Managing USB Mass Storage Devices – Best Practices

The Importance of Consolidation, Correlation, Detection – Enterprise Security Series
Abstract

In the last few years, portable, high capacity USB storage devices like thumb/flash drives have become increasingly prevalent in corporations, and devices such as cell phones, PDA’s, iPods all can serve as USB storage devices. These devices are incredible productivity aids – large files can be moved from computer to computer without the need to maintain shared drives, or even worry about file sizes preventing email. Personnel are also able to take files home to work on home computers off hours. The issue is that all these advantages introduce significant security vulnerabilities at the same time.

This White Paper discusses how you can take advantage of the power of these devices without leaving your operation wide open to critical company information being misappropriated. Until now the choice has been to either shut down USB devices – either in Active Directory or through more extreme methods (the “glue in the USB port’ trick comes to mind) - or simply trust every user to do the right thing. This paper introduces a third way that Prism Microsystems calls “Trust but Verify’ which is made possible by EventTracker’s advanced USB monitoring capability.

The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
The Upside/Downside of USB Devices

High capacity portable storage devices are a powerful productivity enhancement for knowledge workers today, and their upsides are numerous. A flash drive allows personnel to move files and data easily without worrying about shared drives, FTP, network access, or large files getting stripped by mail servers. USB devices are cheap, reusable and convenient. Insert a USB, drag a file or files, unplug and you are done. In a surgical center at a hospital, for instance, the X-ray technician can capture an X-ray as a digital image, drag it onto a USB drive, and walk it down to the physician in the Examination or Operating Room. No need for network connectivity between the two departments, and no need to develop an expensive and slow print image of the X-ray.

The Challenges of USBs, however, are also clear. Number one is that sensitive data can often go outside the “green zone”. This can be through an inadvertent act such as an employee copies a file onto a USB legitimately, but then forgets to delete it and subsequently loses the USB device, or an overt action where an employee intentionally copies sensitive materials and carries them off premises. The result however, is the same – you have sensitive data “in the wild’. There is a huge potential for damage from both the “whoops’ case and the outright malice case of a disgruntled employee or cyber-criminal.

With USB devices being so widespread, it also becomes very difficult to exercise granular control. How do you prevent USB devices that are no larger than car-keys from entering the premises? And with cell-phones and iPods all having storage capability, what do you do – forbid those onsite as well? Doing so results in a lot of very unhappy employees that either ignore the policy or are less productive.

After studying the typical profiles of people that represent insider threats Prism Microsystems came up with the following four user profiles that must be defended against:

- The D’oh!
  - My MP3 player has a disk? Who knew? I was just plugging it in to charge it. This person is not generally a security threat, but if all you can monitor are USB inserts/removes, this sends a red flag up every time.
- The Opportunist
  - Well, well, lookie here, payroll.xls, let me grab it and look at it later.
- The Disgruntled
  - I deserved that raise, mutter, I’ll show you guys
- The Professional
  - Gone in sixty seconds

If you treat everyone as a potential “Professional’ you end up spending all your time chasing your tail for that one in a hundred or thousand instances, but if you ignore the problem and feel that everyone is the “D’Oh” type, you will, eventually, get burned by a leak either malicious or innocent.
USBs - Fad or Real Problem?

Recently, RSA Conference released the results of a 2008 Survey\(^1\) on critical industry and infrastructure issues that security professionals feel they will face in the next 12 months. 49% of respondents reported that data leakage was their number one security threat. When queried about their security challenges, lost and stolen devices was also number one at 49%.

![Image of survey results]

Although it would be unfair to tie all data leakage to USB devices, they undoubtedly account for a great part of the increased risk profile. Other studies on the cost of different types of security breaches have found that data leakage is one of the costliest types of breach when it occurs. There has been a sea-change in the security industry recently from perceiving insider threats as being insignificant, to the realization that while outsider attacks happen more frequently, the success rate of such attacks is quite small, and, while the number of insider threat numbers are more modest, the likelihood of success and the damage inflicted in terms of company reputation and lost profits is generally far higher.

