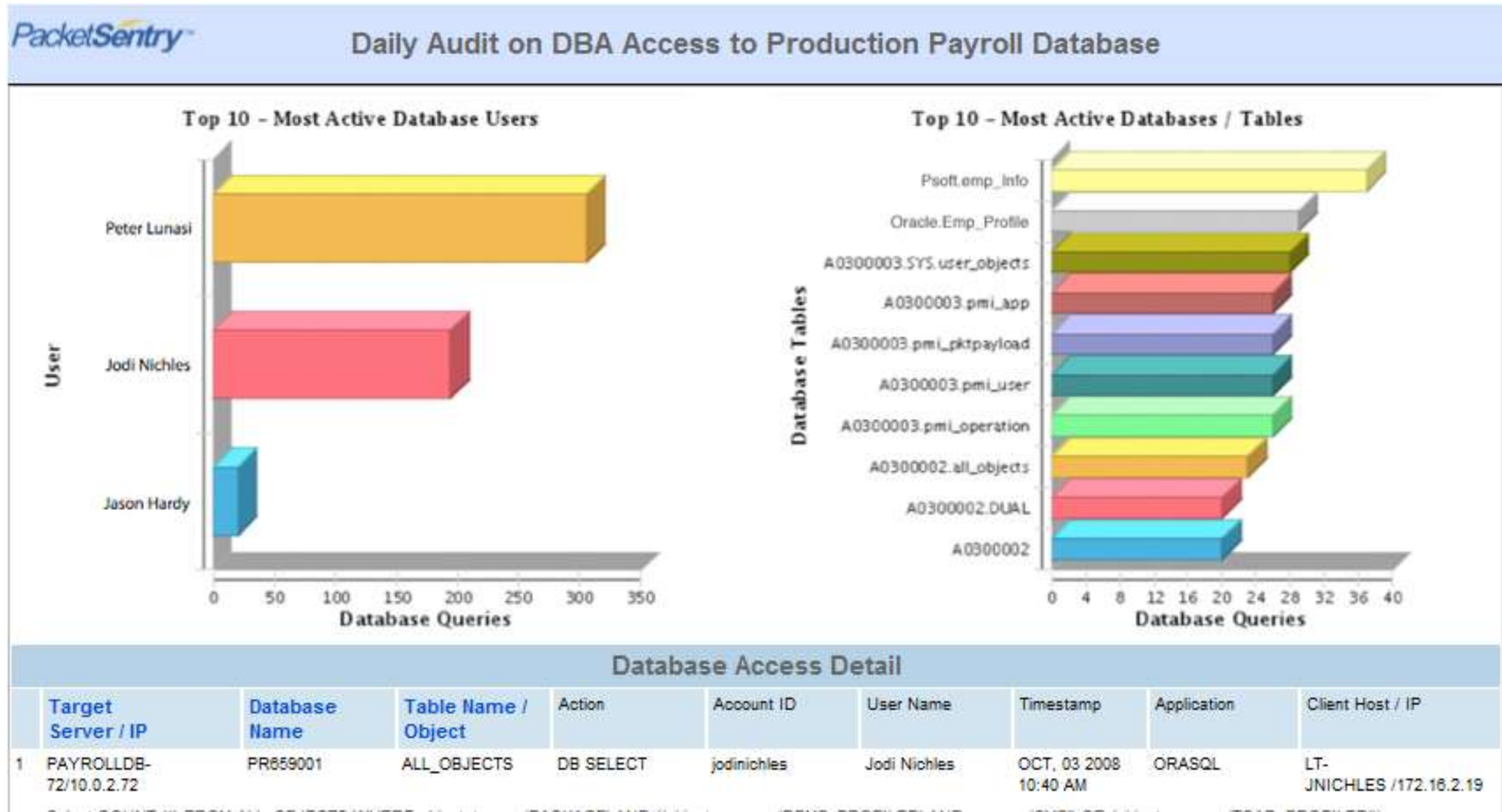
- Provides enterprise visibility of all Citrix activity based on each user's identity
- Proactively detects and blocks user activity and behavior that violates compliance regulations or company policy
- Detailed audit trail
- Tracks sensitive data access and movement
- Automates audit, investigation, and compliance reporting

