Idaho Palm Software

Intrusion Detection
with Login Locator
for Salesforce.com

Idaho Palm
Software
idahopalm.com

Agenda

- The Unnoticed Security Threat to Salesforce.com Environments
- Product Overview
  - Email Alerts
  - Rules and Actions
  - Maps
- Alternatives
- Free Trial

Protection for your Salesforce.com Environment

- Salesforce offers some protection against hackers, but it does not protect you if someone logs in using a stolen username and password.
- 95% of all security breaches are because of human error
- Hackers use phishing and social engineering to obtain login information

How Do You Know Where Your Users are Logging In From?

- If someone were logging in from a foreign country as one of your users, would you know about it?
- Where do your users login from?
- Could someone be logged in as you right now?

Intrusion Detection with Login Locator (IDLL) for Salesforce.com

- What does it do?
  - Monitors IP addresses and locations for Salesforce.com logins
  - Exclusive risk assessment technology tracks each user login
  - Alerts security administrators when malicious login activities occur
  - Provides a current login map of all users

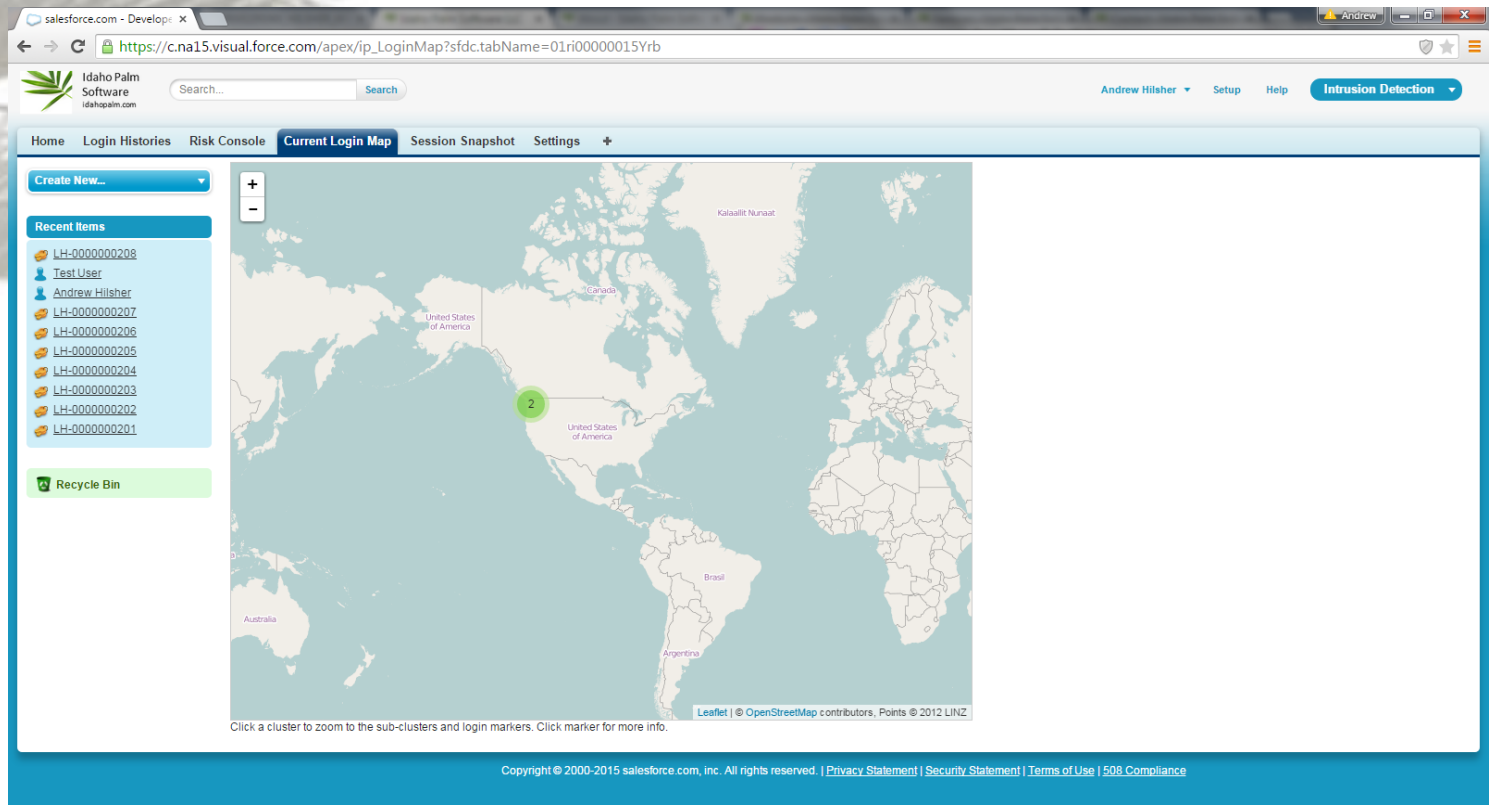
What Rules Can Be Set?

