



A real world look at practical implementation issues and solutions of Intrusion Prevention

Ralph Harvey

Chief Technology Officer, Prevx Inc

December 9th 2004

Agenda

- ▶ **Motivation**
- ▶ **Terminology**
- ▶ **Challenges**
- ▶ **Case Study: Our Solution**
- ▶ **Summary**

Motivation

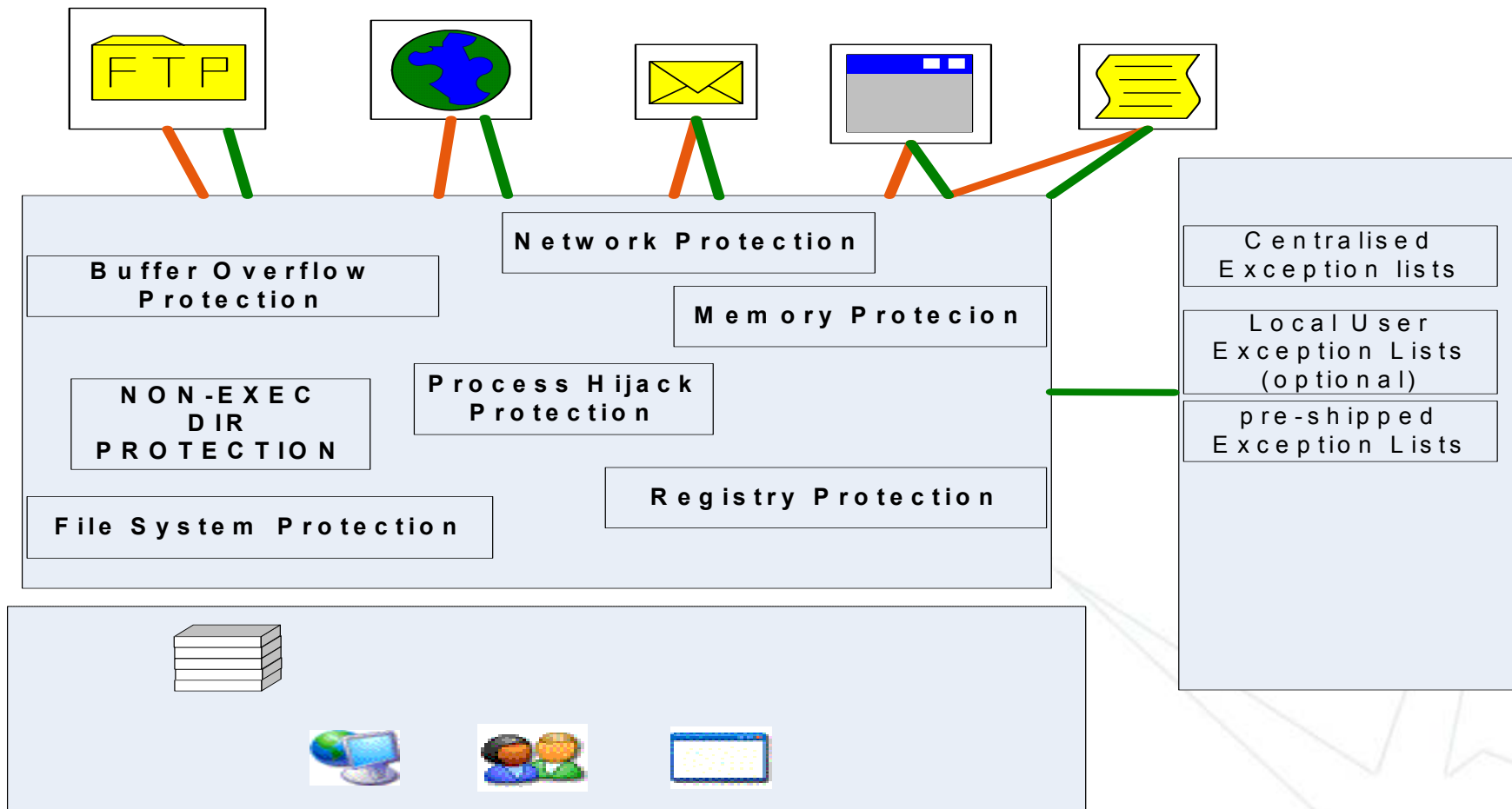
- ▶ **Fight Cyber-Crime and Make Money 😊**
- ▶ **Current forms of protection alone are not generally effective**

What is Intrusion Prevention Software?

- ▶ **For this case study, Intrusion Prevention Software refers to:**
 - ▶ **PREVENTION** of intrusion of zero day and non-zero day threats
 - ▶ Non-signature centric
 - ▶ Protects system resources via policies/rules
 - ▶ Records rule violations via 'events'
 - ▶ For practical purposes – it needs to be manageable

There is no accepted single industry standard definition for IPS today!

What is a policy?



Challenges for Intrusion Prevention Technology

- ▶ **False Positives (noise)**
- ▶ **False Negatives**
- ▶ **Usability**
- ▶ **Defining Policies/Rules**
- ▶ **Managing Policies/Rules**
- ▶ **Collating, Reporting, analyzing on Data**
- ▶ **Cost of Ownership**
- ▶ **Performance**
- ▶ **Scalability**
- ▶ **Sabotage and Subterfuge**

Challenges: A real world trade off.....