Citrix User Activity Management Case Study

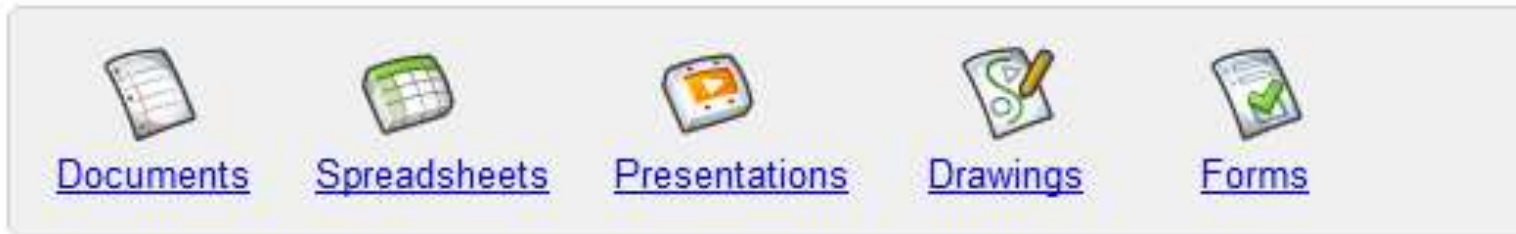
- Pharmaceutical
 - Forbes 1000 (\$14+B Revenue) Global Manufacturer
- Customer Services Agents Working From Home
 - Citrix Server 100.1.3.121
 - Needed Identity Assignment
- Competition
 - Do Nothing
- Why PacketSentry?
 - Low risk, easy integration
 - Small Agent on XenApp Server
 - Not in-line
 - Windows Server administrator auditing
 - Comprehensive Reports
 - Block Unauthorized Access



Citrix User Activity Management Case Study



File Share Activity Monitoring



The main reasons why PacketSentry is often selected are:

- No agents on servers; no use of FPolicy API on NetApp appliances
- Much broader coverage for employee activity (databases, email, etc).
- Simple licensing model

File Share Auditing Case Study

- Technology
 - Fortune 100 (not Apple); Brand Name Global IT Manufacturer
 - Concern – Data Mobility
- Multi-Platform Auditing
 - No Agents
 - Includes Mainframe Support
- Competition
 - Varonis
- Why PacketSentry?
 - Low risk, easy integration
 - No agents on servers
 - No use of FPolicy API on NetApp
 - Much broader coverage
 - Employee activity (databases, email, etc).
 - Simpler licensing model