- Monitor Failed Login Attempts
- Detect if a user logs in from two different countries in the same day
- Detect the distance and time difference between logins in mph to detect a possible fraudulent login
- Set higher standards on System Administrator logins
- Accumulate risk assessment information to spot suspect users amongst hundreds of logins

What Actions Can Be Taken?

- In the event of a suspected fraudulent login, we have a “Disable User” button which immediately marks the user login as “inactive”.
- This immediately logs the user out of all connections and they will not be able to log back in until an Administrator flags their account Active

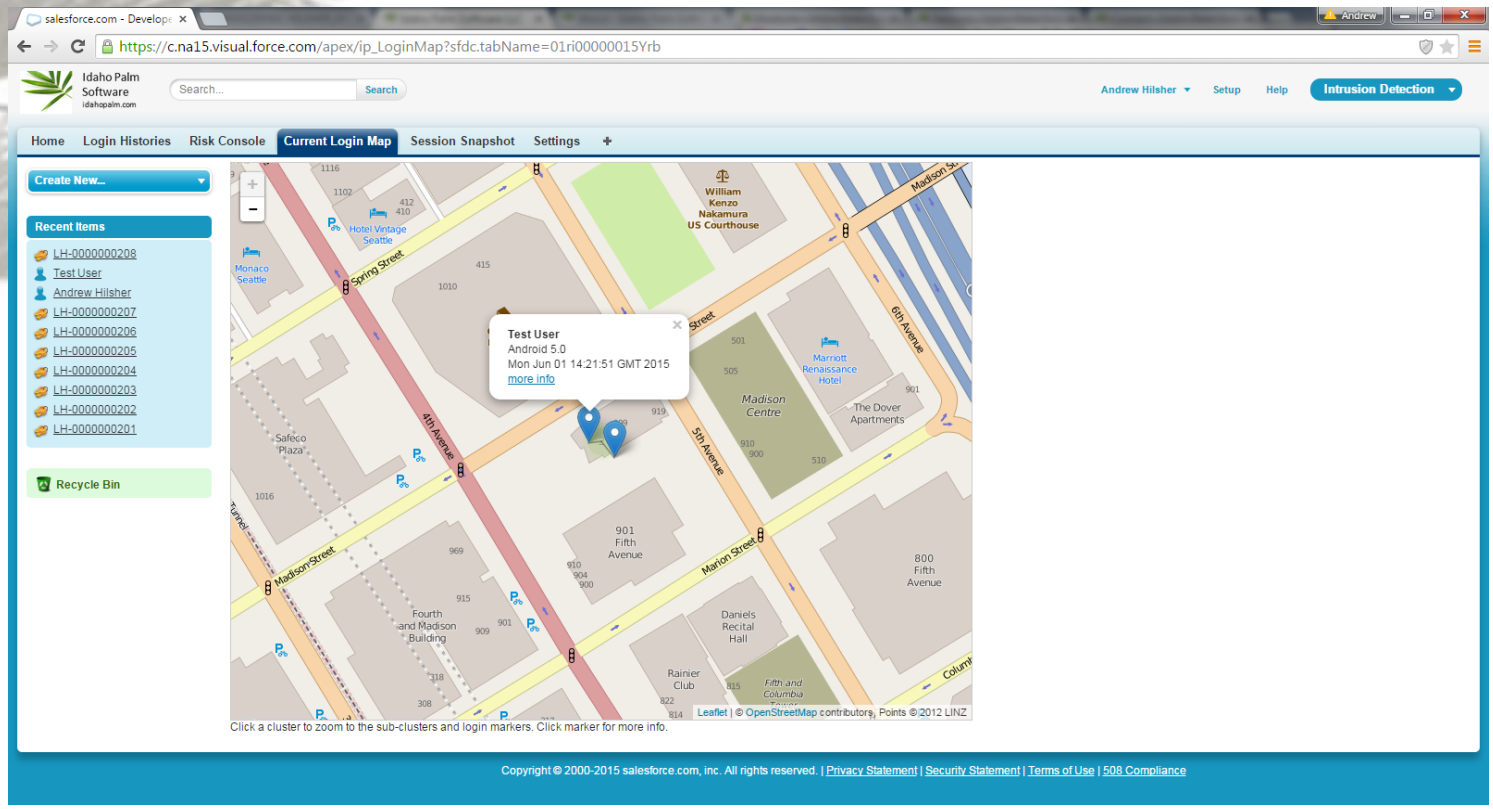
Current Login Map



- Login markers are clustered for easy visibility. Click to drill down.

Idaho Palm Software
idahopalm.com

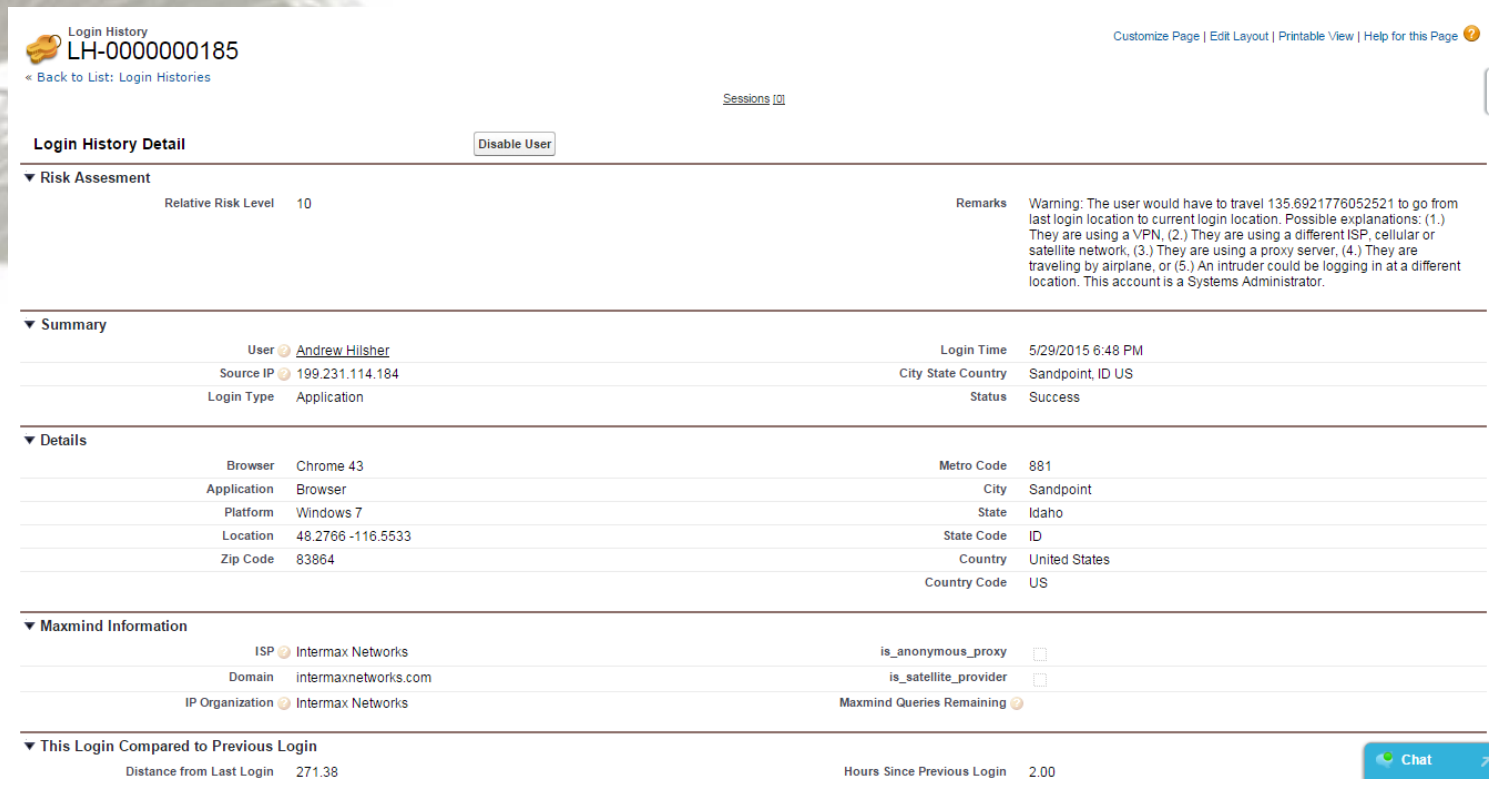
Current Login Map



- Markers provide basic information and allow a click for more details.