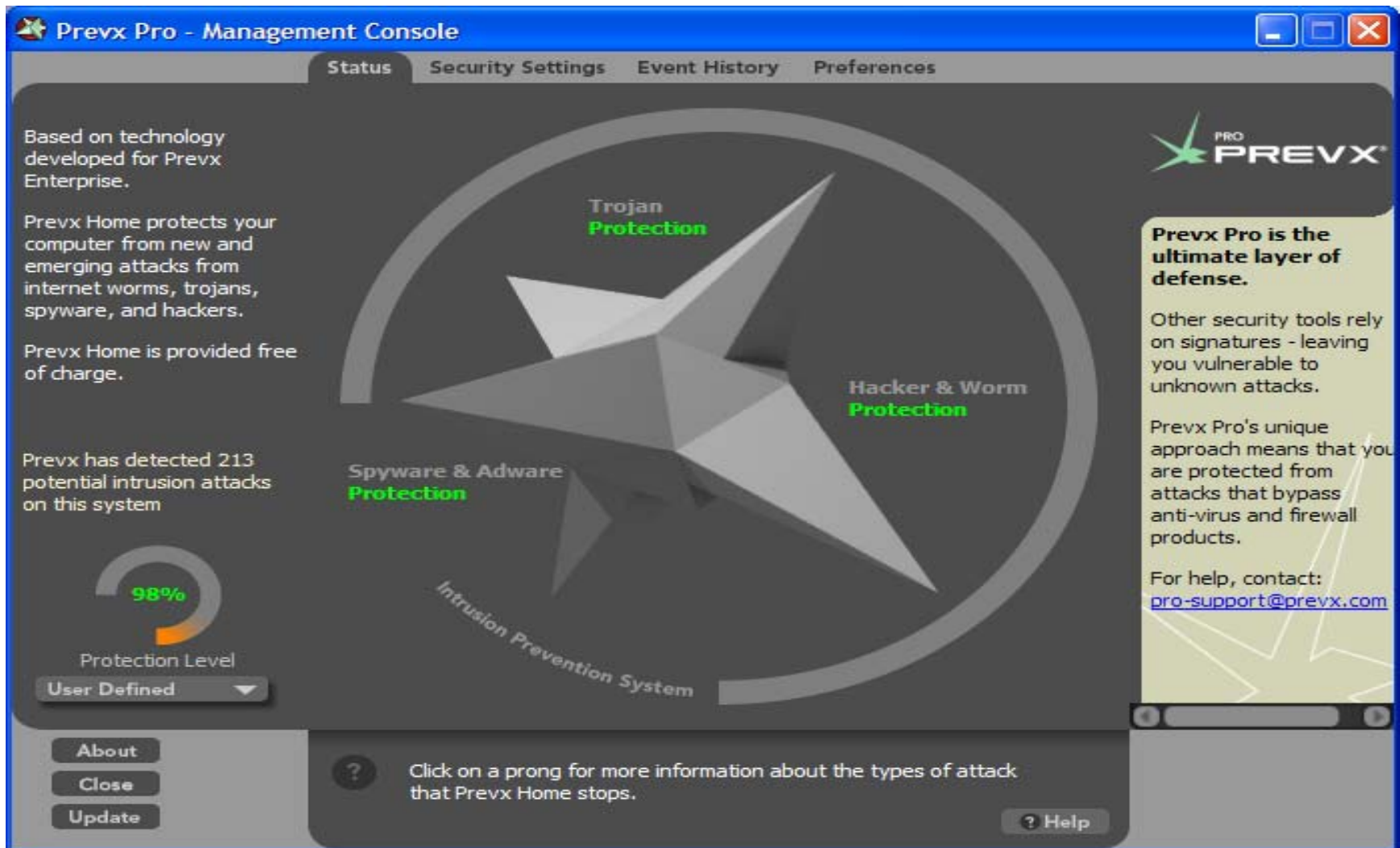
- ▶ **Implementing secure systems is a matter of compromise.**
- ▶ **The more you compromise the more you are compromised.**
- ▶ **The less you compromise the less viable the solution becomes.**

- ▶ **We realised we didn't have all the answers, but we had more than anybody else.**
- ▶ **The only way to gain a holistic insight was to hunt in packs. Expertise was obtained by unique heuristics approach to IPS.**

Case Study: The Prevx Solution

- ▶ **Provide a Scalable back end database technology**
- ▶ **Implement a Kernel Device Driver**
- ▶ **Provide a user interface for the desktop**
- ▶ **Provide a web based administration interface**
- ▶ **Provide a web based reporting and query interface**
- ▶ **Provide a DNA architecture for threat events**
- ▶ **Implement a white list scheme**
- ▶ **Implement realtime 'get advice' assistance**
- ▶ **Allow the IPS system to 'hunt in packs'**

Agent User Interface – Main Screen



Prevx Pro - Management Console

Status Security Settings Event History Preferences

Based on technology developed for Prevx Enterprise.

Prevx Home protects your computer from new and emerging attacks from internet worms, trojans, spyware, and hackers.

Prevx Home is provided free of charge.

Prevx has detected 213 potential intrusion attacks on this system

98%

Protection Level

User Defined

About

Close

Update

Trojan Protection

Hacker & Worm Protection

Spyware & Adware Protection

Intrusion Prevention System

PRO PREVX

Prevx Pro is the ultimate layer of defense.

Other security tools rely on signatures - leaving you vulnerable to unknown attacks.