All About The Data

File Share Auditing Sample Report



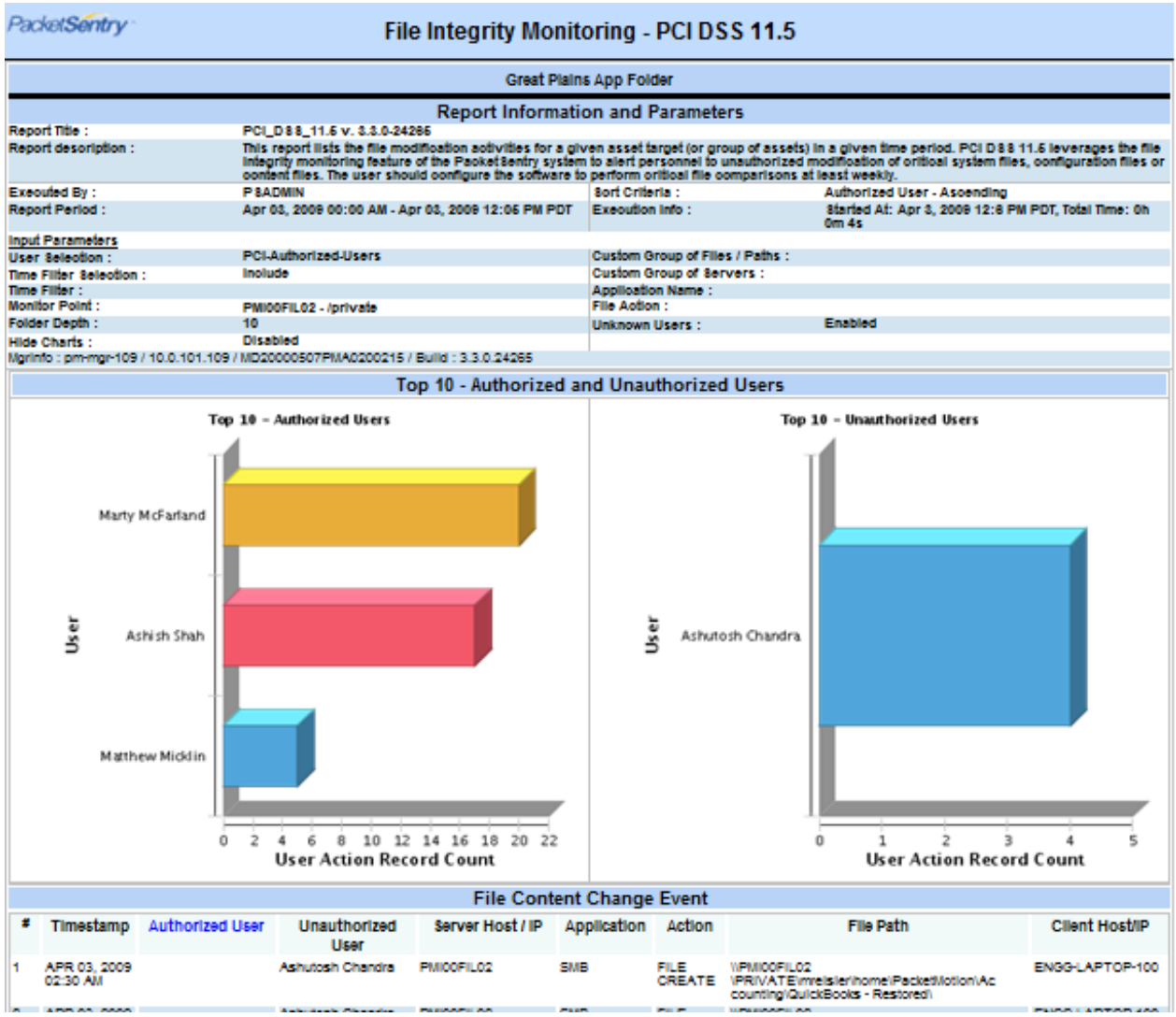
Email File Attachment Report

Terminated Employees: Engineering Group

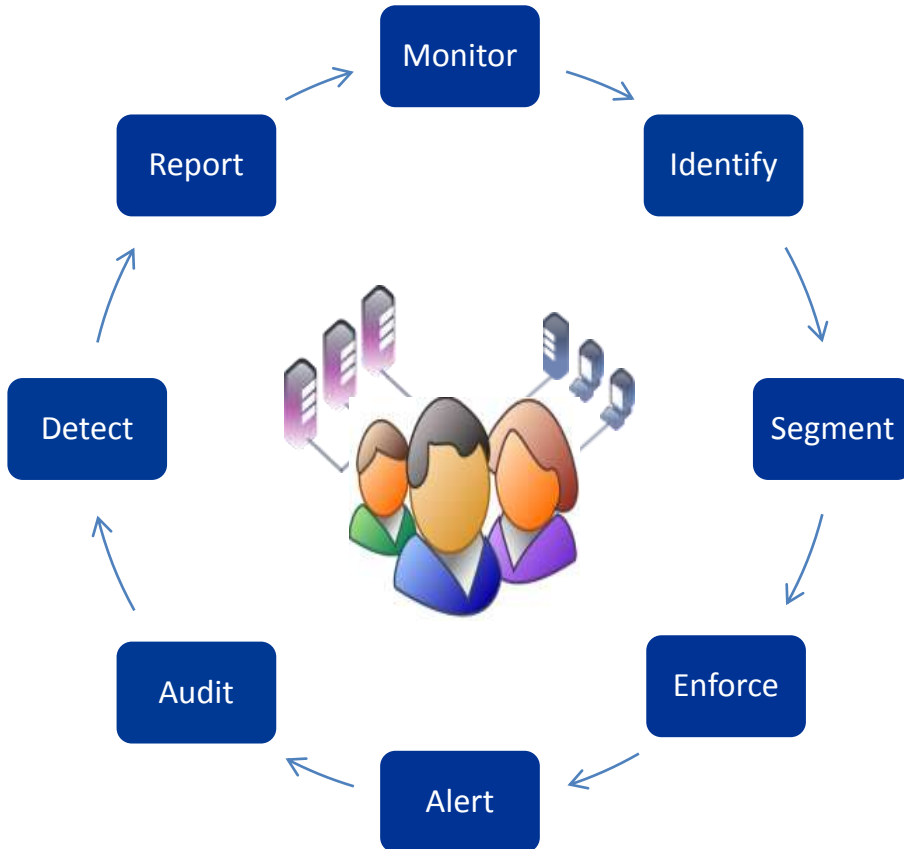
Email Activity

	User	From	To	Subject	Attachments	Application	Time	Client Host/IP
1	Jeremy Chilterns	doarmatt@gmail.com	RJohnson@attinteractive.com / scharsky@attinteractive.com	Status and Invoice f or period ending 3/3 1/09	attinteractive_invoic ce_20090331.pdf	GOOGLE_MAIL	APR 01, 2009 01:42 PM	172.16.3.12
2	Jeremy Chilterns	doarmatt@gmail.com	ap@broadcom.com / gregd@broadcom.com	Invoice for Subversi on Consulting attach ed (PO #1000094297)	broadcom_invoice_svn _20090331.pdf	GOOGLE_MAIL	APR 01, 2009 02:11 PM	172.16.3.12
3	Jeremy Chilterns	doarmatt@gmail.com	ap@broadcom.com / rnugent@broadcom.com	Status and Invoice f or period ending 3/3 1/09	broadcom_invoice_200 90331.pdf	GOOGLE_MAIL	APR 01, 2009 02:29 PM	172.16.3.12