Jim Slaby at the Yankee group recently came out with a list of myths about Endpoint Security\(^2\) which includes USB access that he feels people in the industry still need education on. He included a few important points:

- The traditional network security perimeter provides adequate protection against endpoint security threats.
- End-users can be trusted to follow best practices to maintain a secure endpoint environment.

---


None he believes are true and leaves the necessity to act in the hands of the security professionals. The challenge is clear – how do you harness the advantages of USB devices without suffering the potentially serious consequences?

**Trust but Verify (doverai, no proveryai)**

**Recommendations**

1. Any successful program begins with a policy and education. In talking with customers we have found that there are still many users that fall into the first category (the “D’Oh!”) described above. It is necessary to put in place a formal policy and publish it. This policy should document what types of devices are permitted and what types of files are permitted to be put onto these devices. Also inform users that USB activities are being monitored for compliance. This alone will reduce the number of users in category one, as well as deter the ‘Opportunist’.

2. Classify assets by value and risk. For USB usage on critical servers for instance, we recommend restricting USB devices to a list of devices known and tracked by IT staff, with any other access disabled. Workstations are trickier – you want employees to have the freedom to move work around if they are working in multiple locations and are collaborating with others. We suggest leaving USB access open but monitoring the usage and the files being placed on USBs.

3. Employ continuous monitoring. First, log every insert and removal of any type of device. Second, disable and immediately alert IT staff on an attempt to violate policy. Third, log all the files copied to USB devices in every instance, and retain those records for forensic and reporting purposes.

4. Schedule reports and actively review all USB activities. Make it part of the security policy for someone to analyze, investigate any suspicious activity, and sign-off on the reports.

**Implementation**

EventTracker Security LCC has added support for “Trust but Verify’ within the EventTracker solution. Within EventTracker’s policy console, security personnel can define a list of permitted USB devices (by their serial numbers) for each Windows machine or group of machines. Using the EventTracker Windows agent this list of permitted devices is pushed out to the local machines so access can be controlled immediately with no requirement to look up policy on an EventTracker Console.
Every time a USB is inserted, the EventTracker agent looks at its permission list, and if there is no violation of policy, permits the device access, while logging the insert activity. If a violation of policy is detected, access is prevented and the violation is immediately sent to the EventTracker Console. At this point if access is permitted, EventTracker also begins to actively monitor all activity on the device, and every file that is written to or deleted from the device is recorded. A complete audit trail that consists of the user, device type, serial number, time and all the file activity is captured and sent as an event to the EventTracker Console for processing.

EventTracker further provides several preconfigured alerts on device inserts, as well as reports that provide daily and weekly analysis of USB activity by machine or by user. Using EventTracker’s advanced analytics engine you can also look for patterns of behavior – for instance, every user that has copied a file in the last \( n \) months. This provides powerful capability to trace a breach should one occur.

### Sample Reports

#### Sample Report #1: USB Activity Report by Machine

<table>
<thead>
<tr>
<th>USB Device Detail Report</th>
<th>EventTracker Report PMI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer LEMONYELLOUSB devices used is 1</td>
<td></td>
</tr>
<tr>
<td>USB Device (G: ) with Serial No. 761664230 active users is 1</td>
<td></td>
</tr>
<tr>
<td>User LEMONYELLO\JAGAT file activity is 4</td>
<td></td>
</tr>
<tr>
<td>Active Users: PRISMUSA\Jagat</td>
<td></td>
</tr>
<tr>
<td>File Activity Time</td>
<td>File Activity</td>
</tr>
<tr>
<td>9/8/2008 12:20:08PM</td>
<td>Modified</td>
</tr>
<tr>
<td>9/8/2008 12:21:06PM</td>
<td>Added</td>
</tr>
</tbody>
</table>

#### Sample Report#2: Summary Report

This report shows 'files added/modified/deleted' to usb device from your enterprise.