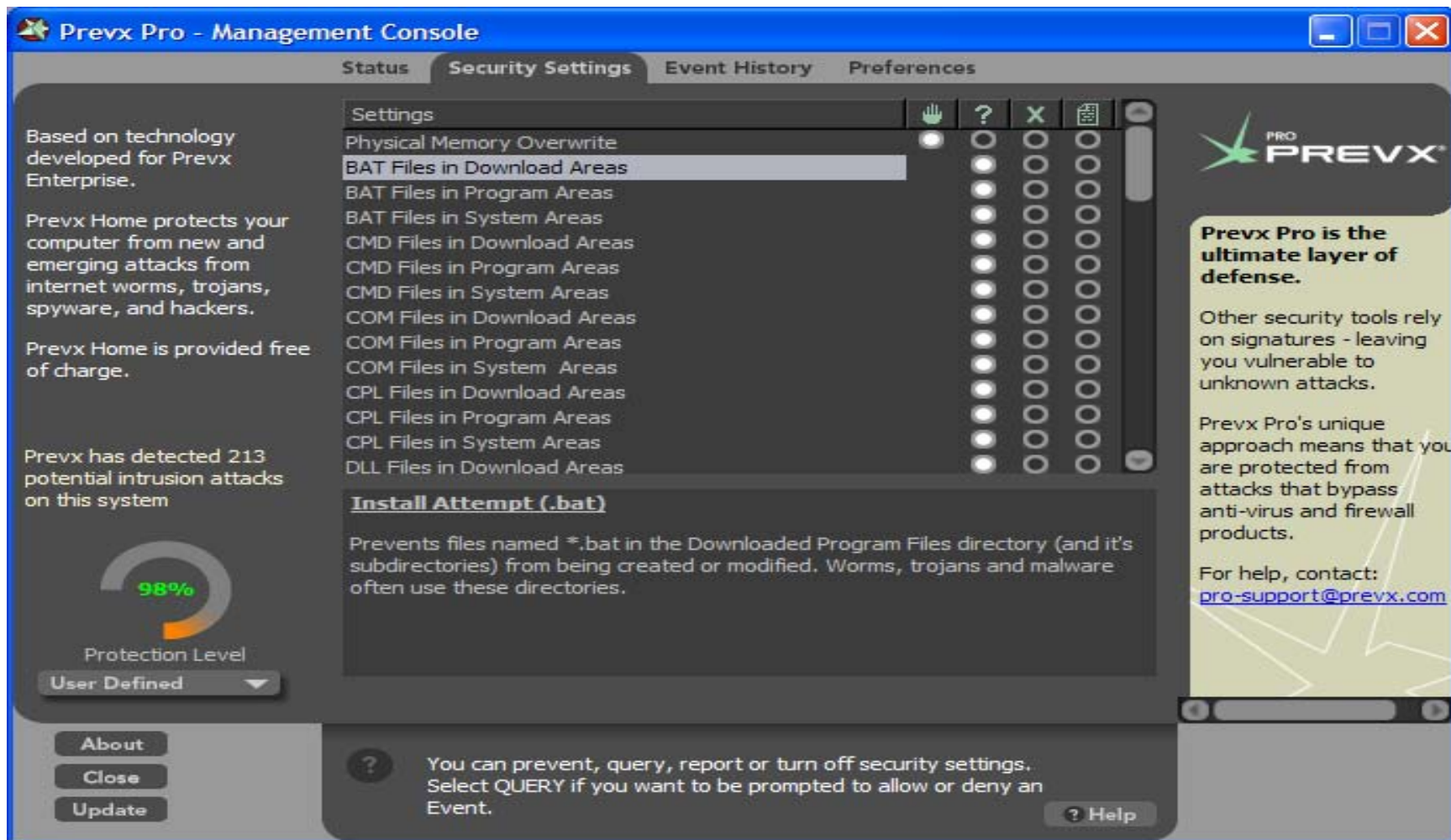
Prevx Pro's unique approach means that you are protected from attacks that bypass anti-virus and firewall products.

For help, contact: pro-support@prevx.com

? Click on a prong for more information about the types of attack that Prevx Home stops.

? Help

Agent User Interface – Security Settings



Prevx Pro - Management Console

Status **Security Settings** Event History Preferences

Settings

Physical Memory Overwrite

BAT Files in Download Areas

BAT Files in Program Areas

BAT Files in System Areas

CMD Files in Download Areas

CMD Files in Program Areas

CMD Files in System Areas

COM Files in Download Areas

COM Files in Program Areas

COM Files in System Areas

CPL Files in Download Areas

CPL Files in Program Areas

CPL Files in System Areas

DLL Files in Download Areas

Install Attempt (.bat)

Prevents files named *.bat in the Downloaded Program Files directory (and it's subdirectories) from being created or modified. Worms, trojans and malware often use these directories.

Based on technology developed for Prevx Enterprise.

Prevx Home protects your computer from new and emerging attacks from internet worms, trojans, spyware, and hackers.

Prevx Home is provided free of charge.

Prevx has detected 213 potential intrusion attacks on this system

98%
Protection Level
User Defined

About
Close
Update

PRO **PREVX**

Prevx Pro is the ultimate layer of defense.

Other security tools rely on signatures - leaving you vulnerable to unknown attacks.

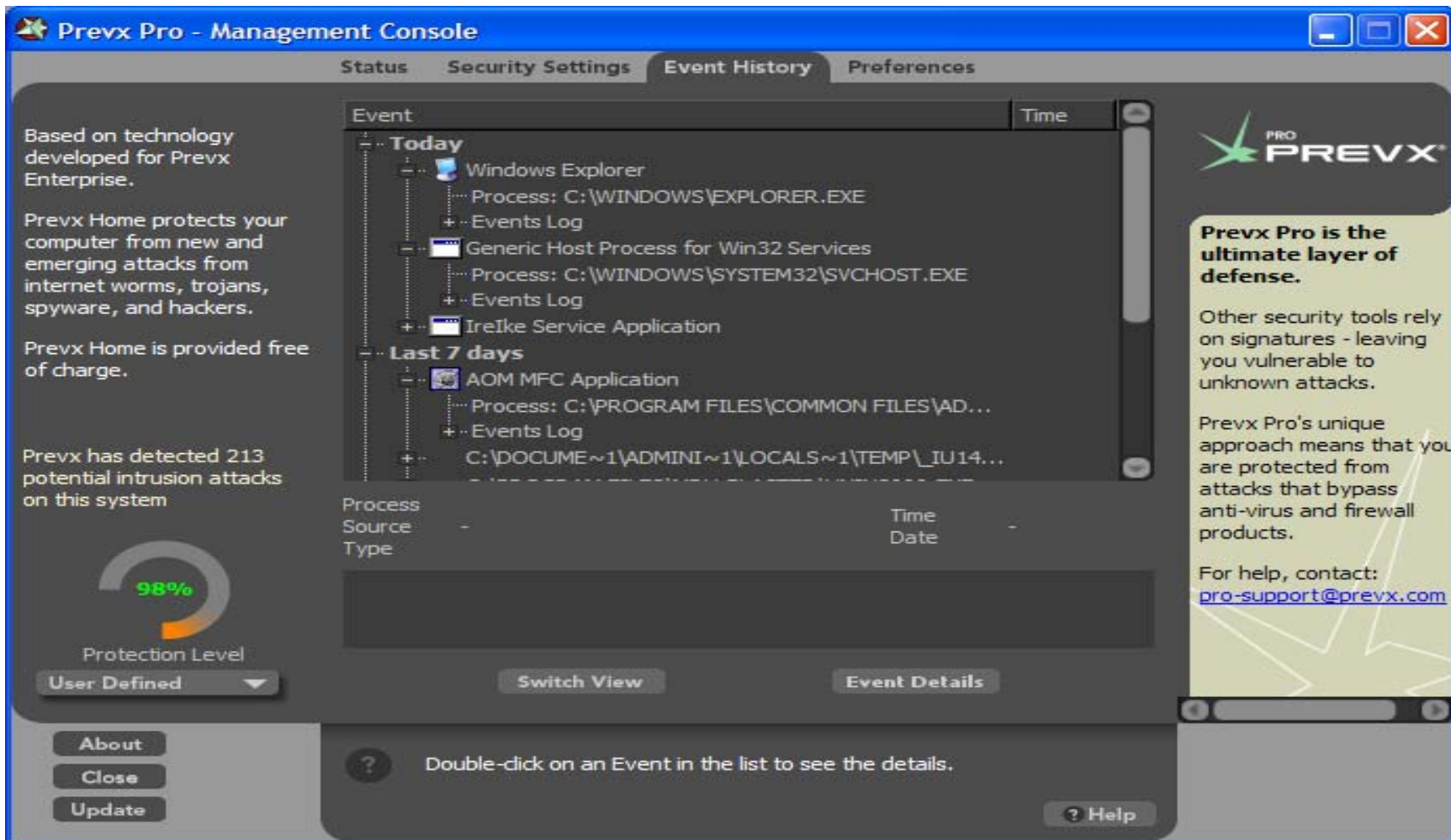
Prevx Pro's unique approach means that you are protected from attacks that bypass anti-virus and firewall products.