Idaho Palm Software
idahopalm.com

Login History Details



Login History
LH-0000000185
« Back to List: Login Histories

Customize Page | Edit Layout | Printable View | Help for this Page

Sessions [0]

Login History Detail Disable User

Risk Assesment

Relative Risk Level	10	Remarks	Warning: The user would have to travel 135.6921776052521 to go from last login location to current login location. Possible explanations: (1.) They are using a VPN, (2.) They are using a different ISP, cellular or satellite network, (3.) They are using a proxy server, (4.) They are traveling by airplane, or (5.) An intruder could be logging in at a different location. This account is a Systems Administrator.

Summary

User	Andrew Hilsher	Login Time	5/29/2015 6:48 PM
Source IP	199.231.114.184	City State Country	Sandpoint, ID US
Login Type	Application	Status	Success

Details

Browser	Chrome 43	Metro Code	881
Application	Browser	City	Sandpoint
Platform	Windows 7	State	Idaho
Location	48.2766 -116.5533	State Code	ID
Zip Code	83864	Country	United States
		Country Code	US

Maxmind Information

ISP	Intermax Networks	is_anonymous_proxy	
Domain	intermaxnetworks.com	is_satellite_provider	
IP Organization	Intermax Networks	Maxmind Queries Remaining	

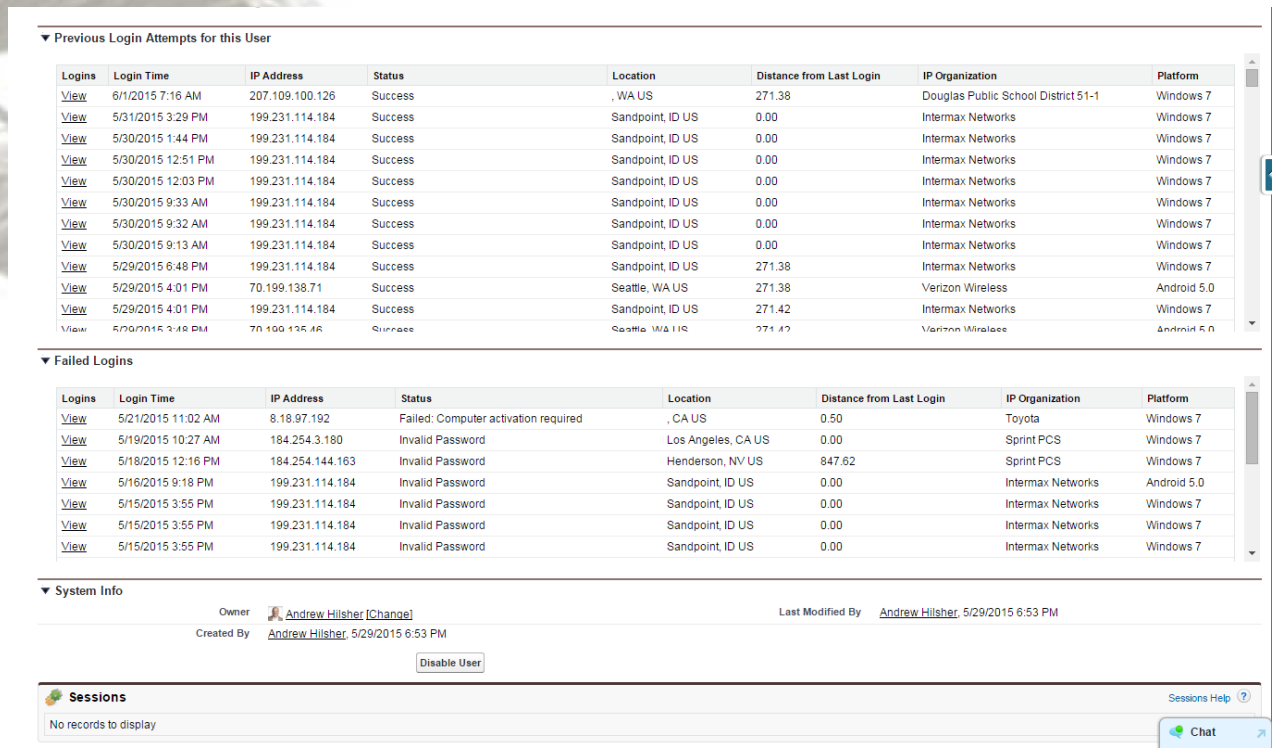
This Login Compared to Previous Login

Distance from Last Login	271.38	Hours Since Previous Login	2.00

Chat

- Login history details include risk assessment and location information.