From Date: 07-Sep-2008 4:01:47 pm
To Date: 08-Sep-2008 4:01:47 pm

Computers Selected: LEMONYELLO

<table>
<thead>
<tr>
<th>USB Device Serial No</th>
<th>Event User</th>
<th>Active Users</th>
<th>Added Files</th>
<th>Modified Files</th>
<th>Deleted Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>761664230</td>
<td>LEMONYELLO\JON</td>
<td>PRISMUSA\JON</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
The EventTracker Solution

The EventTracker solution is a scalable, enterprise-class Security Information and Event Management (SIEM) solution for Windows systems, Syslog/Syslog NG (UNIX and many networking devices), SNMP V1/2, legacy systems, applications and databases. EventTracker enables “defense in depth”, where log data is automatically collected, correlated and analyzed from the perimeter security devices down to the applications and databases. To prevent security breaches, Event Log data becomes most useful when interpreted in near real time and in context. Context is vitally important because often the critical indications of impending problems and security violations can only be learned by watching patterns of events across multiple systems. Complex rules can be run on the event stream to detect signs of such a breach. EventTracker also provides real-time alerting capability in the form an email, page or SNMP message to proactively alert security personnel to an impending security breach.

The original Event Log data is also securely stored in a highly compressed event repository for compliance purposes and later forensic analysis. For compliance, EventTracker provides a powerful reporting interface, scheduled or on-demand report generation, automated compliance workflows that proves to auditors that reports are being reviewed and many other features. With pre-built auditor grade reports included for most of the compliance standards (FISMA, HIPAA, GLBA, SOX and NISPOM); EventTracker represents a compliance solution that is second to none. EventTracker also provides advanced forensic capability where all the stored logs can be quickly searched through with a powerful Google-like search interface to perform quick problem determination.

EventTracker provides the following benefits

- A highly scalable, component-based architecture that consolidates all Windows, SNMP V1/V2, legacy platforms, Syslog received from routers, switches, firewalls, critical UNIX servers (Red Hat Linux, Solaris, AIX etc), Solaris BSM, workstations and various other SYSLOG generating devices.
- Automated archival mechanism that stores activities over an extended period to meet auditing requirements. The complete log is stored in a highly compressed (>90%), secured archive that is limited only by the amount of disk storage.
- Real-time monitoring and parsing of all logs to analyze user activities such as logon failures, failed attempts to access restricted information.
- Alerting interface that generates custom alert actions via email, pager, beep, console message, etc.
- Event correlation modules to constantly monitor for malicious hacking activity. In conjunction with alerts, this is used to inform network security officers and security administrators in real time. This helps minimize the impact of breaches.
- Various types of network activity reports, which can be scheduled or generated as required for any investigation or meeting audit compliances.
• Host-based Intrusion Detection (HIDS).
• Role-based, secure event and reporting console for data analysis.
• Change Monitoring on Windows machines
• Built-in compliance workflows to allow inspection and annotation of the generated reports.

Conclusion

USB devices are here to stay and are simply too valuable a productivity aid to prohibit their use. By using EventTracker and implementing a “Trust but Verify” policy, an enterprise is able to put in place a cost-effective, pragmatic approach to handling USB devices that will substantially improve USB security without inconveniencing the correct and proper usage of these devices. With powerful and integrated log and change management, combined with USB monitoring, EventTracker represents the most powerful single solution for improving security on Windows desktops and servers.

About EventTracker

EventTracker’s advanced security solutions protect enterprises and small businesses from data breaches and insider fraud, and streamline regulatory compliance. The company’s EventTracker platform comprises SIEM, vulnerability scanning, intrusion detection, behavior analytics, a honeynet deception network and other defense in-depth capabilities within a single management platform. The company complements its state-of-the-art technology with 24/7 managed services from its global security operations center (SOC) to ensure its customers achieve desired outcomes—safer networks, better endpoint security, earlier detection of intrusion, and relevant and specific threat intelligence. The company serves the retail, hospitality, healthcare, legal, banking and financial services, utilities and government sectors.

EventTracker is a division of Netsurion, a leader in remotely-managed IT security services that protect multi-location businesses’ information, payment systems and on-premise public and private Wi-Fi networks. www.eventtracker.com.