For help, contact:
pro-support@prevx.com

? You can prevent, query, report or turn off security settings. Select QUERY if you want to be prompted to allow or deny an Event.

? Help

The Agent User Interface – Event History



Prevx Pro - Management Console

Status Security Settings **Event History** Preferences

Based on technology developed for Prevx Enterprise.

Prevx Home protects your computer from new and emerging attacks from internet worms, trojans, spyware, and hackers.

Prevx Home is provided free of charge.

Prevx has detected 213 potential intrusion attacks on this system

98%
Protection Level
User Defined

Event

Event	Time
Today Windows Explorer Process: C:\WINDOWS\EXPLORER.EXE Events Log	
Generic Host Process for Win32 Services Process: C:\WINDOWS\SYSTEM32\SVCHOST.EXE Events Log	
IreIke Service Application	
Last 7 days AOM MFC Application Process: C:\PROGRAM FILES\COMMON FILES\AD... Events Log	
C:\DOCUME~1\ADMINI~1\LOCALS~1\TEMP_IU14...	

Process Source Type Time Date

Switch View Event Details

About Close Update

Double-click on an Event in the list to see the details.

Help

PRO PREVX

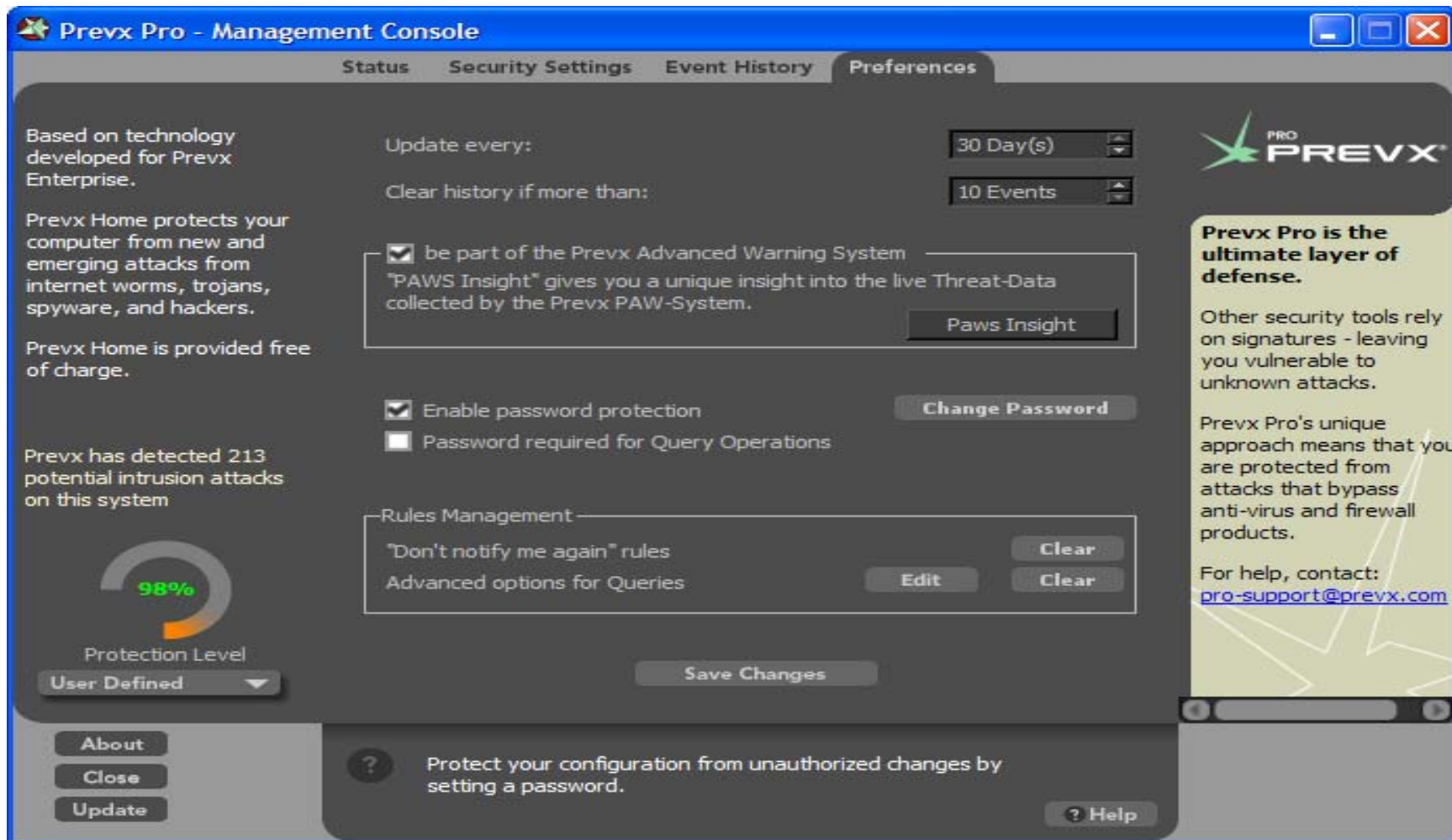
Prevx Pro is the ultimate layer of defense.