Login History Details



▼ Previous Login Attempts for this User

Logins	Login Time	IP Address	Status	Location	Distance from Last Login	IP Organization	Platform
View	6/1/2015 7:16 AM	207.109.100.126	Success	, WA US	271.38	Douglas Public School District 51-1	Windows 7
View	5/31/2015 3:29 PM	199.231.114.184	Success	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/30/2015 1:44 PM	199.231.114.184	Success	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/30/2015 12:51 PM	199.231.114.184	Success	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/30/2015 12:03 PM	199.231.114.184	Success	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/30/2015 9:33 AM	199.231.114.184	Success	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/30/2015 9:32 AM	199.231.114.184	Success	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/30/2015 9:13 AM	199.231.114.184	Success	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/29/2015 6:48 PM	199.231.114.184	Success	Sandpoint, ID US	271.38	Intermax Networks	Windows 7
View	5/29/2015 4:01 PM	70.199.138.71	Success	Seattle, WA US	271.38	Verizon Wireless	Android 5.0
View	5/29/2015 4:01 PM	199.231.114.184	Success	Sandpoint, ID US	271.42	Intermax Networks	Windows 7

▼ Failed Logins

Logins	Login Time	IP Address	Status	Location	Distance from Last Login	IP Organization	Platform
View	5/21/2015 11:02 AM	8.18.97.192	Failed: Computer activation required	, CA US	0.50	Toyota	Windows 7
View	5/19/2015 10:27 AM	184.254.3.180	Invalid Password	Los Angeles, CA US	0.00	Sprint PCS	Windows 7
View	5/18/2015 12:16 PM	184.254.144.163	Invalid Password	Henderson, NV US	847.62	Sprint PCS	Windows 7
View	5/16/2015 9:18 PM	199.231.114.184	Invalid Password	Sandpoint, ID US	0.00	Intermax Networks	Android 5.0
View	5/15/2015 3:55 PM	199.231.114.184	Invalid Password	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/15/2015 3:55 PM	199.231.114.184	Invalid Password	Sandpoint, ID US	0.00	Intermax Networks	Windows 7
View	5/15/2015 3:55 PM	199.231.114.184	Invalid Password	Sandpoint, ID US	0.00	Intermax Networks	Windows 7

▼ System Info

Owner Andrew Hilsher [Change]
Last Modified By Andrew Hilsher, 5/29/2015 6:53 PM
Created By Andrew Hilsher, 5/29/2015 6:53 PM

Disable User

Sessions
Sessions Help
No records to display
Chat

- And previous login attempt information for this user.

Solution Positioning

Manual Monitoring
Salesforce Logs

- Low value and Low cost
- No Alerts
- Requires Export and Manual Analysis of Login Log Files

Security Information Event Management (SIEM)

- Wide enterprise value, high cost
- Adds additional burden to Salesforce
- Requires custom integration
- Lacks our location based risk assessment methodology

Idaho Palm Software
idahopalm.com

Solution Positioning

Manual Monitoring Salesforce Logs

- Low value and Low cost
- No Alerts
- Requires Export and Manual Analysis of Login Log Files

Intrusion Detection with Login Locator

- High value and low cost
- No additional performance burden to Salesforce
- No custom integration required
- Self-contained within Salesforce
- Login Maps

Security Information Event Management (SIEM)

- Wide enterprise value, high cost
- Adds additional burden to Salesforce
- Requires custom integration
- Lacks our location based risk assessment methodology

Idaho Palm Software
idahopalm.com

Conclusion

- Intrusion Detection with Login Locator (IDLL) for Salesforce.com
  - Login information with mapping, rules and alerts to prevent fraudulent logins
- High Value / Low Cost – Login Protection
- More information at http://idahopalm.com

- Free 14 Day Trial Available in the Salesforce.com AppExchange
  - https://appexchange.salesforce.com/listingDetail?listingId=a0N30000000qEPCEA2