4	Mitchell Christensen	mitchellch@gmail.com	kaganz@sbcglobal.net	Gorilla Economist	EconomistGorilla.jpg	GOOGLE_MAIL	APR 02, 2009 04:44 PM	LT-MITCHC/172.16.3.27
5	Ken Jisser	cloezr@yahoo.com	Tom_thimot@yahoo.com / tthimot@casecentral.com	Per your request	c8ead423defc792b3d4a a09e77250f86" dispos ition="attachment	YAHOO_MAIL	MAR 18, 2009 12:23 PM	LT-KJISSER/172.16.2.8
6	Jeremy Chilterns	doarmatt@gmail.com	mark@keystream.com / schuyler@keystream.com	SVN Changelog script attached	svn2cl.tgz	GOOGLE_MAIL	MAR 19, 2009 08:18 AM	172.16.3.24
7	Ken Jisser	ken.jisser@gmail.com	sdalencon@casecentral.com	Fwd: Please sign the Revised	Revised Genius _ Cen tral Agreement - uns igned.pdf	GOOGLE_MAIL	MAR 20, 2009 10:25 AM	LT-KJISSER/172.16.2.8

File Share Auditing Sample Report



Comprehensive User Activity Management Platform



- ✓ Meet & Maintain Compliance
- ✓ Protect Against Insider Data Breaches
- ✓ Ensure Data Integrity
- ✓ Guard Against Fraud



PacketMotion™

Thank You