Other security tools rely on signatures - leaving you vulnerable to unknown attacks.

Prevx Pro's unique approach means that you are protected from attacks that bypass anti-virus and firewall products.

For help, contact:
pro-support@prevx.com

Agent User Interface - Preferences



Prevx Pro - Management Console

Status Security Settings Event History **Preferences**

Based on technology developed for Prevx Enterprise.

Prevx Home protects your computer from new and emerging attacks from internet worms, trojans, spyware, and hackers.

Prevx Home is provided free of charge.

Prevx has detected 213 potential intrusion attacks on this system

98%
Protection Level
User Defined

Update every: 30 Day(s)

Clear history if more than: 10 Events

be part of the Prevx Advanced Warning System
"PAWS Insight" gives you a unique insight into the live Threat-Data collected by the Prevx PAW-System.
Paws Insight

Enable password protection **Change Password**

Password required for Query Operations

Rules Management
"Don't notify me again" rules **Clear**
Advanced options for Queries **Edit** **Clear**

Save Changes

PRO PREVX

Prevx Pro is the ultimate layer of defense.

Other security tools rely on signatures - leaving you vulnerable to unknown attacks.

Prevx Pro's unique approach means that you are protected from attacks that bypass anti-virus and firewall products.

For help, contact:
pro-support@prevx.com

About
Close
Update

? Protect your configuration from unauthorized changes by setting a password.

? Help

Agent User Interface – Editing Rules

Prevx Pro - Rule Editor

The Rule Editor is used to manage user defined rules.
 Note: These rules only apply to security settings that have been set to Query mode.

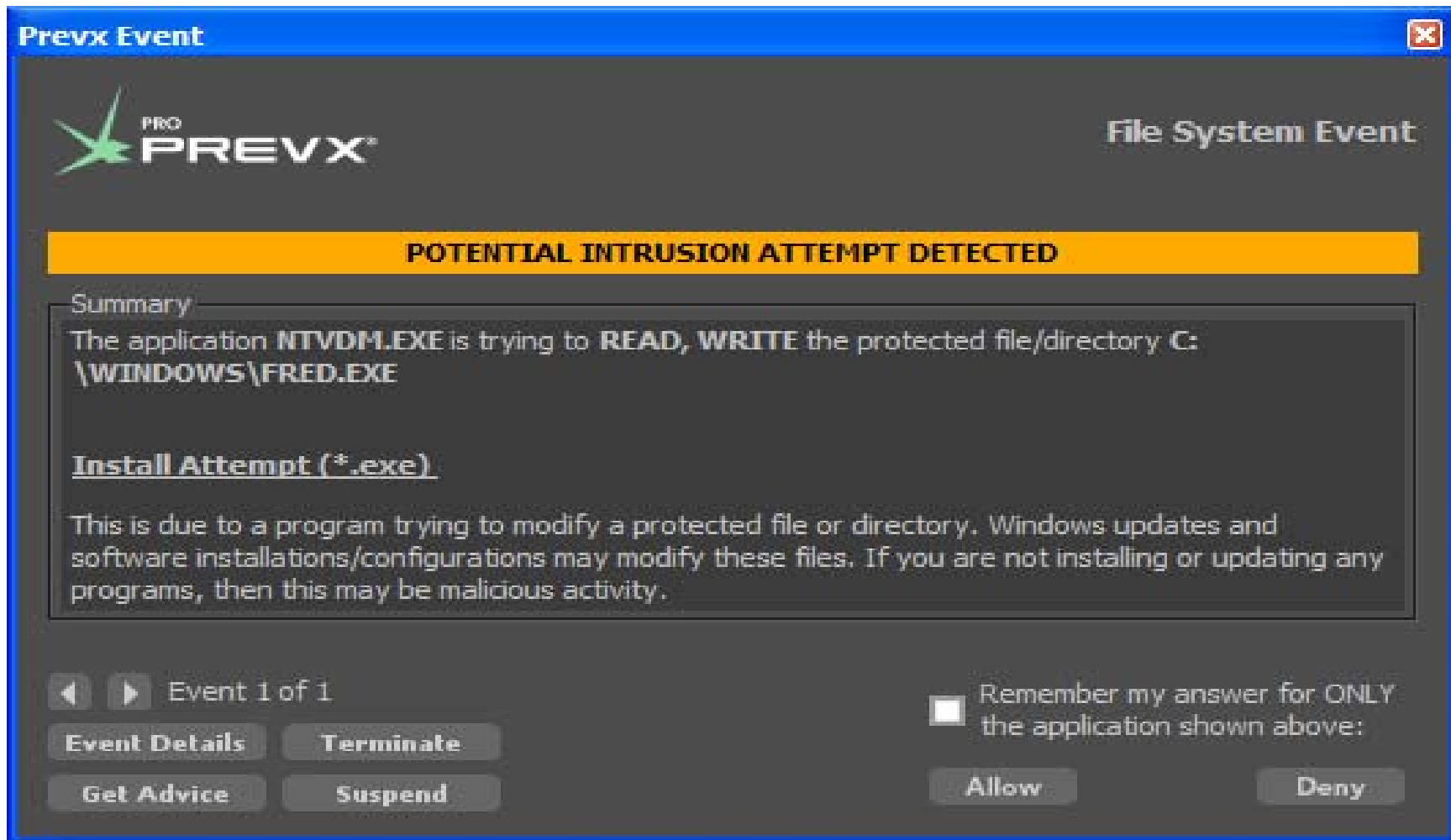
Right-click on an item for more options.

Application	Mode	Security Settings
Internet Explorer		
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO
...DBD 1DAD-C946-4A17-ADC1-64B5B4FF55D0}\n/a	ALLOW	IE - BHO


Item information

OK
Cancel

Event Pop UP



Prevx Event ✕

 **File System Event**

POTENTIAL INTRUSION ATTEMPT DETECTED

Summary

The application **NTVDM.EXE** is trying to **READ, WRITE** the protected file/directory **C:\WINDOWS\FRED.EXE**

Install Attempt (*.exe)

This is due to a program trying to modify a protected file or directory. Windows updates and software installations/configurations may modify these files. If you are not installing or updating any programs, then this may be malicious activity.

◀ ▶ Event 1 of 1

Remember my answer for ONLY the application shown above:

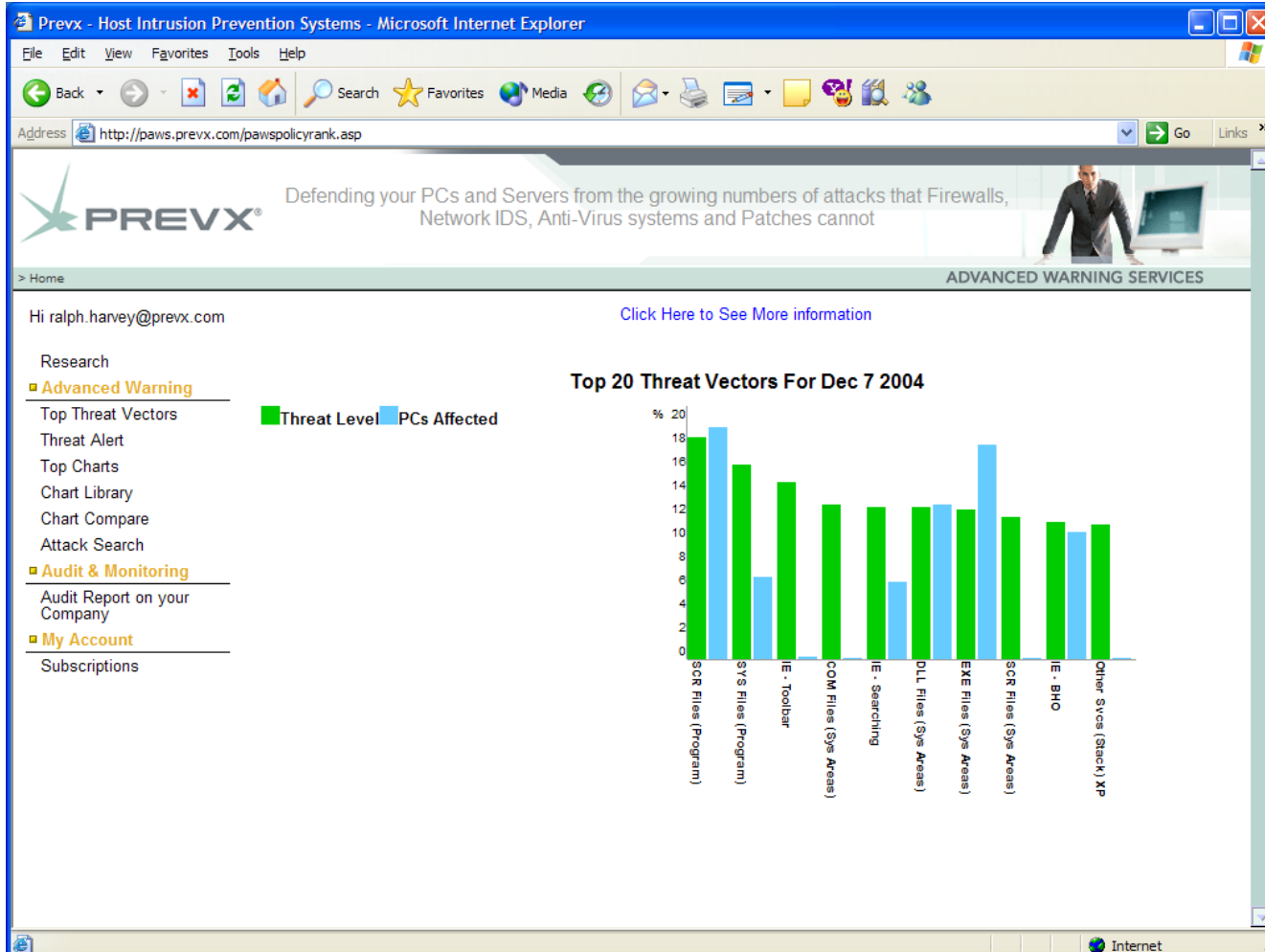
Event Details **Terminate**

Get Advice **Suspend** **Allow** **Deny**

IPS Case Study: Policy Definition via XML (raw view)

- ▶ **Meta Policy Data ===== Title: MS Installer (Installing Attemp) Key: / Version: 00.0 Platform: Windows Security Type: Registry Attributes: Queryable, Reportable, Mutable Install Mode: Mandatory Default: query Policy ID: 0100103000 -->**
- ▶ **.. <policy ID="0100103000" inherit="all">**
- ▶ **.. <process>**
- ▶ **<name />**
- ▶ **<platform>Windows</platform>**
- ▶ **</process>**
- ▶ **.. <image> <!-- All executables -->**
- ▶ **<path>\...*</path>**
- ▶ **<path>*</path> <!-- PREVX Applications excluded -->**
- ▶ **<excludedPath>%ProgramFiles%\PREVX\...\PXL1.exe</excludedPath>**
- ▶ **<excludedPath>\$\$PREVX:Reg:PREVXHome\$\$\PXL1.exe</excludedPath> <!-- Windows Update Applications -->**
- ▶ **<excludedPath>%SystemRoot%\System32\wuauclt*.exe</excludedPath>**
- ▶ **<excludedPath>\WUTemp\com_microsoft.**.exe</excludedPath> <!-- Microsoft Management Console -->**
- ▶ **<excludedPath>%SystemRoot%\system32\mmc.exe</excludedPath>**
- ▶ **<excludedPath>%WinDir%\system32\mmc.exe</excludedPath> <!-- Exclude the following Anti-Virus tools: --> <!-- Kaspersky -->**

Top threat monitoring



Coolwebsearch attack

Prevx - Host Intrusion Prevention Systems - Microsoft Internet Explorer

Address <http://paws.prevx.com/pawsresearch.asp?pg=agentchron&direct=F&IID=426520>

Google Search Web 9 blocked AutoFill Options

Hi paul.stubbs@prevx.com

Research

- Advanced Warning
- Top Threat Vectors
- Threat Alert
- Top Charts
- Chart Library
- Chart Compare
- Attack Search

Audit & Monitoring

- Audit Report on your Company

My Account

- Subscriptions

Agent 800012222 in Area US with DNA of PDCAB

Date	Times Seen	Policy	Allowed	Actor File	Victim File	Actor Path	Vi
30/11/2004 16:21:31	1	Temp Areas Exec (200000006)	Allowed, Policy in report mode	CALYX.POINT.4.0.EXE	MMWORK.EXE	%systemdrive%\mydownloads\	%ter
30/11/2004 16:22:01	1	EXE Files (Sys Areas) (110100002)	Allowed once by user	MMWORK.EXE	UNSTALL.EXE	%temp%\varstb\0\	%
30/11/2004 16:22:22	1	EXE Files (Sys Areas) (110100002)	Allowed once by user	MMWORK.EXE	DOWNLOAD.EXE	%temp%\varstb\0\	%
30/11/2004 16:22:51	1	Run-Keys (100100002)	Allowed once by user	DOWNLOAD.EXE	DEALHELPERDOWN.*REGVAL	%windir%\ hku*\software\microsc	
30/11/2004 16:22:52	1	EXE Files (Sys Areas) (110100002)	Allowed once by user	MMWORK.EXE	MMUPS.EXE	%temp%\varstb\0\	%
30/11/2004 16:30:08	1	EXE Files (Sys Areas) (110100002)	Allowed once by user	DOWNLOAD.EXE	DEALHELPER.EXE	%windir%\	%
30/11/2004 16:30:09	1	Run-Keys (100100002)	Allowed once by user	MMUPS.EXE	MEDIAMOTOR.EXE.*REGVAL	%windir%\ hklm\software\microsc	

Internet

Policy Management and Tracking

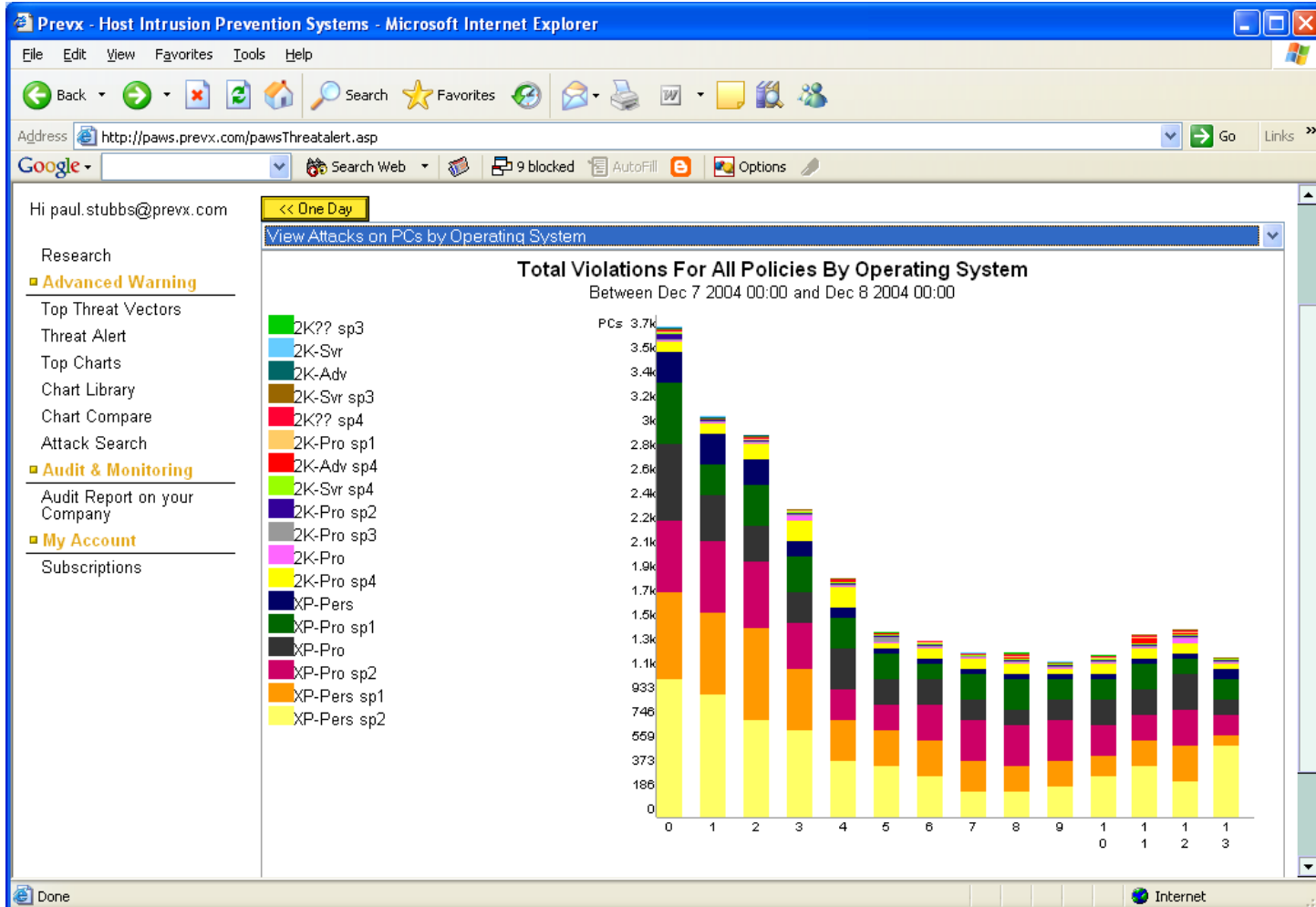
Prevx ADMIN Site. - Microsoft Internet Explorer

Address: https://admin.prevx.com/adminactstats.asp

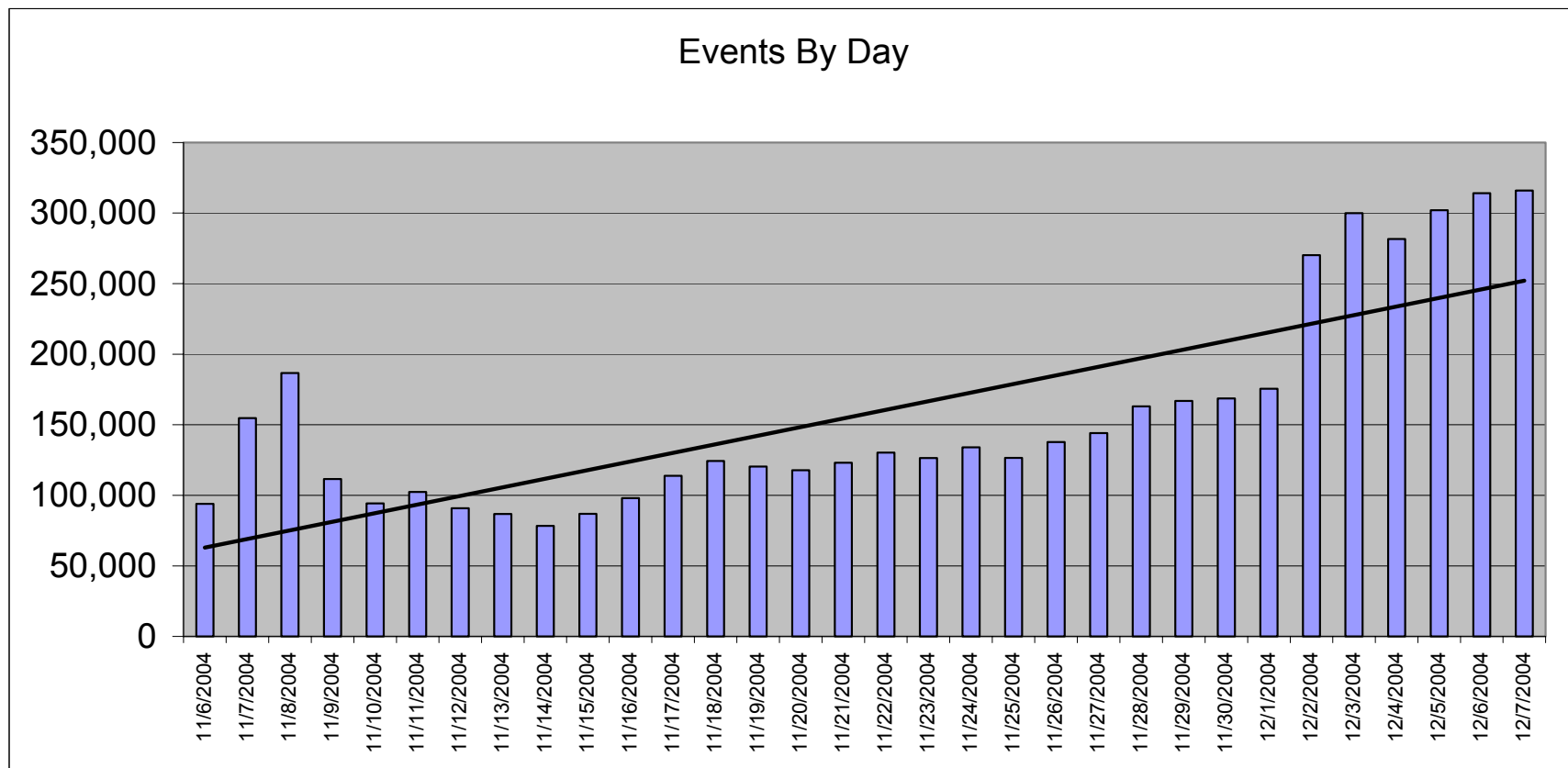
ACT Updater Content Served Statistics

DNA Table	Nov 21	Nov 21	Nov 21	Nov 21	Nov 22	Nov 23	Nov 24	Nov 25	Nov 26	Nov 27	Nov 28	Nov 29	Nov 30	Dec 1	Dec 2	Dec 3	Dec 4	Dec 5	Dec	
DNA Table	62714	100692	97459	97559	98028	99586	104458	109017	86812	95170	112465	113978	111487	115879	1215					
Version: 1	-	-	-	-																
MARKETING UPDATE: BvhluxPL7zH1eJf0+NHBg==	3847	2967	2900	2796	2748	1834	1588	1738	1823	1978	2142	2291	3169	2949	2737	2763	2894	30		
POLICY CATALOGUE	7546	7194	7890	8160	8801	6320	5952	6150	6251	6703	7350	8137	9195	8877	9041	9278	9261	9716	1	
POLICY: 100000000	30	18	25	28	31	33	13	17	11	14	18	20	14	24	17	26	12			
POLICY: 100001000	30	15	25	27	31	33	13	17	11	14	18	19	14	24	17	26	12			
POLICY: 100002000	30	15	25	27	31	33	13	17	12	14	18	19	14	24	17	26	12			
POLICY: 100003000	30	18	25	28	31	33	13	17	12	14	18	20	14	24	17	26	12			
POLICY: 100004000	30	15	25	27	31	33	13	17	12	14	18	19	14	24	17	26	12			
POLICY: 100100000	30	16	25	27	31	37	16	18	12	14	18	19	14	24	17	26	12			
POLICY: 100101000	30	18	25	28	31	33	13	17	12	14	18	20	14	24	17	26	12			

Policy Violations Monitoring



Tracking Events



Intrusion Prevention – Case Study Summary

- ▶ **Prevx have implemented a product and expertise based solution that is working for > 250,000 active users today**
- ▶ **The techniques and software adopted can be applied to both controlling and monitoring access to key resources as well as pure Intrusion Prevention**
- ▶ **The product and knowledge based architecture scale from consumer (free) versions through to Enterprise implementations.**

- ▶ **Try it for free at www.prevx.com**

QUESTIONS?

Ralph Harvey

CTO Prevx Inc

ralph.harvey@prevx.com

www.prevx.com